Algebra

Anders Thorup

Matematisk Afdeling
Københavns Universitet

Anders Thorup, e-mail: thorup@math.ku.dk
Algebra, 3. udgave

Matematisk Afdeling
Universitetsparken 5
2100 København Ø
ISBN 87-91180-28-7

Advarsel

»Mindre i skat«. SuperGeil
skrotter folkekirken og tager til asebryllup med
vikinger, mjød og hornmusik. Sex Pistol får flasker
i hovedet, Djarnis-drengen giver Frank-drengen en lussing,
og færgespotteren Thomas bliver varm om hjertet af at tælle færger.
[Avisomtalen af et tv-program på DR2, onsdag kl 20.10 den 15.1.97.]

Læs ikke noterne før du har gjort dig klart, at en matematisk tekst ikke læses på samme måde som en almindelig tekst. Citatet ovenfor må antages at være skrevet i et ungt, levende, nutidigt sprog. Teksten er næppe beregnet for min generation, og for mig er informationsværdien i hvert fald forsvindende. Det er formodentlig muligt at skrive en matematisk tekst i et tilsvarende sprog. Du vil opdage, at det er ikke forsøgt med nærværende notesæt. Her er sproget noget tungt og lidt gammeldags — for at minde om at matematik er en alvorlig sag — og vel fordi det er det der falder mig lettest.

Det er imidlertid ikke sproget, der er den væsentligste forskel mellem matematisk og anden tekst. En matematisk tekst skal kunne læses som enhver anden tekst, men den er ikke beregnet til kun at blive læst: den skal forstås, og den skal sætte tanker igang. Noterne skal ikke bare kommunikere mine tanker, de skal sætte dig i gang med at tænke selv. Forskellen ligger specielt i beviserne, og det er også her fælderne ligger. I beviset ligger svaret på, hvorfor en påstand er rigtig (men ikke et svar på, hvorfor den er interessant). Dybest set er et bevis blot en serie argumenter, der kan overbevise andre (og helst også en selv) om påstandens rigtighed. Et godt bevis er et, der kan overbevise mange. Et matematisk bevis er et, der kan overbevise alle.

Du går i fælden, hvis du læser beviser med den positive holdning, at du da gerne vil overbevises. Vær negativ! Vær antiautoritær! Tro ikke på noget! Mine forsøg på at få dig til at tænke selv er ofte gemt i en række nøgleord som „øjensynlig“, „klart“, „trivielt“, „altså“, „derfor“, „medfører“, „dvs“, „følger“ og mange, mange flere. Lad os tage et par af ordene: Hvis der står, at „tallet $i\sqrt{2}$ er øjensynlig rod i polynomiet $x^2 + 3$“, så er det ikke alene fordi jeg kan se det for mig, men fordi jeg mener at *du* bør kunne se det. Du *skal* prøve at se det; kan du ikke, er det måske fordi du ikke har de rigtige forudsætninger: du mangler måske tilstrækkelig fortrolighed med komplekse og irrationale tal, eller med de indgående begreber som rod og polynomium — det kan jo også være fordi jeg har skrevet noget sludder. At der står om en påstand, at den er „triviel“, betyder ikke, at jeg har let ved at indse den. Det betyder, at påstanden er enkel og at den kan begrundes simpelt udfra et indlysende begrænset antal forudsætninger; men først og fremmest betyder det, at *du* skal kunne indse den. Tag aldrig alene mit ord for, at noget er trivielt. Vendingen „nu følger det, at $2 + 2 = 4$" står der ikke fordi jeg mener, at nu må det være på tide at anføre denne påstand; det betyder, at *du* skal kunne indse, at påstanden er en konsekvens af foregående påstande.

Noterne er delt i 5 dele: TAL om tallene, GRP om grupper, SYM om symmetrier, RNG om ringe og legemer, og POL om polynomier. At de 5 dele ikke er nummererede, afspejler, at matematisk teoridannelse ikke er lineær. Det optimale er at læse samtlige dele på én gang. Men mindre kan gøre det. En rimelig gennemgang af materialet vil dog uundgåeligt indeholde nogle spring mellem delene: Interessante eksempler på grupper kommer fra geometrien, og en række geometriske påstande ses bedst i et gruppeteoretisk lys. Polynomiumsringe er en vigtig klasse af ringe, som illustrerer nogle af de generelle begreber i ringteori. Og omvendt, en række egenskaber ved polynomiumsringe er den klare inspiration for nogle af de generelle begreber.

Hver del er opdelt i nummererede kapitler, som igen er delt i nummererede afsnit. En henvisning til (3.15) er altså til afsnit 15 i kapitel 3 i den del, hvor henvisningen står. De få krydshenvisninger til andre dele af noterne foregår typisk ved at referere til resultatet ved navn.

Matematisk Institut, den 1. februar 1997

I nærværende 2. udgave er der foretaget et antal mindre rettelser. Herefter er noterne fejlfrie.

Matematisk Institut, den 1. november 1998

I nærværende 2. oplag af 2. udgave er der foretaget et mindre antal mindre rettelser. Noterne er stadig fejlfrie.

Matematisk Afdeling, den 1. juli 2003

I nærværende 4. oplag af 2. udgave er der foretaget et mindre antal mindre rettelser og tilføjelser. Noterne er stadig fejlfrie.

Matematisk Afdeling, den 9. januar 2006

I denne (tredie) udgave er der foretaget en række ændringer og tilføjelser. Der kan have indsneget sig en enkelt fejl i forløbet.

Matematisk Afdeling, den 9. januar 2007
Anders Thorup

Indhold

Tallene

1. Regnereglerne.

(1.1) Indledning. Tallene spiller den helt centrale rolle i al matematik. De er grundlaget i de fleste matematiske discipliner, og de er uundværlige i anvendelser af matematik i forklaringen og forståelsen af vores omverden. Vi kan addere og multiplicere tal, vi kan sammenligne dem, vi kan producere nye tal ved grænseovergang, fx som integraler, osv. Kort sagt, vi kan regne med dem.

Et tilbageblik på et skoleforløb fortæller lidt om udviklingen af vores forståelse af tallene: først kommer de naturlige tal med sum og produkt, så kommer differens med nul og negative tal (altså de hele tal), så kommer division og brøker (altså de rationale tal), og til sidst kommer irrationale tal (og dermed de reelle tal). Det skal understreges, at forløbet ikke er parallelt med den historiske udvikling. I langt de fleste kulturer er forståelsen af nul og negative tal kommet sidst i udviklingen.

Når vi manipulerer med tallene benytter vi en række regler. De simpleste kan sammenfattes i følgende regneregler, som er velkendte (måske bortset fra navnene knyttet til de enkelte regler):

$$\textit{kommutativitet:}\quad x + y = y + x, \tag{a0}$$
$$\textit{associativitet:}\quad x + (y + z) = (x + y) + z, \tag{a1}$$
$$\textit{neutralt element:}\quad x + 0 = 0 + x = x, \tag{a2}$$
$$\textit{inverst element:}\quad x + (-x) = (-x) + x = 0, \tag{a3}$$
$$\textit{kommutativitet:}\quad xy = yx, \tag{m0}$$
$$\textit{associativitet:}\quad x(yz) = (xy)z, \tag{m1}$$
$$\textit{neutralt element:}\quad x1 = 1x = x, \tag{m2}$$
$$\textit{inverst element:}\quad xx^{-1} = x^{-1}x = 1, \quad \text{når } x \neq 0, \tag{m3}$$
$$\textit{totalitet:}\quad x = y \text{ eller } x < y \text{ eller } y < x, \tag{o0}$$
$$\textit{irrefleksivitet:}\quad x \not< x, \tag{o1}$$
$$\textit{transitivitet:}\quad \text{hvis } x < y \text{ og } y < z,\ \text{ så er } x < z, \tag{o2}$$
$$\textit{distributivitet:}\quad x(y + z) = xy + xz, \quad (x + y)z = xz + yz, \tag{am}$$
$$\textit{harmoni:}\quad \text{hvis } x < y,\ \text{ så er } x + z < y + z, \tag{ao}$$
$$\textit{harmoni:}\quad \text{hvis } x < y \text{ og } 0 < z,\ \text{ så er } xz < yz. \tag{mo}$$

Der er skam mange flere, men de regler, der udelukkende udtrykker egenskaber ved addition, multiplikation og ordning af de reelle tal, kan udledes af disse simple regler. Fundamental for udviklingen af grænseværdibegrebet, altså for hele den matematiske analyse, er følgende egenskab ved de reelle tal:

Enhver ikke-tom, opad begrænset mængde af reelle tal har et supremum.

Vi tager her som udgangspunkt de simple regneregler. Vi kommenterer de enkelte regler, og deres navne, og vi udleder en række velkendte konsekvenser. I de følgende kapitler ser vi nærmere på de naturlige, de hele, de rationale, og de komplekse tal.

(1.2) Additionen. Reglerne (a0)–(a3) omhandler *addition*. Addition er en *komposition* af tal, dvs en afbildning, der til hvert par af tal (x, y) knytter et nyt tal. Addition afbilder parret (x, y) i *summen* $x + y$. Reglen (a0) er den *kommutative lov*. Vi kan tale om summen af to tal x og y uden at specificere, hvilket af tallene der er det første og hvilket der er det andet.

Reglen (a1) er den *associative lov*. Vi kan tale om summen $x + y + z$ af tre tal x, y og z, uden at specificere i hvilken rækkefølge additionerne foretages. Det er klart, hvorledes vi for et sæt $(x_1, \dots, x_n)$ af n tal kan definere summen $\sum_{i=1}^{n} x_i = x_1 + \dots + x_n$. Den kommutative lov tillader os at tale om summen af n tal uden at vi specificerer rækkefølgen.

Reglen (a2) udsiger, at det specielle tal 0 (kaldet „nul“) har en speciel egenskab: det er neutralt element for addition i den forstand, at ligningerne i (a2) gælder, altså at et vilkårligt tal x ikke ændres ved addition af 0. Den første ligning i (a2) er naturligvis en konsekvens af den kommutative lov. Tallet 0 er i øvrigt det eneste tal, der har denne specielle egenskab. Antager man nemlig om et tal a, at $x = x + a$ for alle tal x, så får man jo specielt $0 = 0 + a = a$.

I reglen (a3) indgår tallet $-x$, der kaldes det *modsatte* til x. For to tal x og y defineres *differensen*,

$$x - y := x + (-y),$$

som summen af x og det modsatte til y. Af (a1), (a2) og (a3) får vi $(y + x) + (-x) = y + (x + (-x)) = y + 0 = y$, altså

$$(y + x) + (-x) = y. \tag{1.2.1}$$

I denne forstand er $-x$ *invers* til x: Tallet y ændres ikke, hvis man først adderer x og dernæst $-x$. Reglen (1.2.1) bruges i forbindelse med ligninger: De to ligninger,

$$a + x = b, \quad x = b - a,$$

er ensbetydende. Ved addition af $-a$ på begge sider af den første ligning fremkommer nemlig den anden, og ved addition af a på begge sider af den anden ligning fremkommer den første. Det er let at udlede følgende regler for modsat element:

$$-(-x) = x, \quad -(a + b) = -a - b, \quad -(a - b) = -a + b. \tag{1.2.2}$$

Med en sprogbrug, som vi senere vil se nærmere på, udsiger reglerne, at de reelle tal med addition udgør en *kommutativ gruppe*.

(1.3) Multiplikationen. Reglerne (m0)–(m3) omhandler *multiplikation*, som er endnu en komposition af tallene. Multiplikation knytter til hvert par af tal (x, y) *produktet* $x \cdot y$, der sædvanligvis skrives xy. Bemærk, at reglerne for multiplikation er analoge til reglerne for addition med én undtagelse: tallet x^{-1}, der kaldes det *reciprokke* til x, er kun defineret, når $x \neq 0$. *Kvotienten* er produktet $y/x := yx^{-1}$.

Det er en konsekvens af nul-reglen, som kommenteres nedenfor, at hvis to tal x, y er forskellige fra 0, så er også produktet xy forskelligt fra 0. Det følger specielt, at multiplikationen kan opfattes som en komposition i mængden af tal forskellige fra 0, og i denne talmængde er reglerne for multiplikation helt analoge til reglerne for addition. Tallene forskellige fra 0 udgør altså en kommutativ gruppe.

(1.4) Ordningen. Reglerne (o0), (o1) og (o2) omhandler *ordningen*. Ordningen er en *relation* blandt tallene. Skrivemåden $x < y$ udtrykker, at x er *mindre end* y eller at y er *større end* x; alternativt kan der skrives $y > x$. De *positive tal* og de *negative tal* er, henholdsvis, tallene større end 0 og mindre end 0. Reglen (o0) udsiger, at ordningen er *total:* hvilkesomhelst to tal kan sammenlignes. Specielt er altså hvert tal forskelligt fra 0 enten positivt eller negativt. Reglen (o1) fastlægger, at relationen er den „skarpe“ ulighed. Den tilsvarende bløde ulighed, $x \leqslant y$, betyder, at enten er $x = y$ eller $x < y$. For den bløde ulighed gælder:

$$\textit{refleksivitet:}\ x \leqslant x.$$

Bemærk, at *irrefleksiviteten* for ‘$<$’ i (o1) er den modsatte yderlighed af *refleksiviteten* for ‘$\leqslant$’. Egenskaben (o2) for relationen ‘$<$’ kaldes den *transitive* egenskab. Det er let at se, at også den bløde ulighed er transitiv,

$$x \leqslant y \text{ og } y \leqslant z \implies x \leqslant z.$$

(1.5) Den distributive lov. Reglen (am), der kaldes den *distributive lov*, udtrykker en sammenhæng mellem addition og multiplikation. Mere præcist siges multiplikationen at være *distributiv* mht additionen. Det er umiddelbart at udstrække loven til en regel for multiplikation af et tal med en sum af flere end to tal. Fx er

$$x(y_1 + y_2 + y_3) = x(y_1 + y_2) + xy_3 = xy_1 + xy_2 + xy_3,$$

og generelt, for en sum af n tal,

$$x(y_1 + \cdots + y_n) = xy_1 + \cdots + xy_n. \tag{1.5.1}$$

Antag her, at x er en sum af p tal, $x = x_1 + \cdots + x_p$. Gentagen anvendelse af (1.5.1) giver så ligningen,

$$(x_1 + \cdots + x_p)(y_1 + \cdots + y_n) = \sum x_i y_j,$$

eller, med ord: *Et produkt af summer er lig med summen af alle produkter, der som faktorer har et led fra hver af summerne.*

Mere generelt får vi for et produkt af et endeligt antal summer, at

$$\Big(\sum a_i\Big)\Big(\sum b_j\Big)\cdots\Big(\sum z_l\Big) = \sum a_i b_j \cdots z_l\,. \tag{1.5.2}$$

Af den distributive lov (og egenskaberne ved addition) følger, at

$$0 \cdot y = 0, \qquad (-x)y = -(xy), \quad \text{specielt: } (-1)y = -y. \tag{1.5.3}$$

Vi har nemlig $0 \cdot y + 0 \cdot y = (0 + 0) \cdot y = 0 \cdot y$, og heraf følger, efter addition af $-(0 \cdot y)$, at $0 \cdot y = 0$. Nu fås videre, at $xy + (-x)y = (x + (-x))y = 0 \cdot y = 0$, og heraf ses, at $-(xy) = (-x)y$. Endelig følger den sidste ligning i (1.5.3) af den midterste for $x := 1$, idet $1 \cdot y = y$.

(1.6) Eksempel. For hvert naturligt tal n gælder *binomialformlen*,

$$(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$

Formlens venstreside er nemlig et produkt af n summer (n parenteser),

$$(x + y)^n = (x + y)(x + y)\cdots(x + y).$$

Ifølge den distributive lov (1.5.2) er $(x + y)^n$ altså summen af alle produkter med n faktorer, der kan dannes ved at udvælge én faktor fra hver parentes. Der er kun to mulige faktorer, nemlig x og y, så hvert sådant produkt har formen $x^i y^{n-i}$. Mere præcist ses det, at produktet $x^i y^{n-i}$ fremkommer, når der fra i af parenteserne vælges x og fra de øvrige $n - i$ parenteser vælges y. Antallet af måder, hvorpå i parenteser kan udvælges af de n parenteser, er netop binomialkoefficienten $\binom{n}{i}$. Derfor gælder formlen.

(1.7) Harmoni. Den distributive lov (am) udtrykker en harmoni mellem addition og multiplikation. Tilsvarende udtrykker de to sidste regler (ao) og (mo) en harmoni mellem addition og ordning og mellem multiplikation og ordning: ordning bevares, når man adderer samme tal på begge sider af en ulighed, eller når man multiplicerer med samme positive tal. Heraf følger for eksempel, at ulighederne,

$$x < y, \qquad 0 < y - x,$$

er ensbetydende. Ved addition af $-x$ på begge sider af den første ulighed fremkommer nemlig den anden, og ved addition af x på begge sider af den anden ulighed fremkommer den første. Det følger også, at tallet x er positivt, hvis og kun hvis $-x$ er negativt.

Videre følger det, at multiplikation med negative tal „vender uligheden“:

$$x < y \text{ og } z < 0 \implies zx > zy.$$

Det følger specielt af reglerne, at produktet af to positive tal er positivt, at produktet af et positivt tal og et negativt tal er negativt, og at produktet af to negative tal er positivt. Specielt ses, at produktet af to tal, som begge er forskellige fra 0, er forskelligt fra 0.

(1.8) Nul-reglen. Af den distributive lov og harmonien mellem multiplikation og ordning følger *nul-reglen*,

$$xy = 0 \iff x = 0 \text{ eller } y = 0, \tag{1.8.1}$$

eller, ækvivalent,

$$xy \neq 0 \iff x \neq 0 \text{ og } y \neq 0. \tag{1.8.2}$$

Vi har nemlig $0 \cdot y = 0$ ifølge den første ligning i (1.5.3) og tilsvarende, eller ved brug af den kommutative lov, fås $x \cdot 0 = 0$. Altså gælder implikationen fra højre mod venstre i (1.8.1). Omvendt så vi i (1.7), at et produkt af to tal forskellige fra 0 er forskelligt fra 0. Hvis $xy = 0$, må en af faktorerne altså være 0.

(1.9) Numerisk værdi. Endelig minder vi om, at den *numeriske værdi* af x, betegnet $|x|$, kan defineres som det største af tallene x og $-x$. Herom gælder:

$$|-x| = |x|, \tag{n1}$$

$$|x| \geqslant 0, \text{ og } |x| = 0 \text{ kun når } x = 0. \tag{n2}$$

Ligningen (n1) følger nemlig af definitionen, da $-(-x) = x$. For $x = 0$ har vi $x = -x = 0$, og altså $|0| = 0$. For $x \neq 0$ er et af tallene x og $-x$ positivt og det andet er negativt. Det største af tallene x og $-x$ er derfor positivt. Altså gælder (n2).

For tal x og y gælder specielt $x \leqslant |x|$ og $y \leqslant |y|$. Ved gentagen addition ses, at $x + y \leqslant x + |y| \leqslant |x| + |y|$. Altså er $x + y \leqslant |x| + |y|$. Tilsvarende er $-x - y \leqslant |x| + |y|$. De to tal, $x + y$ og $-(x + y)$, er altså mindre end eller lig med $|x| + |y|$. Og så er også det største af de to tal mindre end eller lig med $|x| + |y|$. Men det betyder netop, at der gælder følgende ulighed:

$$|x + y| \leqslant |x| + |y|. \tag{n3}$$

Endelig noterer vi ligningen,

$$|xy| = |x|\,|y|\,. \tag{n4}$$

Da $-(xy) = (-x)y$ følger det nemlig af (n1), at de to sider af ligningen ikke ændres, hvis x erstattes med $-x$. For at bevise (n4) kan vi derfor antage, at $x \geqslant 0$. Tilsvarende kan vi antage, at $y \geqslant 0$. Men så er også $xy \geqslant 0$, og begge sider af (n4) er lig med xy. Altså gælder (n4).

(1.10) Opgaver.

1. Angiv supremum for mængden af de reelle tal a for hvilke $a^2 < 2$.

2. I et produkt af 4 tal kan parenteserne sættes på 5 måder. Den associative lov sikrer at produkterne er ens: $a(b(cd)) = a((bc)d) = (ab)(cd) = ((ab)c)d = (a(bc))d$. På hvor mange måder kan man sætte parenteser i et produkt af 5 tal? 6 tal? n tal? (Svaret på det sidste spørgsmål er $\binom{2n-1}{n}/(2n-1)$, men det er ikke så let at bevise!)

3. Vis, at $||a| - |b|| \leqslant |a - b|$.

4. Vis „trinomialformlen" $(x + y + z)^n = \sum_{i+j+k=n} \binom{n}{i,j,k} x^i y^j z^k$, hvor trinomialkoefficienten er antallet af måder . . . . Bestem et regneudtryk for dette antal.

2. Naturlige tal.

(2.1) Indledning. Mængden $\mathbb{N}$ af *naturlige tal* består af tallene,

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \dots,$$

altså de tal, man kan „tælle til". Sum og produkt af naturlige tal er igen naturlige tal, og for systemet af naturlige tal gælder de regneregler, som ikke omhandler tallet nul, modsat element, eller reciprokt element, altså reglerne,

$$\begin{gathered} x+y=y+x, \quad x+(y+z)=(x+y)+z, \\ xy=yx, \quad x(yz)=(xy)z, \quad 1x=x, \\ x=y \text{ eller } x<y \text{ eller } y<x, \quad x \not< x, \quad x<y \text{ og } y<z \implies x<z, \\ x(y+z)=xy+xz, \\ x<y \implies x+z<y+z, \quad x<y \implies xz<yz, \\ x<x+1. \end{gathered}$$

Den sidste regel følger naturligvis af de almindelige regneregler for tallene; vi har medtaget den her, da den ikke er en konsekvens af de foregående regler.

Fra et matematisk synspunkt er beskrivelsen af de naturlige tal ganske ynkelig. Vi kan ikke bruge den til at afgøre, om et givet tal er naturligt eller ikke. Betragt for eksempel tallet,

$$10^{120},$$

altså produktet $10 \cdot 10 \cdot 10 \cdots$ med 120 faktorer. Vores regneregler siger, at tallet er et naturligt tal. Men kan man tælle til 10^{120}? Det er en god tommelfingerregel, at makrokosmos måles i enheder af en størrelsesorden på 10^{50}, mikrokosmos i enheder af størrelsen 10^{-50}. Ifølge denne regel er der højst 10^{50} atomer i en kop vand, og der medgår højst 10^{50} kopper vand til at fylde universet. Antallet af atomer i universet er altså højst 10^{100}. Ifølge samme regel er universets diameter højst $10^{50}m$. Hvis vi anslår, at universet udvider sig mindst $1\,m/s$, så er universets alder altså højst 10^{50} sekunder.

Disse størrelser er naturligvis anslåede, men konklusionen er klar: det er ikke muligt at tælle til 10^{120}.

På trods af, at vi alle har en intuitiv forståelse af hvad de naturlige tal er, må vi acceptere, at det faktisk ikke er så nemt at definere mængden $\mathbb{N}$ af naturlige tal. I det følgende antager vi alligevel, at vi ved hvad vi taler om, når vi præciserer nogle yderligere (velkendte) egenskaber ved de naturlige tal.

(2.2) Velordningsprincip for naturlige tal. *Lad der være givet en ikke-tom mængde M af naturlige tal. Da findes et mindste tal i M, dvs der eksisterer et tal m_0 i M således, at $m_0 \leqslant m$ for alle tal m i M.*

Bevis. Dette er en velkendt egenskab ved systemet af naturlige tal. $\square$

(2.3) Eksempel. Et naturligt tal p kaldes som bekendt et *primtal*, hvis $p > 1$ og p kun har trivielle divisorer (dvs hvis de eneste positive divisorer i p er 1 og p). De naturlige tal større end 1, som ikke er primtal, er de *sammensatte* tal, dvs tal af formen kd, hvor k og d er større end 1.

Ethvert naturligt tal $n > 1$ har en *primdivisor*, dvs der findes et primtal p, der er divisor i n. Hertil bemærkes først, at der i n findes divisorer $d > 1$, idet fx $d = n$ er en sådan divisor. Lad nu p være det mindste blandt de tal, som er divisor i n og er større end 1. Tallet p er et primtal. I modsat fald ville p nemlig have en divisor d med $1 < d < p$. Da $d \mid p$ og $p \mid n$, er d divisor i n, og så er ulighederne $1 < d < p$ i modstrid med valget af p. Bemærk, at det var Velordningsprincippet, der sikrede, at vi overhovedet kunne tale om „det mindste blandt de tal, som … “.

(2.4) Induktionsprincippet. *Lad der være givet et udsagn $\wp(n)$ om naturlige tal n. Antag, at $\wp(1)$ er sandt. Antag videre, at for ethvert naturligt tal n gælder udsagnet,*

$$\wp(n) \implies \wp(n+1). \tag{2.4.1}$$

Da gælder udsagnet $\wp(n)$ for alle naturlige tal n.

Bevis. Ifølge forudsætningen gælder $\wp(1)$. Af (2.4.1) anvendt på $n = 1$ følger nu, at der gælder $\wp(2)$. Af (2.4.1) anvendt på $n = 2$ følger videre, at der gælder $\wp(3)$. Altså gælder

$$\wp(1), \wp(2), \wp(3), \dots,$$

dvs udsagnet $\wp(n)$ gælder for alle naturlige tal n. □

(2.5) Note. En række „indlysende“ påstande om naturlige tal følger ikke alene af reglerne i (2.1), men kan vises ved induktion. Eksempler er følgende:

$$1 \leqslant n, \qquad k < n+1 \iff k \leqslant n, \qquad n \neq 1 \implies n = k+1.$$

Det første påstand udsiger, at 1 er det mindste naturlige tal, og den mellemste udsiger, at tallet $n + 1$ er *efterfølgeren* af n. I den sidste påstand, at $n \neq 1$ har formen $n = k + 1$, er k *forgængeren* af n, naturligt betegnet $n - 1$. Med denne notation kan forudsætningen i Induktionsprincippet – at udsagnet (2.4.1) gælder for *alle* n – erstattes med, at følgende udsagn gælder for alle $n \neq 1$:

$$\wp(n-1) \implies \wp(n). \tag{2.5.1}$$

(2.6) Eksempel. For alle naturlige tal n gælder formlen,

$$1^2 + 2^2 + \cdots + n^2 = n(n+1)(2n+1)/6. \tag{2.6.1}$$

Vi viser påstanden ved induktion. Lad $\wp(n)$, for et naturligt tal n, betegne udsagnet, at ligningen (2.6.1) gælder. Lad S_n være summen på venstresiden af (2.6.1). For $n = 1$ er $S_1 = 1^2 = 1$, og højresiden er $1 \cdot 2 \cdot 3/6 = 1$. Altså gælder $\wp(1)$. I induktionsskridtet antages, at $n > 1$ og at $\wp(n-1)$ gælder. Vi har altså $S_{n-1} = (n-1)n(2n-1)/6$. Det skal bevises, at $\wp(n)$ gælder. Vi får

$$S_n = S_{n-1} + n^2 = \frac{(n-1)n(2n-1)}{6} + n^2 = \frac{n(n+1)(2n+1)}{6},$$

idet det sidste lighedstegn følger af udregningen,

$$(n-1)n(2n-1) + 6n^2 = n(2n^2 - 3n + 1 + 6n) = n(n+1)(2n+1).$$

Følgelig gælder $\wp(n)$.

(2.7) Princippet om fuldstændig induktion. *Lad der være givet et udsagn $\wp(n)$ om tal $n \in \mathbb{N}$. Antag, at $\wp(1)$ er sandt. Antag videre, at for alle $n \in \mathbb{N}$ gælder udsagnet,*

$$(\wp(k) \text{ for alle } k \leqslant n) \implies \wp(n+1). \tag{2.7.1}$$

Da gælder udsagnet $\wp(n)$ for alle naturlige tal n.

Bevis. Ifølge antagelsen gælder $\wp(1)$. Af (2.7.1) følger så, at $\wp(2)$ er sandt. Altså gælder $\wp(1)$ og $\wp(2)$, og nu følger af (2.7.1), at $\wp(3)$ er sandt. Altså gælder $\wp(1)$, $\wp(2)$, $\wp(3)$, og nu følger af (2.7.1), at $\wp(4)$ er sandt. Ved at fortsætte således indses, for ethvert naturligt tal n, at $\wp(n)$ er sandt. □

(2.8) Note. (1) Forudsætningen i Princippet om fuldstændig induktion – at (2.7.1) gælder for alle n – erstattes ofte med, at der for alle n gælder udsagnet,

$$(\wp(k) \text{ for alle } k < n) \implies \wp(n). \tag{2.8.1}$$

Bemærk, at udsagnet (2.8.1) for $n = 1$ faktisk medfører, at $\wp(1)$ er sandt. For $n = 1$ findes der jo ingen naturlige tal k således, at $k < n$. Venstresiden i (2.8.1) er altså sand for $n = 1$, og (2.8.1) medfører derfor, at $\wp(1)$ er sandt. [Men det føles jo næsten som snyd!]

(2) Bemærk forskellen mellem de to principper: Et induktionsbevis for et udsagn $\wp(n)$ består typisk af to dele. Den første er et bevis for at $\wp(1)$ er sandt (og dette bevis er typisk ganske trivielt). Den anden del går ud på at bevise, for $n > 1$, at $\wp(n)$ er sandt. Ved simpel induktion kan det i denne anden del antages, at $\wp(n-1)$ er sandt. Ved fuldstændig induktion kan det antages, at $\wp(k)$ er sandt for alle $k < n$. I denne forstand er Princippet om fuldstændig induktion et stærkere værktøj: ved beviset for at $\wp(n)$ er sandt har vi flere antagelser, hvilket (måske) gør beviset lettere.

(2.9) Eksempel. Ethvert naturligt tal $n > 1$ har en *primopløsning*, dvs der findes en fremstilling, $n = p_1 \cdots p_s$, af n som et produkt af primtal p_i. Her opfattes naturligt, når n selv er et primtal p, ligningen $n = p$ som en fremstilling af n som et produkt med én faktor. Påstanden, 'enten er $n = 1$ eller n er et produkt af primtal', vises ved fuldstændig induktion. Påstanden er trivielt sand for $n = 1$. I induktionsskridtet antages, at $n > 1$ og at påstanden er sand for alle $k < n$. Det skal vises, at påstanden gælder for n.

Hvis n er et primtal, er påstanden sand. Antag derfor, at n er sammensat, $n = kd$, hvor k og d er større end 1. Specielt er så både k og d mindre end n. Altså gælder påstanden for både k og d. Vi har derfor fremstillinger,

$$k = p_1 \cdots p_s, \quad d = q_1 \cdots q_t,$$

hvor tallene $p_1, \dots, p_s, q_1, \dots, q_t$ er primtal. Da $n = kd$ får vi fremstillingen,

$$n = kd = p_1 \cdots p_s \cdot q_1 \cdots q_t,$$

af n som produkt af primtal. Altså gælder påstanden for n.

(2.10) Note. Lad os igen kigge lidt på de tre principper. For Velordningsprincippet argumenterede vi bare med, at „det er jo velkendt". Hvor ved vi egentlig det fra? For Induktionsprincippet argumenterede vi ved at sætte tre prikker. Vi argumenterede for at $\wp(1)$ og $\wp(2)$ og $\wp(3)$ er sande. Vi kunne have fortsat med at argumentere for at $\wp(4)$ er sandt og for at $\wp(5)$ er sandt. Men uanset hvor længe vi fortsætter, må vi altid ende med tre prikker, eller „og så videre", eller „og så fremdeles", eller lignende. Hvordan kan vi påstå, at uendelig mange udsagn er sande, når vi kun kan vise endelig mange af dem? Tilsvarende argumenterede vi for Princippet om fuldstændig induktion ved at sige, at man kunne „fortsætte således"; men hvorfor gjorde vi ikke beviset færdigt?

Svaret på spørgsmålene er simpelt (men måske ikke helt tilfredsstillende): Det er nødvendigt i vores opbygning af matematik at *antage*, at de tre principper gælder; vi kan faktisk ikke bevise dem.

Man kan vise, at de tre principper følger af andre antagelser. Under forudsætning af de „indlysende" egenskaber i (2.5) kan man specielt vise, at det er nok at antage ét af principperne, idet man så kan bevise de to andre. Lad os fx vise, at Velordningsprincippet medfører Princippet om fuldstændig induktion. Betragt altså et udsagn $\wp(n)$, for hvilket (2.8.1) gælder for alle n. Lad S være mængden af de naturlige tal n, for hvilket udsagnet $\wp(n)$ er falsk. Vi skal vise, at S er den tomme mængde. Vi fører beviset indirekte, og antager at $S \neq \emptyset$. Ifølge Velordningsprincippet findes så et mindste tal n i S. Da n ligger i S er $\wp(n)$ falsk. Da n er det mindste tal i S, må der for ethvert naturligt tal $k < n$ gælde, at $k \notin S$, altså at $\wp(k)$ er sandt. Altså er forudsætningen på venstresiden af (2.8.1) opfyldt. Det følger derfor, at $\wp(n)$ er sandt. Hvilket er i modstrid med at vi lige indså, at $\wp(n)$ er falsk. Altså er den ønskede modstrid opnået.

(2.11) Bemærkning. Lad os afslutningsvis understrege, at Velordningsprincippet er et eksistensudsagn: Det påstår, at under givne forudsætninger eksisterer der et tal med visse egenskaber, men princippet udtaler sig ikke om hvordan vi bestemmer dette tal. Lad for eksempel n være tallet herunder,

$$403973053172146480004640109925029870946484075995819629605478298423496995260211882781424365195345494425377235497204137003.$$

Det har 120 cifre, og er altså et forholdsvis stort tal, jfr (2.1), men det er alligevel ikke større end at det (med lidt behændighed) kan stå på en enkelt linie. Det er en konsekvens af

Velordningsprincippet, jfr (2.3), at der eksisterer et primtal p, som er divisor i tallet n. Det er ikke svært at få en computer til at udføre regninger med tal af denne størrelsesorden, og der er metoder som ret let vil fastslå, at tallet n ikke selv er et primtal. I princippet kunne man lade en computer prøve med tallene $d = 1, 2, 3, \dots, 10^{60}$ om d er divisor i n. Men det er ikke en farbar vej i praksis (hvorfor ikke?), og det er min påstand, at ingen læsere af dette kapitel nogensinde† vil være i stand til at angive et sådant primtal p. Her undtages forfatteren, som bestemte n ved at multiplicere to primtal med 60 cifre.

(2.12) Opgaver.
1. Det er vel klart, at 1 er det mindste naturlige tal? Men uligheden $1 \leqslant n$ for alle $n \in \mathbb{N}$ er jo ikke nævnt blandt regnereglerne for naturlige tal. Kan du bevise uligheden?

2. Vis, alene ved brug af regnereglerne og Induktionsprincippet, følgende „indlysende“ påstande om naturlige tal: (1) $1 \leqslant n$. (2) $n < n + k$. (3) $n < m \Rightarrow \exists k : n + k = m$. (4) $n < m \Rightarrow n + 1 \leqslant m$.

3. For naturlige tal gælder, at $n < m \Rightarrow n + 1 \leqslant m$. Slut heraf, at Induktionsprincippet medfører Velordningsprincippet. [Vink: Antag, at $M \subseteq \mathbb{N}$ er ikke-tom. Lad $\wp(n)$ være udsagnet, at $n \leqslant m$ for alle $m \in M$. Vis, at $\wp(1)$ er sandt og at $\wp(n)$ ikke kan være sandt for alle n. Udled, at der findes et naturligt tal n_0 således, at $\wp(n_0)$ er sandt og $\wp(n_0 + 1)$ er falsk. Vis, at n_0 er det mindste tal i M.]

4. Mængden X har n elementer. Hvor mange elementer har potensmængden $\mathcal{P}(X)$, bestående af alle delmængder af X? Hvor mange delmængder af X har præcis k elementer?

5. Vis, at $1^3 + 2^3 + \cdots + n^3 = n^2(n + 1)^2/4$.

6. MK’erne bor i MK-land. Hver MK føder, når den er 20 år gammel, α nye MK’er. Hver MK dør, når den er 80 år gammel. Det vil altid være sådan, at der er flere levende MK’er end afdøde. Hvor stor mon α er?

7. Vis, at $n! > 2^n$ for $n \geqslant 4$.

8. Med $f^{(n)}$ betegnes den n’te afledede af funktionen f. Vis Leibniz’ formel for den n’te afledede af et produkt: $(fg)^{(n)}(t) = \sum_{i=0}^{n} \binom{n}{i} f^{(i)}(t) g^{(n-i)}(t)$.

9. Vis, at hvis $2^p - 1$ er et primtal, så må p være et primtal.

10. Angiv primopløsninger af tallene 10^{120}, 10!, og 542.097.

11. Angiv en afbildning $f : \mathbb{N} \to \mathbb{N}$, som er injektiv, men ikke surjektiv, og angiv en afbildning $g : \mathbb{N} \to \mathbb{N}$, som er surjektiv, men ikke injektiv.

12. Betragt for to afbildninger $f : X \to Y$ og $g : Y \to Z$ den sammensatte afbildning $g \circ f : X \to Z$. Vis: (1) Hvis f og g er injektive, så er $g \circ f$ injektiv. (2) Hvis $g \circ f$ er injektiv, så er f injektiv. (3) Hvis f og g er surjektive, så er $g \circ f$ surjektiv. (4) Hvis $g \circ f$ er surjektiv, så er g surjektiv.

---

†På initiativ af Jes Hansen blev n (ganske let) faktoriseret i april 2003 af en gruppe under NFSNET. Estimeret tidsforbrug: 10 dage på én computer med 1GHz CPU og 512 MB RAM.

13. Betragt to afbildninger $f\colon X \to Y$ og $g\colon Y \to X$. Vis, at hvis $g \circ f = \mathrm{id}_X$ og $f \circ g = \mathrm{id}_Y$, så er f bijektiv og $g = f^{-1}$.

14. Betragt en afbildning $f\colon X \to Y$, og delmængder $A, A' \subseteq X$ og $B, B' \subseteq Y$. (1) Vis, at $f^{-1}(B \cup B') = f^{-1}B \cup f^{-1}B'$, $f^{-1}(B \cap B') = f^{-1}B \cap f^{-1}B'$, og $f^{-1}(Y \setminus B) = X \setminus f^{-1}B$.

(2) Vis, at $f(A \cup A') = fA \cup fA'$ og $f(A \cap A') \subseteq fA \cap fA'$, og vis ved et eksempel, at inklusionen ikke altid er en lighed.

(3) Vis, at $A \subseteq f^{-1}(fA)$, og vis ved et eksempel, at inklusionen ikke altid er en lighed.

(4) Vis, at $f(f^{-1}B) \subseteq B$, og at inklusionen er en lighed, hvis $B \subseteq f(X)$; er inklusionen altid en lighed?

15. Sæt $a_n := \lfloor 10^{n-1}\pi/2 \rfloor \bmod 10^{100} + 1$ for $n = 1, 2, \dots$, hvor $\lfloor \alpha \rfloor$ betegner den hele del af det reelle tal α og $x \bmod d$ betegner den principale rest af x ved division med d. Vis, at $S := \{a_n \mid n \in \mathbb{N}\}$ er en begrænset delmængde af $\mathbb{N}$. Lad m være det mindste tal i S. Vis, at $1 \leqslant m \leqslant 2$. Kan du afgøre, hvilken af de to muligheder der indtræffer?

16. Vis, at $1^4 + 2^4 + \cdots + n^4 = n(6n^4 + 15n^3 + 10n^2 - 1)/30$.

17. Vis, at alle naturlige tal n er karakteriseret ved en interessant egenskab. [Vink: brug Velordningsprincippet.]

18. Hvordan viser man lettest formlen for en differensrække,

$$a + (a+d) + (a+2d) + \cdots + (a + (k-1)d) = \tfrac{1}{2}k\big(2a + (k-1)d\big).$$

Og for en kvotientrække,

$$a + aq + aq^2 + \cdots + aq^{k-1} = a(q^k - 1)/(q-1), \quad q \neq 1.$$

19. Vis, at tallene $10^{120} - 1$ og $10^{121} - 1$ ikke kan være primtal. Vis, at tallet $2^{125} - 1$ er deleligt med 31. Vis, at tallet $2^{125} + 1$ er deleligt med 33.

20. Er tallet 7.387 et primtal?

3. Hele tal.

(3.1) Indledning. Mængden $\mathbb{Z}$ af *hele tal* består af tallene,

$$\dots, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \dots,$$

altså af de naturlige tal, og tallet 0, og for hvert naturligt tal n det modsatte tal $-n$. Sum og produkt af hele tal er igen hele tal, og for systemet af hele tal gælder de simple regneregler, bortset fra eksistensen af reciprokke tal. Lad os gentage de simple regler med ord: Addition af hele tal er kommutativ og associativ, tallet 0 er neutralt element, og hvert helt tal x har det modsatte $-x$ som inverst med hensyn til addition; multiplikation af hele tal er kommutativ og associativ, og tallet 1 er neutralt element; relationen 'mindre end' er total, irrefleksiv og transitiv; multiplikation er distributiv mht addition, og addition og multiplikation harmonerer med ordningen 'mindre end'. (Prøv med dig selv, om du kan huske hvad alle de fine ord betyder.)

I det følgende minder vi om en række velkendte begreber i forbindelse med multiplikation af hele tal.

(3.2) Divisorer. Lad a være et helt tal. For et helt tal d siger vi som bekendt, at d er *divisor* i a, eller a er et *multiplum* af d, eller at d *går op* i a, og vi skriver $d \mid a$, hvis der findes et helt tal q således, at $a = qd$. Ifølge denne definition er ethvert helt tal d divisor i 0, idet $0 = 0 \cdot d$. Oftest er vi derfor interesserede i divisorer d i tal a, hvor $a \neq 0$.

Antag, at $a \neq 0$. Hvis $a = qd$, så er $a = (-q)(-d)$ og $-a = (-q)d$. Heraf ses, at d er divisor i a, hvis og kun hvis $-d$ er divisor i a og videre, at d er divisor i a, hvis og kun hvis d er divisor i $-a$. Ofte kan man derfor indskrænke sig til at betragte positive divisorer i positive tal.

For enhver divisor d i a gælder, at

$$|d| \leqslant |a|. \tag{3.2.1}$$

Antag nemlig, at $a = qd$. Da $a \neq 0$, er både q og d forskellige fra 0. Specielt er $|q| \geqslant 1$, og så er $|a| = |q|\,|d| \geqslant |d|$ ifølge regnereglerne.

Specielt er der kun endelig mange divisorer i a, og de positive divisorer i a skal søges blandt tallene $1, 2, \dots, |a|$.

Af ligningerne,

$$a = a \cdot 1 = (-a)(-1) = 1 \cdot a = (-1)(-a),$$

fremgår, at tallene ± 1 og $\pm a$ altid er divisorer i tallet a. Disse divisorer kaldes de *trivielle divisorer* i a. Der er kun 2 trivielle divisorer i 1, nemlig ± 1. Når $|a| > 1$, er der 4 trivielle divisorer i a.

Et *primtal* er som bekendt et tal $p > 1$, som kun har trivielle divisorer.

Ved en *fælles divisor* for to tal a, b forstås et tal, som er divisor i både a og b. Hvis for eksempel $b = 0$, så er de fælles divisorer øjensynlig netop divisorerne i a. Hvis et af tallene, fx a, er forskelligt fra 0, så skal de fælles divisorer søges blandt de endelig mange divisorer i a. Specielt er der så kun endelig mange fælles divisorer, og vi kan betragte den største af dem, den *største fælles divisor* for a, b. At tallet d er den største fælles divisor for a, b udtrykkes ved at skrive $d = (a, b)$.

Tallet 1 er altid en fælles divisor for a, b. Specielt er den største fælles divisor altid mindst lig med 1, altså altid positiv. Hvis tallet 1 er den største fælles divisor for a, b, siger vi, at a er *primisk* med b, eller at a og b er *primiske*. At a og b er primiske kan udtrykkes ved at skrive $(a, b) = 1$.

Den *største fælles divisor* for r tal $a_1, \dots, a_r$, hvor mindst ét af tallene er forskelligt fra nul, defineres tilsvarende som den største af de fælles divisorer, dvs som det største af de tal d, som går op i hvert af tallene a_i. At d er den største fælles divisor udtrykkes ved at skrive $d = (a_1, \dots, a_r)$. Tallene kaldes *primiske*, eller *indbyrdes primiske*, hvis $d = 1$ er den største fælles divisor. Det *mindste fælles multiplum* for tallene $a_1, \dots, a_r$ er det mindste af de positive tal m således, at m er et multiplum af hvert a_i.

At tallene $a_1, \dots, a_r$ er primiske må ikke forveksles med, at de er *parvis primiske*. Det sidste betyder, at $(a_i, a_j) = 1$ for alle $i \neq j$.

(3.3) Observation. Lad p være et primtal. Da er p primisk med tallet a, hvis og kun hvis p ikke går op i a. Den største fælles divisor for p og a skal nemlig søges blandt de positive divisorer i p. Den største fælles divisor må altså være enten 1 eller p. Det er klart, at den største fælles divisor er p, netop når p er divisor i a. Altså er den største fælles divisor lig med 1, netop når p ikke er divisor i a.

(3.4) Sætningen om division med rest. *Lad der være givet et tal $d \in \mathbb{N}$. Da findes for hvert helt tal a entydigt bestemte hele tal q og r således, at*

$$a = qd + r \text{ og } 0 \leqslant r < d. \tag{3.4.1}$$

Bevis. Betragt tallene af formen qd for $q \in \mathbb{Z}$. Da $d > 0$, er $qd < (q+1)d$. Vi har altså ulighederne,

$$\cdots < -3d < -2d < -d < 0 < d < 2d < 3d < \cdots .$$

Det er derfor klart, at hvert helt tal a ligger mellem to på hinanden følgende hele tal af formen qd eller, mere præcist, at der findes et entydigt bestemt helt tal q således, at vi har ulighederne,

$$qd \leqslant a < (q+1)d. \tag{3.4.2}$$

For et givet q kan vi naturligvis entydigt skrive $a = qd + r$ med et helt tal r, nemlig med $r = a - qd$. Det er klart, at de to uligheder i (3.4.2) er ensbetydende med de to uligheder for r i (3.4.1). Hermed er Sætningen om division med rest bevist. □

(3.5) Rester. Når $d \geqslant 1$ er givet, siges et tal af formen $r = a - qd$ også at være en *rest* af a ved division med d. Den entydige rest bestemt ved uligheden i (3.4.1) kaldes den *principale rest*. Den er øjensynlig bestemt som den mindste af de ikke-negative rester. Det er klart, at der også findes en *numerisk mindste rest* s bestemt ved betingelserne,

$$a = qd + s \text{ og } -\frac{d}{2} < s \leqslant \frac{d}{2}.$$

Når r er den principale rest, så er $s = r$ hvis $r \leqslant d/2$, og $s = r - d$, hvis $r > d/2$.

(3.6) Euklid's algoritme. Den største fælles divisor for a, b kan bestemmes ved en effektiv algoritme. Antag, at $a \geqslant b > 0$. Sæt $r_0 := a$ og $r_1 := b$. Anvend Sætningen om division med rest, med $d := r_1$, til at bestemme q_1 og r_2 således, at

$$r_0 = q_1 r_1 + r_2, \text{ med } 0 \leqslant r_2 < r_1.$$

Hvis $r_2 > 0$, anvendes igen Sætningen om division med rest, med $a := r_1$ og $d := r_2$. Induktivt, hvis r_{i-1} og r_i er bestemt, med $r_{i-1} > r_i > 0$, anvendes Sætningen om division med rest til at bestemme q_i og r_{i+1} således, at

$$r_{i-1} = q_i r_i + r_{i+1}, \text{ med } 0 \leqslant r_{i+1} < r_i. \tag{3.6.1}$$

Vi har så $r_0 \geqslant r_1 > r_2 > \cdots > r_i > r_{i+1} \geqslant 0$. Heraf ses, at algoritmen må stoppe ved at vi for et passende trin n har $r_n > r_{n+1} = 0$, altså

$$r_{n-1} = q_n r_n. \tag{3.6.2}$$

Det følger umiddelbart af ligningen (3.6.1), at et tal d går op i både r_{i-1} og r_i, hvis og kun hvis det går op i både r_i og r_{i+1}. For $i = 1, \dots, n$ gælder altså, at de fælles divisorer for r_{i-1}, r_i netop er de fælles divisorer for r_i, r_{i+1}. For $i = n$ er situationen simpel, idet $r_{n+1} = 0$. De fælles divisorer for r_n og r_{n+1} er derfor netop divisorerne i r_n. Altså gælder for alle $i = 1, \dots, n$, at de fælles divisorer for r_{i-1}, r_i netop er divisorerne i r_n.

For $i = 1$ slutter vi, at de fælles divisorer for a, b netop er divisorerne i r_n. Da $r_n > 0$, følger det specielt, at r_n er den største fælles divisor for a, b. Den sidste positive rest r_n, der fremkommer inden algoritmen stopper med resten $r_{n+1} = 0$, er altså den største fælles divisor for a, b.

(3.7) Sætning. *Lad a, b være hele tal, hvoraf mindst ét ikke er 0, og lad $d = (a, b)$ være den største fælles divisor. Da er de fælles divisorer for a, b netop divisorerne i d. Yderligere gælder, at der findes en fremstilling med hele tal x, y,*

$$d = xa + yb. \tag{3.7.1}$$

Bevis. Ved eventuelt at erstatte a med $-a$ og/eller b med $-b$ kan vi antage, at ingen af tallene a, b er negative. Yderligere kan vi ombytte a og b, så vi kan antage, at $a \geqslant b \geqslant 0$. Hvis $b = 0$, er de fælles divisorer netop divisorerne i a; specielt er a den største fælles divisor, og vi har fremstillingen $a = 1a + 0b$. Antag derfor, at $b > 0$. Da er antagelserne i Euklid's algoritme opfyldt. Algoritmen producerer derfor den største fælles divisor $d = r_n$, og som vi har set i (3.6) er de fælles divisorer for a, b netop divisorerne i d.

Yderligere kan vi få fremstillingen $d = xa + yb$ ved „tilbageregning“ i algoritmen. Det påstås, at vi for alle $i = 1, \dots, n$ har en fremstilling $d = x_i r_{i-1} + y_i r_i$ med hele tal x_i, y_i. For $i = n$ har vi nemlig fremstillingen $d = 0 r_{n-1} + 1 r_n$, og antages $d = x_{i+1} r_i + y_{i+1} r_{i+1}$, så får vi af (3.6.1),

$$d = x_{i+1} r_i + y_{i+1} r_{i+1} = x_{i+1} r_i + y_{i+1}(r_{i-1} - q_i r_i) = y_{i+1} r_{i-1} + (x_{i+1} - y_{i+1} q_i) r_i,$$

hvilket er en fremstilling af den ønskede form med $x_i := y_{i+1}$ og $y_i := x_{i+1} - y_{i+1} q_i$. For $i = 1$ får vi specielt den søgte fremstilling $d = x_1 r_0 + y_1 r_1 = x_1 a + y_1 b$. $\square$

(3.8) Eksempel. For $a = 1568$ og $b = 161$ giver Euklid's algoritme:

$$\begin{aligned} 1568 &= 9 \cdot 161 + 119, \\ 161 &= 1 \cdot 119 + 42, \\ 119 &= 2 \cdot 42 + 35, \\ 42 &= 1 \cdot 35 + 7, \\ 35 &= 5 \cdot 7. \end{aligned}$$

Tallet 7 er altså den største fælles divisor for 1568 og 161. Tilbageregning giver ligningerne,

$$\begin{aligned} 7 &= 42 - 1 \cdot 35 = 42 - (119{-}2 \cdot 42) = 3 \cdot 42 - 119 \\ &= 3(161{-}119) - 119 = 3 \cdot 161 - 4 \cdot 119 \\ &= 3 \cdot 161 - 4(1568 - 9 \cdot 161) = 39 \cdot 161 - 4 \cdot 1568. \end{aligned}$$

(3.9) Korollar. *To hele tal a, b er primiske, hvis og kun hvis der findes hele tal x og y således, at $1 = xa + yb$.*

Bevis. Hvis a og b er primiske, så er 1 den største fælles divisor for a og b, og fremstillingen $1 = xa + yb$ fås af Sætningen. Antag omvendt, at $1 = xa + yb$. Så vil ethvert tal d, som er divisor i a og b, også være divisor i 1. Altså er $d = \pm 1$. Følgelig er 1 den største fælles divisor, dvs a og b primiske. ▯

(3.10) Korollar. *Hvis a er primisk med b_1 og primisk med b_2, så er a primisk med produktet $b_1 b_2$.*

Bevis. Ifølge Korollar (3.9) findes fremstillinger $1 = x_1 a + y_1 b_1$ og $1 = x_2 a + y_2 b_2$. Heraf fås, at

$$1 = (x_1 a + y_1 b_1)(x_2 a + y_2 b_2) = (x_1 x_2 a + x_1 y_2 b_2 + y_1 b_1 x_2) a + (y_1 y_2) b_1 b_2.$$

Af Korollar (3.9) følger så, at a er primisk med $b_1 b_2$. ▯

(3.11) At gå op i et produkt. Lad n være et naturligt tal, og lad a, b være hele tal. Det er klart, at hvis n går op i a eller i b, så går n også op produktet ab. Det omvendte gælder ikke i almindelighed: Fx går 6 op i $3 \cdot 4$, men 6 går hverken op i 3 eller i 4. Eller simplere: 4 går op i $2 \cdot 2$, men 4 går ikke op i nogen af faktorerne (som begge er lig med 2).

Det er indholdet af det efterfølgende resultat, at det omvendte gælder, når $n = p$ er et primtal.

Det fundamentale Primtalslemma. *For et primtal p og hele tal a, b gælder:*

$$p \mid ab \implies p \mid a \text{ eller } p \mid b. \tag{3.11.1}$$

Bevis. Antag, at $p \mid ab$. Antag yderligere, at $p \nmid a$; det skal så vises, at $p \mid b$. Den største fælles divisor for p, a er specielt divisor i p, og må derfor være lig med enten 1 eller p. Da p

ikke er divisor i a, må den største fælles divisor altså være 1. Nu følger det af Korollar (3.9), at der findes hele tal x, y med $1 = xa + yp$. Følgelig gælder ligningerne:

$$b = 1b = (xa + yp)b = xab + ypb.$$

På højresiden er xab delelig med p ifølge antagelsen, og ypb er øjensynlig delelig med p. Derfor er højresiden delelig med p. Altså er b er delelig med p, som ønsket. □

Som nævnt er det klart, at hvis $p \,|\, a$ eller $p \,|\, b$, så vil $p \,|\, ab$. Implikationen i Primtalslemmaet kan altså erstattes af en biimplikation.

Resultatet kan også generaliseres: *Hvis primtallet p går op i et produkt $a_1 \cdots a_s$ med s faktorer, så går p op i en af faktorerne a_i.* Produktet kan nemlig skrives $(a_1 \cdots a_{s-1})a_s$. Af Det fundamentale Primtalslemma følger så, at p går op i $a_1 \cdots a_{s-1}$ eller i a_s. Hvis p går op i a_s, er det ønskede opnået. I modsat fald går p op i produktet $a_1 \cdots a_{s-1}$ med $s - 1$ faktorer; induktivt slutter vi så, at p går op i en af faktorerne $a_1, \dots, a_{s-1}$.

(3.12). I beviset for Det fundamentale Primtalslemma blev det kun benyttet, at p, a var primiske. Implikationen i (3.11.1) gælder altså, hvis det blot antages, at p og a er primiske. Faktisk giver en drejning af beviset det helt generelle resultat:

Sætning. *Lad a, b, n være hele tal, hvor $n \geqslant 1$. Lad d være den største fælles divisor for a, n. Da gælder:*

$$n \,|\, ab \iff \tfrac{n}{d} \,|\, b.$$

Specielt, hvis $n \,|\, ab$ og n er primisk med a, så vil $n \,|\, b$.

Bevis. „$\Rightarrow$“: Ifølge Sætning (3.7) findes hele tal x, y med $d = xa + yn$. Derfor gælder:

$$bd = (xa + yn)b = xab + ynb.$$

På højresiden er xab delelig med n ifølge antagelsen, og ynb er øjensynlig delelig med n. Derfor følger det af ligningerne, at bd er delelig med n. Altså er $bd = qn = q\frac{n}{d}d$ med et helt tal q. Da $d \neq 0$, følger det, at $b = q\frac{n}{d}$. Tallet b er derfor deleligt med $\frac{n}{d}$, som ønsket.

„$\Leftarrow$“: Af $d \,|\, a$ og $\frac{n}{d} \,|\, b$ følger, at produktet $n = d\frac{n}{d}$ er divisor i ab. □

(3.13) Korollar. *Antag, at $n = n_1 \cdots n_r$ er et produkt af parvis primiske naturlige tal n_i. Da gælder for alle hele tal a:*

$$n \,|\, a \iff n_i \,|\, a \text{ for } i = 1, \dots, r.$$

Bevis. Hvert n_i går op i n, så hvis n går op i a, vil også n_i gå op i a.

Den omvendte implikation vises ved induktion efter antallet, r, af faktorer n_i. For $r = 1$ er påstanden triviel. Antag, at $r > 1$, og at $n_i \,|\, a$ for $i = 1, \dots, r$. Induktivt følger det så, at produktet $n' := n_1 \cdots n_{r-1}$ er divisor i a. Vi har altså $a = n'b$ med et helt tal b. Ifølge antagelsen er n_r primisk med hvert af tallene $n_1, \dots, n_{r-1}$. Ved gentagen anvendelse af Korollar (3.10) følger, at n_r er primisk med n'. Desuden er n_r divisor i $a = n'b$. Af sætningen i (3.12) følger derfor, at n_r er divisor i b. Vi har altså $b = cn_r$ med et helt tal c. Heraf fås, at

$$a = n'b = n'n_rc = nc,$$

og det følger, at n er divisor i a. Hermed er de to implikationer bevist. □

(3.14) Note. Forudsætningen om at faktorerne er parvis primiske kan ikke undværes: Fx gælder for $n = 4 = 2 \cdot 2$, altså $n_1 = n_2 = 2$, at $n_1 \,|\, 2$ og $n_2 \,|\, 2$, men $4 \nmid 2$.

(3.15) Sætning (Euklid). *Der er uendelig mange primtal.*

Bevis. Vi viser, at for vilkårlige n givne primtal $p_1, \dots, p_n$ findes der et primtal p, der er forskelligt fra de givne. Hertil betragtes tallet,

$$N := p_1 \cdots p_n + 1.$$

Øjensynlig er $N > 1$. Følgelig findes et primtal p, som er divisor i N, jfr Eksempel (2.3). Det påstås, at primtallet p er forskelligt fra primtallene $p_1, \dots, p_n$. Antag nemlig, indirekte, at p er lig med et af p_i'erne. Da er p divisor i $p_1 \cdots p_n = N - 1$. Tallet p er altså divisor i $N - 1$ og i N. Følgelig er p også divisor i differensen $N - (N - 1) = 1$. Hermed er opnået en modstrid, idet tallet 1 har 1 som den eneste positive divisor. □

(3.16) Aritmetikkens Fundamentalsætning. *Ethvert helt tal $a > 1$ har en primopløsning, dvs der findes en fremstilling,*

$$a = p_1 \cdots p_s, \tag{3.16.1}$$

af a som et produkt af primtal p_i. Primopløsningen er entydig i den forstand, at hvis $a = q_1 \cdots q_t$ er endnu en primopløsning, så er $t = s$, og efter en passende omnummerering af q_j'erne er $q_i = p_i$ for $i = 1, \dots, s$.

Bevis. Eksistensen af fremstillingen blev bevist i Eksempel (2.9).

For at vise entydigheden af fremstillingen skal det vises, at hvis der er givet s primtal $p_1, \dots, p_s$ og t primtal $q_1, \dots, q_t$ og en ligning,

$$p_1 \cdots p_s = q_1 \cdots q_t, \tag{1}$$

så er $s = t$, og efter passende omnummerering af q_j'erne er $p_i = q_i$ for $i = 1, \dots, s$.

Denne påstand vises ved induktion efter s. For $s = 1$ er venstresiden i (1) det ene primtal p_1. Hvert q_j på højresiden er altså divisor i p_1. Da p_1 kun har trivielle divisorer og $q_j > 1$, slutter vi, at $t = 1$ og at ligningen er den trivielle: $p_1 = q_1$.

I induktionsskridtet antages, at $s > 1$ og at påstanden gælder for $s - 1$ primtal. Primtallet p_s er divisor i venstresiden af (1), og dermed i højresiden. Højresiden er et produkt af t faktorer. Det følger derfor af Det fundamentale Primtalslemma (3.11), at p_s går op i en af faktorerne q_j. Efter omnummerering af faktorerne q_j kan vi antage, at p_s går op i q_t. Da q_t er et primtal, har q_t kun trivielle divisorer. Da $p_s > 1$, slutter vi, at $p_s = q_t$. Af ligningen (1) følger derfor, at

$$p_1 \cdots p_{s-1} = q_1 \cdots q_{t-1}. \tag{2}$$

I ligningen (2) er venstresiden større end 1, da $s - 1 \geqslant 1$. Altså er også $t - 1 \geqslant 1$. Ligningen (2) har altså samme form som (1), blot med $s - 1$ primtal på venstresiden. Da påstanden er antaget at gælde for $s - 1$ primtal, følger det, at $s - 1 = t - 1$, og at vi efter omnummerering af faktorerne q_j har $q_j = p_j$ for $j = 1, \dots, t - 1$.

Hermed er også entydigheden bevist. □

(3.17) Primopløsninger. I primopløsningen (3.16.1) antages ikke, at primtallene p_i er forskellige. Hvis man i fremstillingen skriver primfaktorer, der forekommer flere gange, som potenser, får fremstillingen formen,

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \tag{3.17.1}$$

hvor $p_1, \dots, p_r$ er *forskellige* primtal. Fremstillingen (3.17.1) udtrykker, at i primopløsningen af a forekommer primtallet p_j som faktor α_j gange.

Bemærk, at vi i fremstillingen (3.17.1) kan tillade, at en eller flere af eksponenterne α_j er 0, idet jo $p^0 = 1$. Specielt kan vi, når vi betragter primopløsninger af endelig mange tal, antage, at det er de samme primtal p_j, der indgår i primopløsningerne. Videre kan vi formelt sige, at tallet 1 har primopløsningen $1 = p_1^0 \cdots p_r^0$. Entydighedsdelen af Fundamentalsætningen udsiger, at der af en ligning,

$$p_1^{\alpha_1} \cdots p_r^{\alpha_r} = p_1^{\beta_1} \cdots p_r^{\beta_r},$$

hvor $p_1, \dots, p_r$ er forskellige primtal, følger, at $\alpha_i = \beta_i$ for alle i.

Ud fra en primopløsning (3.17.1) kan vi bestemme de positive divisorer i a. Betragt nemlig to positive tal q og d, med primopløsninger,

$$q = p_1^{\nu_1} \cdots p_r^{\nu_r}, \qquad d = p_1^{\delta_1} \cdots p_r^{\delta_r}. \tag{3.17.2}$$

Heraf får vi primopløsningen,

$$qd = p_1^{\nu_1+\delta_1} \cdots p_r^{\nu_r+\delta_r}.$$

Altså gælder ligningen $a = qd$, hvis og kun hvis $\alpha_j = \nu_j + \delta_j$ for alle j. Heraf ses:

Tallet d er divisor i a, hvis og kun hvis der for eksponenterne i primopløsningerne gælder ulighederne $0 \leqslant \delta_j \leqslant \alpha_j$ for alle j.

Bemærk, at den trivielle divisor $d = 1$ i a svarer til eksponenterne $\delta_1 = \cdots = \delta_r = 0$ og den trivielle divisor $d = a$ svarer til eksponenterne $\delta_j = \alpha_j$ for alle j.

Specielt ses, at antallet af positive divisorer i a er bestemt som produktet,

$$(\alpha_1 + 1) \cdots (\alpha_r + 1).$$

Betragt endnu et tal $b > 0$, med primopløsningen,

$$b = p_1^{\beta_1} \cdots p_r^{\beta_r}.$$

Så er d en fælles divisor for a og b, hvis og kun hvis $\delta_j \leqslant \alpha_j$ og $\delta_j \leqslant \beta_j$ for alle j, altså hvis og kun hvis $\delta_j \leqslant \min\{\alpha_j, \beta_j\}$ for alle j. Det følger specielt, at den største fælles divisor for a og b er tallet,

$$p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_r^{\min\{\alpha_r,\beta_r\}}.$$

(3.18) Observation. For en primtalspotens $a = p^\alpha$ følger det, at de positive divisorer i a netop er potenserne p^δ for $0 \leqslant \delta \leqslant \alpha$.

Det tilsvarende gælder naturligvis ikke for en potens af et sammensat tal. For $a = 6^2 = 2^2 \cdot 3^2 = 36$ er $1, 6, 6^2$ divisorer, men desuden har vi divisorerne 2, 3, $2^2 = 4$, $3^2 = 9$, $2^2 \cdot 3 = 12$, og $2 \cdot 3^2 = 18$.

(3.19) Eksempel. Tallene 1568 og 161 har primopløsningerne $1568 = 2^5 \cdot 7^2$ og $161 = 7 \cdot 23$. Den største fælles divisor er derfor $d = 7$, jfr Eksempel (3.8).

(3.20) Note. *Eratosthenes' si* indeholder tal, hvoraf nogle er mærkede. At *ryste sien* betyder, at man mærker det mindste af de umærkede tal, og lader alle egentlige multipla af dette tal drysse ud af sien.

Fyld sien op med tallene større end 1, alle umærkede, altså med tallene,

$$2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,\dots$$

Ryst sien én gang. Herved mærkes det mindste, altså tallet 2, og alle de lige tal drysser ud af sien. Tilbage bliver:

$$\underline{2},3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47,49,51,53,55,57,59,\dots$$

Ryst igen. Herved mærkes det mindste af de umærkede, altså tallet 3, og alle andre tal delelige med 3 drysser ud af sien. Tilbage bliver:

$$\underline{2},\underline{3},5,7,11,13,17,19,23,25,29,31,35,37,41,43,47,49,53,55,59,61,65,67,71,73,77,79,83,85,89,91,\dots$$

Ryst igen. Tilbage bliver:

$$\underline{2},\underline{3},\underline{5},7,11,13,17,19,23,29,31,37,41,43,47,49,53,59,61,67,71,73,77,79,83,89,91,97,101,103,\dots$$

Rystes uendelig mange gange resterer netop primtallene i sien.

(3.21) Opgaver.

1. Er der et største negativt helt tal?

2. Bestem den principale rest af 1010 ved division med 7. Og af -1010.

3. I dag er det mandag. Hvilken ugedag er det om 1000 dage?

4. Er tallene 99, 100, og 101 parvis primiske? Hvilke tal mellem 1 og 100 er ikke primiske med 67?

5. Bestem den største fælles divisor for tallene 6901 og 5293.

6. Lad d være den største fælles divisor og m det mindste fælles multiplum for to naturlige tal a og b. Vis, at $dm = ab$.

7. Lad a og n være hele tal, hvoraf mindst et ikke er 0. Vis, at der findes positive tal i mængden $\mathbb{Z}a + \mathbb{Z}n := \{xa + yn \mid x, y \in \mathbb{Z}\}$, og vis, at det mindste af disse positive tal er den største fælles divisor for a, n. Du må bruge Sætningen om division med rest, og selve definitionen af største fælles divisor. Udled, at enhver fælles divisor for a, n er divisor i den største fælles divisor.

8. Lad $a_1, \dots, a_r$ være r hele tal, hvoraf mindst ét ikke er 0, og lad $d = (a_1, \dots, a_r)$ være den største fælles divisor. Vis, at de fælles divisorer for $a_1, \dots, a_r$ netop er divisorerne i d, og at der findes en fremstilling med hele tal $x_1, \dots, x_r$,

$$d = x_1 a_1 + \cdots + x_r a_r.$$

[Vis påstanden ved induktion efter $r \geqslant 1$. I induktionsskridtet inddrages med fordel den største fælles divisor for $a_1, \dots, a_{r-1}$, givet at et af disse tal ikke er 0.]

9. Antag, at $1 \leqslant i < n$ og at i og n er primiske. Vis, at $\binom{n}{i}$ er delelig med n. [Brug fx at $n\binom{n-1}{i-1} = i\binom{n}{i}$.]

10. Lad p være et primtal. Vis, at alle binomialkoefficienterne $\binom{p}{i}$ for $1 \leqslant i \leqslant p-1$ er delelige med p. Udnyt dette til at vise, ved induktion efter k, at p går op i $k^p - k$ (Fermat's lille Sætning).

11. Euklid's bevis for at der er uendelig mange primtal giver en uendelig følge af forskellige primtal: Vi sætter $p_1 := 2$ og (induktivt) lader vi p_{n+1} være den mindste primdivisor i $p_1 \cdots p_n + 1$. Så er p_2 den mindste primdivisor i $2 + 1 = 3$, altså $p_2 = 3$. Videre er p_3 den mindste primdivisor i $2{\cdot}3 + 1 = 7$, altså $p_3 = 7$, og p_4 er den mindste primdivisor i $2{\cdot}3{\cdot}7 + 1 = 43$, altså $p_4 = 43$. Vis, at $p_1 \cdots p_n + 1$ ikke altid selv er et primtal.

12. Tallene $1, 4, 9, 16, \dots$ er *kvadrattallene*. Vis, at hvis ab er et kvadrattal og a, b er primiske og positive, så er både a og b kvadrattal.

13. Hæld tallene $2, 3, 4, \dots, N$ i Eratosthenes' si og ryst 4 gange. Nu indeholder sien kun primtal. Hvor stor kunne N være?

14. Bestem den største fælles divisor for tallene 10^{120} og $10!$.

15. Vis, at der er uendelig mange primtal af formen $4d - 1$. [Vink: Vis, at for givne primtal $p_1, \dots, p_n$ har $4p_1 \cdots p_n - 1$ en primdivisor af formen $4d - 1$.]

16. Vis, for $n \geqslant 3$, at der er uendelig mange primtal p med $p \not\equiv 1 \pmod{n}$.

17. Lad a, n være to naturlige tal, og lad d være den største fælles divisor for a, n. Der findes da fremstillinger $d = xa - yn$ med hele tal x, y. Vis, at der er et entydigt valg af x, y således, at $1 \leqslant x \leqslant n/d$, og at der med dette valg gælder $0 \leqslant y < a/d$.

18. Et naturligt tal $p > 1$ har følgende egenskab: $p \,|\, ab \implies p \,|\, a$ eller $p \,|\, b$. Vis, at p er et primtal.

19. Antag for naturlige tal a, b, c, d, at $ab = cd$. Vis, at $a \,|\, c \iff d \,|\, b$.

20. (Alternativt bevis for Sætning (3.12)) Betragt for hele tal a, n med $n \geqslant 1$ mængden $Q := \{\, x \in \mathbb{Z} \mid n \,|\, ax \,\}$. Øjensynlig ligger det positive tal n i Q. Lad n_0 være det mindste positive tal i Q. Vis, at $1 \leqslant n_0 \leqslant n$. Vis, at $x \in Q \iff n_0 \,|\, x$, altså at der for alle hele tal x gælder:

$$n \,|\, ax \iff n_0 \,|\, a.$$

Vis, at $n_0 = n/d$, hvor $d = (n, a)$.

21. Lad a, n være to naturlige, primiske tal. Vis, at med $k_0 := an + 1$ gælder: hvert helt tal $k \geqslant k_0$ har en fremstilling $h = xa + yn$ med *positive* heltal x, y. Hvis man i fremstillingen blot kræver $x, y \geqslant 0$, gælder påstanden øjensynlig også for $k_0 := an$. Vis, at påstanden (med kravet $x, y \geqslant 0$) gælder for $k_0 := (a-1)(n-1)$.

22. Er det muligt at dele en terning i 1992 terninger (naturligvis ikke alle af samme størrelse)? [Kilde: Lettisk konkurrence — for 9. klasse!]

23. Når n er primopløst, $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$, er det let at bestemme antallet af (positive) divisorer i n: det er produktet $(\nu_1 + 1) \cdots (\nu_r + 1)$. Kan du finde en formel for summen $\sigma(n)$ af divisorerne i n?

24. Et tal n kaldes *fuldkomment*, hvis n er lig med summen af sine divisorer, fraregnet n selv, altså hvis $\sigma(n) = 2n$. Eksempler: $6 = 1 + 2 + 3$ og $28 = 1 + 2 + 4 + 7 + 14$. Vis (Euklid), at hvis $2^k - 1$ er et primtal, så er $n = 2^{k-1}(2^k - 1)$ fuldkomment. *Vis omvendt (Euler), at ethvert lige fuldkomment tal er af denne form. (Man ved ikke om der findes ulige fuldkomne tal.)

25. Lad $b > 1$ være et naturligt tal. Vis, at hvert naturligt tal n har en *fremstilling i b-talssystemet*,

$$n = d_k b^k + \cdots + d_1 b + d_0, \quad \text{hvor } 0 \leqslant d_i < b \text{ for } i = 0, \ldots, k,$$

entydig, hvis $d_k > 0$. [Vink: Vis, at hvis $d_k > 0$ i fremstillingen, så er $b^k \leqslant n < b^{k+1}$.]

4. Rationale tal.

(4.1) Indledning. Mængden $\mathbb{Q}$ af rationale tal består af alle *brøker*,

$$a/s, \quad \text{hvor } a \text{ og } s \text{ er hele tal og } s \neq 0.$$

Brøken a/s, der også skrives $\frac{a}{s}$, er produktet as^{-1} af tallet a og det reciprokke til s. De rationale tal omfatter de hele tal, idet tallet $a \in \mathbb{Z}$ er lig med brøken $a/1$.

Man kan *forlænge* en brøk: For hvert helt tal $t \neq 0$ gælder ligningen,

$$\frac{at}{st} = \frac{a}{s}\,, \tag{4.1.1}$$

thi ifølge regnereglerne er $(at)/(st) = (at)(st)^{-1} = att^{-1}s^{-1} = as^{-1} = a/s$.

Det skal understreges, at en brøk er et tal, der fremkommer som *resultatet* af et regnestykke; brøken er ikke selve regnestykket. Alligevel er det sædvane for en brøk a/s at kalde a for *tælleren* og s for *nævneren*. Ligningen (4.1.1) udtrykker, at brøken ikke ændres, når nævner og tæller multipliceres med samme tal. Tilsvarende kan en brøk b/u *forkortes*: hvis t går op i både b og u, så ændres brøken ikke, når tæller og nævner divideres med t.

Addition og multiplikation af rationale tal fører igen til rationale tal:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}\,, \tag{4.1.2}$$

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}\,. \tag{4.1.3}$$

Forlænger vi nemlig a/s med t og forlænger vi b/t med s, får vi $a/s = (at)/(st)$ og $b/t = (bs)/(st)$, og så er, ifølge regnereglerne,

$$\frac{a}{s} + \frac{b}{t} = (at)(st)^{-1} + (bs)(st)^{-1} = [at + bs](st)^{-1} = \frac{at + bs}{st}\,.$$

Af regnereglerne følger ligeledes, at

$$\frac{a}{s} \cdot \frac{b}{t} = as^{-1}bt^{-1} = (ab)s^{-1}t^{-1} = (ab)(st)^{-1} = \frac{ab}{st}\,.$$

Tallet 0 er brøken $0/1$, og altså også lig med brøken $0/s$ for $s \neq 0$. Heraf følger, at det modsatte tal til en brøk a/s er brøken $(-a)/s$,

$$-\frac{a}{s} = \frac{-a}{s}\,. \tag{4.1.4}$$

Tallet 1 er brøken $1/1$, og altså også lig med brøken s/s for $s \neq 0$. Heraf følger, at det reciprokke tal til en brøk $a/s \neq 0$ er brøken s/a,

$$\left(\frac{a}{s}\right)^{-1} = \frac{s}{a}\,, \ \text{når } a \neq 0.$$

Regninger med brøker fører altså igen til brøker. Følgelig gælder samtlige simple regneregler for de rationale tal.

(4.2) Observation. En brøk a/s kan forlænges med -1 til brøken $(-a)/(-s)$. Specielt følger det, at enhver brøk kan skrives på formen a/s, hvor nævneren er et positivt helt tal.

Enhver brøk a/s kan forkortes med en fælles divisor for a og s. Specielt fremkommer, når brøken forkortes med den største fælles divisor, en *uforkortelig brøk*, dvs en brøk, hvor tæller og nævner er primiske.

Er der givet r brøker $a_1/s_1, \dots, a_r/s_r$, kan man altid ved at forlænge opnå, at brøkerne har samme nævner. Fx kan den i'te brøk forlænges med produktet af de øvrige nævnere. Herved fremkommer som fælles nævner produktet $s_1 \cdots s_r$.

(4.3) Farey-brøker. For et givet naturligt tal N defineres *Farey-brøkerne* af orden N som brøkerne af formen a/s, hvor $1 \leqslant s \leqslant N$. I ethvert begrænset interval er der øjensynlig kun endelig mange Farey-brøker af orden N, og de kan derfor opskrives i en endelig følge, ordnet efter størrelse. Farey-brøkerne af orden 9 i intervallet $[0,1]$ er brøkerne,

$$0 = \tfrac{0}{1}\ \tfrac{1}{9}\ \tfrac{1}{8}\ \tfrac{1}{7}\ \tfrac{1}{6}\ \tfrac{1}{5}\ \tfrac{2}{9}\ \tfrac{1}{4}\ \tfrac{2}{7}\ \tfrac{1}{3}\ \tfrac{3}{8}\ \tfrac{2}{5}\ \tfrac{3}{7}\ \tfrac{4}{9}\ \tfrac{1}{2}\ \tfrac{5}{9}\ \tfrac{4}{7}\ \tfrac{3}{5}\ \tfrac{5}{8}\ \tfrac{2}{3}\ \tfrac{5}{7}\ \tfrac{3}{4}\ \tfrac{7}{9}\ \tfrac{4}{5}\ \tfrac{5}{6}\ \tfrac{6}{7}\ \tfrac{7}{8}\ \tfrac{8}{9}\ \tfrac{1}{1} = 1\,.$$

(4.4) Opgaver.

1. Vis, at tallet $\sqrt{2}$ er irrationalt, altså at der ikke findes et rationalt tal a/s således, at $(a/s)^2 = 2$.

2. Vis for en brøk a/s, at $a/s > 0$, hvis og kun hvis $as > 0$. Vis, at $a/s < b/t$, hvis og kun hvis $st^2a < s^2tb$.

3. Fibonacci's talfølge 0, 1, 1, 2, 3, 5, 8, 13, ... er bestemt ved $a_0 = 0$, $a_1 = 1$, og rekursivt, $a_{n+1} = a_{n-1} + a_n$. Vis for alle n, at a_n og a_{n+1} er primiske. Vis, at følgen af rationale tal a_n/a_{n+1} er konvergent, og bestem grænseværdien. Vis, at

$$a_n = \frac{1}{\sqrt{5}}\Big[\Big(\frac{1+\sqrt{5}}{2}\Big)^n - \Big(\frac{1-\sqrt{5}}{2}\Big)^n\Big].$$

4. *Betragt Farey-brøkerne af en given orden N, skrevet som uforkortelige brøker og ordnet efter størrelse. Hvis $a'/s' < a/s$ er to på hinanden følgende brøker, så er $s' + s > N$. Hvis $a'/s' < a/s$ er to på hinanden følgende brøker, så er $as' - a's = 1$. Hvis $a'/s' < a/s < a''/s''$ er tre på hinanden følgende brøker, så er $a/s = (a' + a'')/(s' + s'')$. Check disse påstande for følgen af Farey-brøker af orden 9. Farey formodede disse påstande, men kunne ikke bevise dem. Kan du?

5. Reelle og komplekse tal.

(5.1) Indledning. De reelle tal var grundlaget for den indledende gennemgang af de simple regneregler. Vi vil her ganske kort også minde om nogle begreber knyttet til systemet af komplekse tal. Der er ingen ordning af de komplekse tal, så de simple regler vedrørende ordning er meningsløse, når man udvider det reelle område; men regnereglerne for addition og multiplikation gælder også for komplekse tal.

(5.2) Komplekse tal. Mængden $\mathbb{C}$ af *komplekse tal* er mængden $\mathbb{R}^2$, af par (a, b) af reelle tal, organiseret med en addition og en multiplikation,

$$\begin{aligned}(a, b) + (c, d) &:= (a+c\ ,\ b+d),\\ (a, b) \cdot (c, d) &:= (ac-bd\ ,\ ad+bc).\end{aligned} \tag{5.2.1}$$

Addition af parrene er blot den velkendte vektoraddition i $\mathbb{R}^2$ opfattet som reelt vektorrum. Specielt er additionen kommutativ og associativ, parret $(0, 0)$ er neutralt element for addition, og for hvert par (a, b) er $-(a, b) = (-a, -b)$ det modsatte par mht addition. Det er ikke svært at vise, at multiplikationen er kommutativ, associativ, og distributiv mht additionen, og at parret $(1, 0)$ er neutralt element for multiplikation.

Afbildningen $a \mapsto (a, 0)$ er en injektiv afbildning $\mathbb{R} \to \mathbb{C}$, og den giver derfor en bijektiv forbindelse mellem de reelle tal a og de komplekse tal af formen $(a, 0)$. Via denne bijektive forbindelse opfattes de reelle tal som en delmængde af de komplekse tal. Vi identificerer altså det reelle tal a med det komplekse tal $(a, 0)$. Af ligningerne i (5.2.1) fremgår, for $b = d = 0$, at sædvanlig addition og multiplikation af to reelle tal a og c svarer til kompleks addition og multiplikation, når a og c opfattes som komplekse tal. Yderligere fremgår det, at multiplikation af det komplekse tal (c, d) med det reelle tal $(a, 0)$ svarer til at multiplicere vektoren (c, d) med skalaren a.

Bemærk, at de komplekse tal $(0, 0)$ og $(1, 0)$, som, henholdsvis, var neutralt element for addition og multiplikation i $\mathbb{C}$, under identifikationen svarer til de reelle tal 0 og 1.

Det komplekse tal $i := (0, 1)$ kaldes som bekendt den *imaginære enhed*. Tallene $1 = (1, 0)$ og $i = (0, 1)$ er den kanoniske basis for vektorrummet $\mathbb{R}^2$. Den entydige fremstilling,

$$(a, b) = a(1, 0) + b(0, 1),$$

af en vektor (a, b) i denne basis svarer altså til den entydige fremstilling af det komplekse tal $z = (a, b)$,

$$z = a + bi,$$

som en sum af et reelt tal og et reelt tal gange den imaginære enhed. Tallet a er som bekendt *realdelen* af z, og b er *imaginærdelen*.

(5.3) Modulus og konjugering. For et komplekst tal $z = a + ib$ defineres *modulus* eller den *numeriske værdi* (eller *normen*) som det reelle tal,

$$|z| := \sqrt{a^2 + b^2}.$$

Når z opfattes som vektoren (a, b) er modulus altså den sædvanlige (euklidiske) norm af vektoren. Øjensynlig er $|0| = 0$, og når $z \neq 0$ er $|z| > 0$.

Det *konjugerede* til z er det komplekse tal,

$$\overline{z} := a - bi.$$

Øjensynlig er $\overline{z} = z$ netop når $b = 0$, altså netop når z er et reelt tal. Det er let at vise formlerne,

$$\overline{\overline{z}} = z, \quad z\overline{z} = |z|^2, \quad \overline{z+w} = \overline{z} + \overline{w}, \quad \overline{zw} = \overline{z}\,\overline{w}.$$

Af den anden formel følger, at når $z \neq 0$, så er tallet,

$$z^{-1} := \frac{\overline{z}}{|z|^2} = \frac{a - ib}{a^2 + b^2},$$

inverst til z i den forstand, at $z^{-1}z = 1$. Hermed er specielt godtgjort, at de regneregler for reelle tal, der kun vedrører sum og produkt, også gælder for komplekse tal.

(5.4) Geometrisk beskrivelse. De komplekse tal svarer til vektorer i $\mathbb{R}^2$, og de kan derfor også beskrives som punkter i planen: det komplekse tal $z = a + bi$ svarer til punktet med sædvanlige retvinklede koordinater (a, b). Herved svarer de reelle tal til første-aksen, og de komplekse tal af formen $bi = (0, b)$ svarer til anden-aksen.

Modulus er afstanden fra 0, og konjugering svarer til spejling i den reelle akse.

Ethvert komplekst tal $z \neq 0$ bestemmer en halvlinie ℓ_z, nemlig halvlinien fra 0 gennem z. Specielt er ℓ_1 den positive reelle halvakse. Når $z \neq 0$, siges det reelle tal θ at være et *argument* for z, hvis θ er en vinkel fra ℓ_1 til ℓ_z.

Hvis θ er et argument for z, så er de øvrige argumenter for z tallene $\theta + 2\pi q$ for $q \in \mathbb{Z}$. Det følger, at der findes ét argument θ for z således, at $0 \leqslant \theta < 2\pi$, og ét argument θ således, at $-\pi < \theta \leqslant \pi$.

(5.5) Sætning. *Lad z og w være komplekse tal forskellige fra 0, med argumenter θ_z og θ_w. Da er $|zw| = |z|{\cdot}|w|$ og $\theta_z + \theta_w$ er et argument for zw.*

Bevis. Antag, at $z = a+bi$. Da er $zw = aw+biw$. Vektoren zw er altså linearkombinationen,

$$zw = aw + b(iw), \tag{1}$$

af vektorerne w og iw. For $w = c + di$ har vi $iw = -d + ci$. Vektoren iw er altså *tværvektoren* til vektoren w. Den har samme længde som w, men er drejet $\pi/2$ i den positive omløbsretning.

Som vektorer er w og iw et ortogonalsystem. Af fremstillingen (1) slutter vi derfor (Pytagoras), at $|zw|^2 = (a^2 + b^2)|w|^2 = |z|^2|w|^2$. Følgelig er $|zw| = |z||w|$. Yderligere slutter vi, at vinklen fra ℓ_w til ℓ_{zw} er lig med vinklen fra ℓ_1 til ℓ_z. Vinklen fra ℓ_1 til ℓ_{zw} er summen af vinklen fra ℓ_1 til ℓ_w og vinklen fra ℓ_w til ℓ_{zw}, og altså lig med summen $\theta_w + \theta_z$.

Hermed er begge påstande bevist. □

(5.6) Komplekse enheder. Komplekse tal z, for hvilke $|z| = 1$, altså komplekse tal på enhedscirklen, kaldes også *enheder* eller *komplekse fortegn*. Mængden af enheder betegnes også $\mathbb{U}$. Når $z = a + ib$ ligger på enhedscirklen, har vi $a = \cos\theta$ og $b = \sin\theta$, hvor θ er et argument for z. Som bekendt skriver vi også

$$e^{i\theta} = \exp i\theta := \cos\theta + i\sin\theta;$$

de komplekse enheder er altså tallene af formen $e^{i\theta}$.

For hvert komplekst tal $z \neq 0$ har vi $r := |z| > 0$ og $z/|z|$ er en enhed, af formen $e^{i\theta}$, hvor θ er et argument for z. Vi har altså fremstillingen,

$$z = |z|\frac{z}{|z|} = re^{i\theta},$$

af z som produkt af et positivt reelt tal og en kompleks enhed.

Når $w = se^{i\phi}$, finder vi $zw = rse^{i\theta}e^{i\phi}$. Resultatet i Sætning (5.5) er derfor ækvivalent med ligningen,

$$e^{i(\theta+\phi)} = e^{i\theta}e^{i\phi}, \tag{5.6.1}$$

som, skrevet ud i koordinater, er *additionsformlerne*,

$$\cos(\theta+\phi) = \cos\theta\cos\phi - \sin\theta\sin\phi, \quad \sin(\theta+\phi) = \sin\theta\cos\phi + \cos\theta\sin\phi.$$

(5.7) Eksempel. For hvert naturligt tal n er der præcis n komplekse løsninger til ligningen,

$$z^n = 1,$$

nemlig tallene $z = e^{2\pi ia/n}$ for $a = 0, 1, \dots, n-1$.

Hertil bemærker vi først, at hvis z er en løsning, så er $|z|^n = |z^n| = |1| = 1$. Den numeriske værdi $|z|$ er et positivt reelt tal, og da $|z|^n = 1$, må vi have $|z| = 1$. Løsninger z til ligningen skal altså søges blandt tallene i $\mathbb{U}$, dvs blandt tallene af formen $z = e^{i\theta}$. Idet vi kan kræve, at $0 \leqslant \theta < 2\pi$, er θ entydigt bestemt.

Det følger af (5.6.1), at $(e^{i\theta})^n = e^{in\theta}$. Altså er $z^n = 1$, hvis og kun hvis $n\theta$ er et argument for tallet 1, altså hvis og kun hvis $n\theta = (2\pi)a$ med et helt tal a. Da vi kun betragter argumenter θ med $0 \leqslant \theta < 2\pi$, er $z = e^{i\theta}$ altså løsning, hvis og kun hvis $\theta = 2\pi a/n$, hvor $0 \leqslant a < n$, dvs hvis og kun hvis z har den angivne form.

De n løsninger til ligningen $z^n = 1$ kaldes de n'te *enhedsrødder*.

(5.8) Opgaver.

1. Vis, at der ikke findes nogen total ordning af de komplekse tal, som harmonerer med addition og multiplikation (i den forstand at betingelserne (1.1)(ao) og (mo) er opfyldt).

2. Vis, at $\frac{1}{2} + \frac{i}{2}\sqrt{3}$ er en 6'te enhedsrod. Angiv alle de 6'te enhedsrødder.

3. Angiv et element i $\mathbb{U}$, som ikke er en enhedsrod.

4. Lad ζ være en n'te enhedsrod, og lad k være det mindste naturlige tal således, at $\zeta^k = 1$. Vis, at k er divisor i n.

6. Restklasser og kongruens.

(6.1) Indledning. Som bekendt siges to hele tal x og y at være *kongruente* modulo n, og vi skriver $x \equiv y \pmod n$, hvis differensen $x - y$ er delelig med n. Kongruens er en såkaldt *ækvivalensrelation* blandt hele tal. Den deler tallene i klasser af indbyrdes kongruente tal. For $n = 2$ er der to klasser: de *lige* tal er tallene, der er kongruente med 0 modulo 2; resten, de *ulige* tal, er kongruente med 1 modulo 2.

I dette kapitel minder vi kort om nogle begreber knyttet til relationer i almindelighed, og specielt om ækvivalensrelationer og klassedelinger. Hovedeksemplet, som er kongruens, bliver udførligt behandlet.

(6.2) Definition. Ved en *relation* i en mængde X forstås en delmængde $R \subseteq X \times X$. At et par (x, y) tilhører delmængden R udtrykkes med skrivemåden xRy. Det skal understreges, at xRy er et udsagn: det er sandt hvis $(x, y) \in R$, og falsk hvis $(x, y) \notin R$. Som sædvanlig, når man skriver 'xRy', underforstås en påstand om at udsagnet er sandt. Skrivemåden $x \not R y$ udtrykker, at udsagnet xRy er falsk.

En relation R kan være

refleksiv: xRx,
irrefleksiv: $x \not R x$,
symmetrisk: $xRy \implies yRx$,
asymmetrisk: xRy og $yRx \implies x = y$,
transitiv: xRy og $yRz \implies xRz$.

Endelig kaldes relationen *total*, hvis der altid gælder xRy eller yRx eller $x = y$. Det er underforstået, at betingelserne gælder for alle elementer i X.

En relation, der er refleksiv, symmetrisk og transitiv kaldes en *ækvivalensrelation*. Et eksempel er relationen '$=$' ('er lig med'). For ækvivalensrelationer bruges ofte tegn, der minder om lighedstegnet. Almindeligt brugte tegn er '$\equiv$', '$\sim$' (læses: „tilde“), og '$\approx$'.

En relation, der er asymmetrisk og transitiv kaldes en *ordensrelation* eller blot en *ordning*. For eksempel er relationen '$<$' ('er mindre end') en total ordning af tallene. For ordensrelationer bruges ofte tegn, der minder om ulighedstegnet. Almindeligt brugte tegn er '$<$', '$\prec$', '$\succ$', og lignende.

Når man vil understrege, at en ordning ikke nødvendigvis er total, taler man om en *partiel* ordning. Antag, at der er givet en ordning '$\prec$' i mængden X. Et element x_0 i X siges da at være *største element* i X, hvis der for alle $x \neq x_0$ gælder, at $x \prec x_0$. Elementet x_0 siges at være *maksimalt element* i X, hvis der af $x_0 \prec x$ følger, at $x_0 = x$. Bemærk forskellen: x_0 er største element, hvis alle andre elementer „er mindre“, og x_0 er maksimalt element, hvis ingen andre elementer „er større“. Hvis ordningen er total, falder de to begreber sammen. Tilsvarende defineres *minimalt element* og *mindste element*.

(6.3) Eksempel. Familierelationer er gode eksempler (bortset fra at de måske matematisk kan være svære at præcisere). Relationen 'er gift med' er symmetrisk, 'er barn af' er asymmetrisk, 'er i familie med' er en ækvivalensrelation, 'er efterkommer af' er en ordning. Hvilke egenskaber har 'er søster til'?

(6.4) Eksempel. Relationen '$=$' ('er lig med') er en ækvivalensrelation. Relationen '$\neq$' ('er forskellig fra') er symmetrisk og irrefleksiv.

Hvis M er en mængde, så er *potensmængden* $X := \mathcal{P}(M)$, bestående af alle delmængder af M, partielt ordnet ved '$\subset$' ('er strengt indeholdt i'). Ordningen er irrefleksiv (ifølge dansk sædvane). Den tilhørende refleksive ordning er '$\subseteq$' ('er indeholdt i'). Det største element i $\mathcal{P}(M)$ er M, det mindste element er $\emptyset$. Hvis vi i stedet betragter mængden $\mathcal{P}^*(M)$ af ikke-tomme delmængder af M (og antager, at M indeholder mindst to elementer), så er M stadig største element, men der er intet mindste element. Et-punkts-mængderne, altså delmængder af formen $\{a\}$, er de minimale elementer i $\mathcal{P}^*(M)$.

Relationen '$<$' ('er mindre end') er en total, irrefleksiv ordning af de reelle tal. Den tilsvarende refleksive ordning betegnes '$\leqslant$' eller '$\leq$'.

(6.5) Ækvivalensklasser. Lad der være givet en ækvivalensrelation '$\sim$' i mængden X, hvor altså

$$x \sim x, \qquad x \sim y \implies y \sim x, \qquad x \sim y \text{ og } y \sim z \implies x \sim z.$$

For hvert element a i X kan vi da betragte delmængden,

$$[a] := \{x \in X \mid x \sim a\}. \tag{6.5.1}$$

Bemærk, at skrivemåden $[a]$ underforstår den givne ækvivalensrelation i X. Delmængder af X, der er af formen $[a]$ med et passende element a i X, kaldes *ækvivalensklasser*.

Ækvivalensklasserne udgør en *klassedeling* af X, dvs et system af ikke-tomme delmængder således, at hvert element $x \in X$ ligger i præcis én delmængde fra systemet. Mere præcist gælder følgende resultat:

For en given ækvivalensrelation '$\sim$' i X udgør ækvivalensklasserne $[a]$, for $a \in X$, en klassedeling af X. To elementer $a, b \in X$ ligger i samme ækvivalensklasse, hvis og kun hvis $a \sim b$; specielt er $[a] = [b]$, hvis og kun hvis $a \sim b$. Er der omvendt givet en klassedeling af X, så er relationen 'ligger i samme klasse som' en ækvivalensrelation, hvis ækvivalensklasser netop er de givne klasser.

Bevis. Refleksiviteten sikrer, at $a \sim a$. Altså er $a \in [a]$. Specielt er hver ækvivalensklasse ikke-tom, og hvert element $a \in X$ ligger i en ækvivalensklasse, nemlig i $[a]$. For at vise, at ækvivalensklasserne udgør en klassedeling, skal vi bevise, at $[a]$ er den eneste ækvivalensklasse, der indeholder a. Det skal altså vises, at hvis a ligger i en ækvivalensklasse $[b]$, så er $[a] = [b]$.

Antag altså, at $a \in [b]$, altså at $a \sim b$. For at vise inklusionen $[a] \subseteq [b]$ betragtes et element $x \in [a]$. Da er $x \sim a$, og da $a \sim b$, sikrer transitiviteten, at $x \sim b$. Altså er $x \in [b]$. Følgelig gælder inklusionen $[a] \subseteq [b]$. I beviset benyttedes kun, at $a \sim b$. Denne betingelse er imidlertid symmetrisk i a og b, og følgelig gælder også inklusionen $[b] \subseteq [a]$. Altså er $[a] = [b]$. Hermed er vist, at ækvivalensklasserne udgør en klassedeling af X.

For at vise den anden påstand antages først, at $a \sim b$. Da er $a \in [b]$, og da vi også har $a \in [a]$, må $[a]$ og $[b]$ være samme ækvivalensklasse. Elementerne a og b ligger altså i samme ækvivalensklasse, nemlig i $[a] = [b]$. Antag omvendt, at a og b ligger i samme ækvivalensklasse. Denne ækvivalensklasse må være $[b]$, som jo er den eneste ækvivalensklasse, der indeholder b. Altså er $a \in [b]$, dvs $a \sim b$. Hermed er den anden påstand bevist.

Antag endelig, at der er givet en klassedeling af X. Relationen 'ligger i samme klasse som' er øjensynlig refleksiv (a ligger i samme klasse som sig selv), symmetrisk (hvis a og b ligger i samme klasse, så ligger b og a i samme klasse), og transitiv (hvis a og b ligger i samme klasse og b og c ligger i samme klasse, så ligger a og c i samme klasse, nemlig i den entydigt bestemte klasse, der indeholder b). Relationen er altså en ækvivalensrelation, og de tilhørende ækvivalensklasser er øjensynlig netop delmængderne fra den givne klassedeling.

Hermed er resultatet bevist. □

For en given ækvivalensrelation '$\sim$' i en mængde X er det ofte hensigtsmæssigt at betragte mængden af ækvivalensklasser som en (ny, abstrakt) mængde i sig selv. Denne mængde af ækvivalensklasser kaldes *kvotientmængden* (af X mht den givne ækvivalensrelation), og den kan betegnes $X/\sim$. En ækvivalensklasse A kan herefter opfattes på to måder: den er delmængde af den givne mængde X, og den er element i kvotientmængden $X/\sim$. Elementerne i en ækvivalensklasse A siges også at være *repræsentanter* for A.

(6.6) Definition. I det følgende betegner n et fast naturligt tal. To hele tal x, y kaldes *kongruente modulo* n, og vi skriver $x \equiv y \pmod{n}$, hvis n går op i differensen $x - y$, altså,

$$x \equiv y \pmod{n} \overset{\text{DEF}}{\iff} n \mid x-y\,.$$

Relationen er refleksiv, thi n går op i $x - x = 0$. Den er symmetrisk, thi hvis n går op i $x - y$, så går n op i $y - x = -(x - y)$. Og endelig er den transitiv, thi hvis n går op i $x - y$ og i $y - z$, så går n op i $x - z = (x - y) + (y - z)$. Kongruens modulo n er altså en ækvivalensrelation i mængden $\mathbb{Z}$ af hele tal.

For hvert tal $a \in \mathbb{Z}$ er ækvivalensklassen $[a]$ en delmængde af $\mathbb{Z}$. Den består af de hele tal x, for hvilke n går op i $x - a$, altså af de hele tal x af formen $x = a + qn$. Vi har altså

$$[a] = \{\dots, a-2n,\ a-n,\ a,\ a+n,\ a+2n,\ a+3n, \dots\}\,.$$

Elementerne i ækvivalensklassen $[a]$ er altså *resterne* af a ved division med n, og ækvivalensklasserne kaldes *restklasser* modulo n. Kvotientmængden $\mathbb{Z}/\equiv$ er altså mængden af restklasser. Den betegnes $\mathbb{Z}/n\mathbb{Z}$ eller $\mathbb{Z}/n$ (i litteraturen vil man også finde betegnelsen $\mathbb{Z}_n$). Restklassen $[a]$ afhænger naturligvis af det givne tal n. Hvis man vil understrege afhængigheden, skrives $[a]_n$.

Ifølge Sætningen om division med rest (3.4) findes for hvert helt tal a entydigt bestemte tal q og r således, at

$$a = qn + r, \quad \text{og } 0 \leqslant r < n.$$

Tallene r, der tilfredsstiller en ligning $a = qn + r$ med et helt tal q, er netop tallene, der er kongruente med a, altså netop elementerne i restklassen $[a]$. Resultatet udsiger altså, at der i hver restklasse $[a]$ findes et og kun ét tal r med $0 \leqslant r < n$; denne rest er som bekendt den *principale rest* af a ved division med n. Specielt følger det, at antallet af restklasser er lig med antallet af mulige principale rester, altså lig med n. Mængden $\mathbb{Z}/n\mathbb{Z}$ af restklasser består altså af de n restklasser

$$[0], [1], \dots, [n-1].$$

Bemærk specielt, at restklassen [0] består af alle tal, der er delelige med n,

$$\dots, -2n, -n, 0, n, 2n, 3n, \dots;$$

Denne restklasse betegner vi med $\mathbf{0}$. Restklassen [1], som vi også betegner $\mathbf{1}$, består af tallene $\dots, 1-n, 1, 1+n, 1+2n, \dots$. Når man vil understrege afhængigheden af det givne tal n, kan man skrive $\mathbf{0}_n$ og $\mathbf{1}_n$.

(6.7) Eksempel. For $n = 6$ har vi 6 restklasser, $[0], [1], \dots, [5]$. Bemærk, at

$$\cdots = [-8] = [-2] = [4] = [10] = [16] = \cdots.$$

(6.8) Addition og multiplikation af restklasser. For to restklasser A og B modulo n defineres *sum*, $A + B$, og *produkt*, $A \cdot B$, således: Vælg et tal a i restklassen A, hvor altså $A = [a]$, og vælg et tal b i restklassen B, hvor altså $B = [b]$, og sæt

$$\begin{aligned} A + B &:= [a+b], \\ A \cdot B &:= [ab]. \end{aligned} \tag{6.8.1}$$

Denne fastlæggelse er en *lovlig definition*, hvormed menes følgende: I ligningernes højresider indgår a, som er valgt i restklassen A. Dette er et valg blandt flere (endda uendelig mange) muligheder. Tilsvarende er der flere muligheder for at vælge b. Det skal vises, at ligningernes højresider er uafhængige af de foretagne valg. Med andre ord: hvis a' er et andet tal i restklassen A og b' er et andet tal i restklassen B, så er

$$[a' + b'] = [a+b], \qquad [a'b'] = [ab].$$

Hertil bemærkes, at da a og a' ligger i samme restklasse, er de kongruente modulo n; der findes altså et helt tal q således, at $a' = a + qn$. Tilsvarende findes et helt tal s således, at $b' = b + sn$. Nu får vi, at

$$\begin{aligned} a' + b' &= a + qn + b + sn = a + b + (q+s)n, \\ a'b' &= (a+qn)(b+sn) = ab + (qb+as+qsn)n. \end{aligned}$$

Det følger, at $a' + b' \equiv a + b$ og $a'b' \equiv ab$. Altså er $[a' + b'] = [a+b]$ og $[a'b'] = [ab]$. Hermed er vist, at definitionen er lovlig.

Tilsvarende – og lettere – ses, at følgende definition er lovlig: den *modsatte restklasse* til A, betegnet $-A$, defineres ved $-A := [-a]$, hvor a er valgt i restklassen A.

Bemærk, at de to ligninger i (6.8.1) udtrykker, at

$$\begin{aligned} [a] + [b] &= [a+b], \\ [a] \cdot [b] &= [ab], \end{aligned} \tag{6.8.2}$$

hvor '+' og '·' på venstresiderne refererer til addition og multiplikation af restklasser. Som ved multiplikation af tal udelader vi normalt '·'en ved produkt af restklasser.

(6.9) Regnereglerne. *For regning med restklasser A, B, C modulo n gælder følgende regler:*

$$A + B = B + A, \tag{a0}$$
$$A + (B + C) = (A + B) + C, \tag{a1}$$
$$A + \mathbf{0} = \mathbf{0} + A = A, \tag{a2}$$
$$A + (-A) = (-A) + A = \mathbf{0}, \tag{a3}$$
$$AB = BA, \tag{m0}$$
$$A(BC) = (AB)C, \tag{m1}$$
$$A\mathbf{1} = \mathbf{1}A = A, \tag{m2}$$
$$A(B + C) = AB + AC. \tag{am}$$

Yderligere gælder, at hvis $A = [a]$ er restklassen bestemt ved et tal a, der er primisk med n, så findes en restklasse A' således, at

$$AA' = A'A = \mathbf{1}. \tag{m3}$$

Bevis. Vælg tal a og b i restklasserne A og B. Vi har da ligningerne,

$$A + B = [a + b] = [b + a] = B + A.$$

Den første og den sidste ligning er nemlig definitionen på addition af restklasser, og den midterste ligning følger af at addition af hele tal er kommutativ. Hermed er reglen (a0) bevist. På samme måde følger reglerne (a1), (a2), (a3), (m0), (m1), (m2) og (am) af de tilsvarende regler for regning med hele tal.

For at vise den sidste påstand antages, at tallet a, som var valgt i A, er primisk med n. Af Korollar (3.9) følger derfor, at der findes hele tal x og y således, at $xa + yn = 1$. Specielt er så $xa \equiv 1 \pmod{n}$, og dermed er $[xa] = [1]$. Ifølge definition af produkt af restklasser er $[xa] = [x][a]$. Altså gælder ligningen,

$$[x][a] = [1]. \tag{*}$$

Nu var $[a] = A$ og $[1] = \mathbf{1}$. Af (*) fremgår derfor, at med $A' := [x]$ gælder den anden ligning i (m3). Den første følger af (m0).

Hermed er regnereglerne eftervist. □

(6.10) Eksempel. Betragt et naturligt tal a med cifrene $a_k, \dots, a_0$ i 10-talssystemet, altså

$$a = a_k \cdot 10^k + \cdots + a_1 \cdot 10 + a_0.$$

Da gælder modulo 11 kongruensen:

$$a \equiv a_0 - a_1 + a_2 - \cdots + (-1)^k a_k \pmod{11}.$$

Specielt er a delelig med 11, hvis og kun hvis højresiden (den alternerende sum af cifrene) er delelig med 11.

Modulo 11 gælder nemlig $10 \equiv -1$, altså $[10] = [-1]$. Heraf følger $[10^2] = [10]^2 = [(-1)]^2 = [1]$ og, generelt, $[10^i] = [(-1)^i]$. Videre får vi så, at

$$[a_i \cdot 10^i] = [a_i][10^i] = [a_i][(-1)^i] = [(-1)^i a_i],$$

og endelig, at

$$\begin{aligned}[a] &= [a_k \cdot 10^k + \cdots + a_0] = [a_k \cdot 10^k] + \cdots + [a_0] \\ &= [(-1)^k a_k] + \cdots + [a_0] = [(-1)^k a_k + \cdots + a_0].\end{aligned}$$

Undervejs brugte vi gentagne gange ligningerne i (6.8.2).

(6.11) Primiske restklasser. En restklasse modulo n kaldes en *primisk restklasse*, hvis den har formen $[a]$ med et tal a, der er primisk med n. Tallene a, n og tallene $a+qn, n$ har øjensynlig de samme fælles divisorer. Heraf følger, at alle rester i en primisk restklasse er primiske med n. Specielt ses, at de primiske restklasser er restklasserne af formen $[r]$, hvor

$$0 \leqslant r < n \text{ og } (r, n) = 1.$$

Antallet af primiske restklasser er altså antallet af tal r, som opfylder ovenstående to betingelser. Dette antal betegnes $\varphi(n)$. Funktionen $\varphi(n)$, der er defineret for alle naturlige tal n, kaldes *Euler's φ-funktion*.

Restklassen $\mathbf{1}$ er en primisk restklasse, idet 1 er primisk med n. Hvis $n > 1$, er restklassen $\mathbf{0}$ ikke en primisk restklasse, idet n er den største fælles divisor for $0, n$. Tilfældet $n = 1$ er på flere punkter en undtagelse, som vi dog ikke vil udelukke. Hvis $n = 1$, så er alle tal kongruente, så der er kun én restklasse. Denne ene restklasse er altså $\mathbf{0}_1 = \mathbf{1}_1$, og den er primisk ifølge definitionen ovenfor. Specielt er altså $\varphi(1) = 1$.

En restklasse A modulo n kaldes *invertibel*, hvis der findes en restklasse A' således, at $A'A = \mathbf{1}$. Der findes højst én sådan restklasse A'. Antager man nemlig, at også $A''A = \mathbf{1}$, så får man, at

$$A'' = A''\mathbf{1} = A''AA' = \mathbf{1}A' = A'.$$

Når restklassen A er invertibel, er restklassen A' altså entydigt bestemt. Den kaldes den *inverse* restklasse til A, og betegnes A^{-1}.

Af regnereglen (m3) følger, at enhver primisk restklasse er invertibel. Omvendt gælder, at enhver invertibel restklasse er primisk. Antag nemlig, at $A'A = [1]$. Vælg en rest a i A og en rest a' i A'. Så er $A' = [a']$ og $A = [a]$, og dermed er $A'A = [a'a]$. Ifølge antagelsen er altså $[a'a] = [1]$. Følgelig er $a'a \equiv 1 \pmod{n}$. Der findes derfor et helt tal q således, at

$$1 = a'a + qn.$$

Ethvert positivt tal, som er divisor i både a og n, er derfor divisor i 1. Følgelig er a og n primiske.

Mængden af primiske restklasser, som delmængde af mængden $\mathbb{Z}/n$ af alle restklasser, betegnes $(\mathbb{Z}/n)^*$.

(6.12) Eksempel. Modulo 10 er der 10 restklasser: [0], [1], ..., [9]. Af tallene $0, 1, \dots, 9$ er det 1, 3, 7 og 9, der er primiske med 10. Der er altså 4 primiske restklasser, [1], [3], [7], og [9]. Specielt er $\varphi(10) = 4$. Modulo 10 er $1^2 \equiv 1$, $3 \cdot 7 = 21 \equiv 1$ og $9^2 \equiv (-1)^2 = 1$. Altså finder vi,

$$[1]^{-1} = [1], \quad [3]^{-1} = [7], \quad [7]^{-1} = [3], \quad [9]^{-1} = [9].$$

(6.13) Eksempel. For restklasser modulo et primtal p gælder, at alle restklasser forskellige fra [0] er invertible. Når p er et primtal, så er nemlig ethvert tal a med $0 < a < p$ primisk med p. Det følger specielt, at $\varphi(p) = p - 1$ når p er et primtal.

For eksempel finder vi modulo 5, at

$$[1]^{-1} = [1], \quad [2]^{-1} = [3], \quad [3]^{-1} = [2], \quad [4]^{-1} = [4].$$

For en primtalspotens p^r har vi, at a er primisk med p^r, hvis og kun hvis p ikke går op i a. Af tallene $1, 2, \dots, p^r$ er det altså netop tallene af formen bp for $b = 1, \dots, p^{r-1}$, der *ikke* er primiske med p^r. Der er p^{r-1} tal af denne form. For en primtalspotens p^r har vi derfor ligningen,

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p - 1).$$

(6.14) Den kinesiske Restklassesætning. *Antag, at $n = n_1 \cdots n_r$ er et produkt af parvis primiske naturlige tal n_i. Da gælder for hvert sæt $(a_1, \dots, a_r)$ af hele tal, at systemet af kongruenser,*

$$x \equiv a_1 \pmod{n_1}, \quad \dots, x \equiv a_r \pmod{n_r},$$

har løsninger $x \in \mathbb{Z}$, og løsningerne udgør én restklasse modulo n. Ækvivalent gælder: Der er en veldefineret afbildning,

$$\mathbb{Z}/n \to \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r, \tag{6.14.1}$$

bestemt ved at restklassen $[x]_n$, for $x \in \mathbb{Z}$, afbildes i r-sættet $([x]_{n_1}, \dots, [x]_{n_r})$, og denne afbildning er bijektiv.

Bevis. Hvert n_i er divisor i n, så hvis to tal x, y er kongruente modulo n, er de også kongruente modulo n_i. Heraf ses, at den beskrevne afbildning er veldefineret.

For at indse, at de to formuleringer er ækvivalente, bemærkes, at systemet af kongruenser er ækvivalent med systemet af ligninger:

$$[x]_{n_1} = [a_1]_{n_1}, \ \dots, \ [x]_{n_r} = [a_r]_{n_r}.$$

Hvert element i produktmængden $\mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r$ er et r-sæt $([a_1]_{n_1}, \dots, [a_r]_{n_r})$, hvor $a_1, \dots, a_r$ er hele tal. At kongruenserne altid har løsninger betyder derfor, at afbildningen (6.14.1) er surjektiv. At løsningerne, for givne $a_1, \dots, a_r$, udgør én restklasse modulo n, betyder, at afbildningen er bijektiv.

Vi viser først, at afbildningen er injektiv. Antag hertil, at to restklasser $[x]_n$ og $[y]_n$ afbildes på det samme r-sæt, altså at $[x]_{n_i} = [y]_{n_i}$ for $i = 1, \dots, r$. Da er $x \equiv y \pmod{n_i}$, og dermed n_i divisor i $x - y$, for $i = 1, \dots, r$. Af Korollar (3.13) følger, at n er divisor i $x - y$. Følgelig er $[x]_n = [y]_n$. Afbildningen er altså injektiv.

Mængden $\mathbb{Z}/n$ har n elementer, og produktmængden $\mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r$ har $n_1 \cdots n_r$ elementer. Da $n = n_1 \cdots n_r$ har de to mængder altså samme antal elementer. Den injektive afbildning fra den første mængde til den anden må derfor være bijektiv. ∎

(6.15) Tilføjelse. Antag, at $n = n_1 \cdots n_r$, hvor faktorerne n_i er parvis primiske. Hvert n_i er divisor i n, så det følger umiddelbart, at hvis a er primisk med n, så er a primisk med hvert n_i. Af Korollar (3.10) fås det omvendte: hvis a er primisk med hvert n_i, så er a primisk med n. Heraf ses, at restklassen $[a]_n$ modulo n er en primisk restklasse, hvis og kun hvis der for alle i gælder, at restklassen $[a]_{n_i}$ er en primisk restklasse modulo n_i. Under den bijektive afbildning i (6.14) gælder altså, at de primiske restklasser modulo n svarer til r-sæt af primiske restklasser. Specielt gælder, at antallet af primiske restklasser modulo n er produktet, for $i = 1, \dots, r$, af antallet af primiske restklasser modulo n_i. Med andre ord gælder for Euler's φ-funktion ligningen,

$$\varphi(n) = \varphi(n_1) \cdots \varphi(n_r). \tag{6.15.1}$$

For eksempel gælder for en primopløsning $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$, hvor p_i'erne er forskellige primtal, at

$$\varphi(n) = \varphi(p_1^{\nu_1}) \cdots \varphi(p_r^{\nu_r}). \tag{6.15.2}$$

Som nævnt i (6.13) er $\varphi(p^\nu) = p^{\nu-1}(p-1)$, og (6.15.2) bestemmer derfor $\varphi(n)$ ud fra en primopløsning af n.

(6.16) Note. Det er en vigtig del af Den kinesiske Restklassesætning, at systemet af kongruenser i (6.14) altid har løsninger x. Bemærk, at denne del af sætningen i beviset fremkom som konsekvens af at systemet, modulo n, højst har én løsning; det er jo det sidste, der svarer til at afbildningen (6.14.1) er injektiv. Det er muligt at give mere konstruktive beviser for eksistensen af løsninger.

For eksempel kan man gå således frem: Induktivt kan det antages, at løsningerne til de første $r-1$ kongruenser udgør én restklasse modulo $m' := m_1 \cdots m_{r-1}$, altså at løsningerne, for et passende tal a', netop er tallene af formen $x = a' + ym'$ for $y \in \mathbb{Z}$. Løsningerne til hele systemet består så af de tal af denne form, som også tilfredsstiller den sidste kongruens $x \equiv a_r \pmod{m_r}$. Det er en betingelse på y:

$$a' + ym' \equiv a_r \pmod{m_r} \iff ym' \equiv a_r - a' \pmod{m_r}.$$

Tallet m' er produktet af faktorer, som alle er primiske med m_r. Restklassen af m' modulo m_r er derfor invertibel, så der findes et tal k', så $m'k' \equiv 1 \pmod{m_r}$. Den sidste kongruens ovenfor er derfor opfyldt, præcis når $y \equiv (a_r - a')k' \pmod{m_r}$, dvs når y har formen $y = (a_r - a')k' + zm_r$ med $z \in \mathbb{Z}$. De tal x, som opfylder alle kongruenserne, er altså tallene af formen $x = a' + ym' = a' + (a_r - a')k'm' + zm_rm'$. Med $m := m'm_r = m_1 \cdots m_r$ er løsningerne altså præcis tallene af følgende form:

$$x = a' + (a_r - a')k'm' + zm \quad \text{med } z \in \mathbb{Z}. \tag{6.16.1}$$

Det fremgår specielt, at løsningerne udgør én restklasse modulo m. Dette argument giver således et alternativt bevis for (6.14).

I formlen (6.16.1) er k' bestemt modulo m_r ved, at restklassen af k' er den inverse til restklassen af m'. Af og til kan det med fordel udnyttes, at $m' = m_1 \cdots m_{r-1}$: hvis k_i for $i = 1, \dots, r-1$ er repræsentant for den inverse til restklassen af m_i modulo m_r, så kan man som k' bruge $k' = k_1 \cdots k_{r-1}$.

(6.17) Opgaver.

1. Hvilke af følgende relationer i mængden af komplekse tal er ækvivalensrelationer:
(1) $zR_1w \Leftrightarrow |z| = |w|$. (2) $zR_2w \Leftrightarrow |z - w| = 1$. (3) $zR_3w \Leftrightarrow z = w$ eller $z = \overline{w}$.
(4) $zR_4w \Leftrightarrow |z| \leqslant |w|$. (5) $zR_5w \Leftrightarrow \exists r > 0 : z = rw$.
Angiv for hver af ækvivalensrelationerne den tilhørende klassedeling af $\mathbb{C}$.

2. Lad $f : X \to Y$ være en afbildning. Ved *fibrene* for afbildningen forstås originalmængderne $f^{-1}(y)$ af elementerne y i Y. Vis, at de ikke-tomme fibre for f udgør en klassedeling af X. Beskriv den tilhørende ækvivalensrelation.

3. Hvor mange ækvivalensrelationer findes der i en mængde med 4 elementer?

4. Vis, at der ved $x \equiv y \Leftrightarrow x - y \in \mathbb{Z}$ defineres en ækvivalensrelation i $\mathbb{R}$.

5. Angiv de primiske restklasser modulo 18, og angiv for hver af dem den inverse restklasse. Løs samme opgave modulo 20.

6. Idet A og B er givne restklasser modulo n defineres en afbildning af $\mathbb{Z}/n$ ind i sig selv ved $X \mapsto AX + B$. Vis, at afbildningen er bijektiv, hvis og kun hvis A er en primisk restklasse.

7. Bestem for hver af følgende kongruenser de hele tal x, som er løsninger: (a) $5x \equiv 2 \pmod 9$. (b) $5x \equiv 2 \pmod{10}$. (c) $x^2 \equiv -1 \pmod 5$. (d) $x^2 \equiv -1 \pmod 7$.

8. Bestem antallet af løsninger (modulo n) til kongruensen $2x \equiv 0 \pmod n$, når n er lige og når n er ulige.

9. Lad $n = n_1 \cdots n_r$ være et produkt af parvis primiske tal n_i. Sæt $n_i' := n/n_i$, hvor altså $n = n_i n_i'$ og n_i' er produktet af tallene n_j for $j \neq i$. Vis, at der findes hele tal x_i og y_i og en fremstilling $1 = x_i n_i + y_i n_i'$. Sæt $e_i := y_i n_i'$. Vis, at der gælder følgende kongruenser:

$$e_i \equiv 1 \pmod{n_i}, \quad e_i \equiv 0 \pmod{n_i'}, \quad e_1 + \cdots + e_r \equiv 1 \pmod n.$$

[For at vise den sidste betragtes fx $(1 - e_1) \cdots (1 - e_r)$. Udnyt, at $e_i e_j \equiv 0 \pmod n$ for $i \neq j$.] Vis nu, at ethvert system af kongruenser $x \equiv a_i \pmod{n_i}$ har en, og modulo n kun én, løsning, nemlig $x = e_1 a_1 + \cdots + e_r a_r$.
Overvej specielt tilfældet $r = 2$.

10. Lad p være et ulige primtal. Vis, at når $p \nmid x$, så er $x^{p-1} \equiv 1 \pmod p$ (Fermat's lille sætning).

11. *Lad p være et ulige primtal. Vis, at $(p-1)! \equiv -1 \pmod p$ (*Wilson's sætning*).
De $(p-1)/2$ tal b med $(p-1)/2 < b < p$ har formen $p - a$ med $1 \leqslant a \leqslant (p-1)/2$. Slut heraf, at $[((p-1)/2)!]^2 \equiv (-1)^{(p-1)/2} \pmod p$.
Vis, at kongruensen $x^2 \equiv -1 \pmod p$ har en løsning, hvis og kun hvis $p \equiv 1 \pmod 4$.

12. Løs systemet af kongruenser: $x \equiv 1 \pmod 4$, $x \equiv 2 \pmod 5$, $x \equiv 5 \pmod 9$.

13. Lad n være et naturligt tal, fremstillet med k cifre i 10-talssystemet. Antag, at n' er fremkommet af n ved ombytning af de k cifre. Vis, at tallet $n - n'$ er deleligt med 9.

14. En stamme vilde kannibaler fanger 100 matematikere. De skal alle spises, men de får en chance for at slippe fri: De bliver stillet op på en lang række, og alle udstyret med en hat, der er enten rød, gul eller grøn. Den, der gætter farven på sin egen hat, slipper fri. Hver matematiker i rækken kan se de foranstående, men kun høre de bagvedstående. Først gætter den bagerste, så den næstbagerste osv. Matematikerne har på forhånd aftalt en strategi. Hvor mange slipper fri?

15. (Euler's generalisering af Fermat's lille sætning.) Antag, at a er primisk med n. Vis, at $a^{\varphi(n)} \equiv 1 \pmod{n}$. [Vink: Restklassen $A = [a]$ er en primiske restklasse. Derfor er multiplikation med A en bijektiv afbildning af mængden af primiske restklasser på sig selv. Med andre ord: hvis $B_1, B_2, B_3, \dots$ er samtlige primiske restklasser opskrevet i en tilfældig orden, så er $AB_1, AB_2, AB_3, \dots$ igen samtlige primiske restklasser (i en anden orden). Produktet af alle restklasserne B_i er derfor lig med produktet af alle restklasserne AB_i. Heraf følger påstanden.]

16. (Gauss's generalisering af Wilson's sætning.) Lad w være produktet af alle naturlige tal mindre end n og primiske med n. Antag $n > 2$. Vis, at $w \equiv (-1)^{N/2} \pmod{n}$, hvor N er antallet af løsninger modulo n til kongruensen $x^2 \equiv 1 \pmod{n}$. [Vink: Restklassen $[w]$ af w er lig med produktet af alle primiske restklasser. For hver primisk restklasse A indgår også den inverse A^{-1} som faktor i w. De to faktorer går ud mod hinanden, med mindre de er den samme, dvs når $A^{-1} = A$, altså når $A^2 = \mathbf{1}$. Derfor er $[w]$ lig med produktet af de restklasser A, som opfylder $A^2 = \mathbf{1}$. I dette produkt forekommer for hver faktor A også restklassen $-A$ som faktor, og den er forskellig fra A, da $n > 2$. Slår vi faktorerne sammen to og to, kan vi erstatte $A(-A)$ med $A(-A) = -A^2 = -\mathbf{1}$. Heraf fås den ønskede formel.

Vis, at $w \equiv -1 \pmod{n}$, når $n = 4$ eller $n = p^\nu$ eller $n = 2p^\nu$ (med et ulige primtal p), og at $w \equiv 1$ i alle andre tilfælde.

17. Betragt kongruensen $x^2 \equiv 1 \pmod{n}$. Vis, at når $n = p^\nu$ er en potens af et ulige primtal p ($\nu > 0$), så har kongruensen præcis to løsninger. Bestem antallet af løsninger til kongruensen, når $n = 2^\nu$ er en potens af 2. [Vink: antallet afhænger af ν.] Bestem antallet af løsninger modulo n i almindelighed.

18. Findes der 1.000.000 på hinanden følgende ikke-kvadratfrie naturlige tal? (Et tal er *kvadratfrit*, hvis intet kvadrat (bortset fra 1) er divisor i tallet, eller, ækvalent, hvis det er et produkt af indbyrdes forskellige primtal.)

19. Vis, at for alle n er $n^{13} \equiv n \pmod{2730}$.

20. Vis det omvendte af Wilson's sætning, for $n \geqslant 2$: Hvis $(n-1)! \equiv -1 \pmod{n}$, så er n et primtal. Hvad med det omvendte af Fermat's lille sætning?

21. Bestem, udtrykt ved antallet af primdivisorer i n, antallet af kvadratfri divisorer i n.

22. Vis, at ethvert kvadrattal > 9 skrevet i 10-talssystemet indeholder mindst to forskellige ciffre.

Grupper

1. Gruppebegrebet.

(1.1) Indledning. En gruppe er en mængde G forsynet med en komposition, som opfylder visse simple betingelser, se nedenfor. Kompositioner, fx addition eller multiplikation af tal, har naturligvis altid spillet en rolle i matematik, men det blev først i 1800-tallet klart, at en række af de betragtede kompositioner havde fælles træk, som med fordel kunne udkrystalliseres i et abstrakt begreb.

Det skal understreges, at i den abstrakte situation er mængden G en vilkårlig mængde. Elementerne i en gruppe kan altså være alle slags „ting": tal, funktioner, afbildninger, delmængder (fx figurer, linier i et vektorrum, endelige delmængder af en given mængde), og meget mere.

Grupper møder man i al matematik. I nogle situationer er den abstrakte teori væsentlig for forståelsen af problemstillingen, i andre situationer vil den generelle teori ikke fortælle noget særligt, andet end at man står over for en gruppe. I dette indledende kapitel definerer vi den abstrakte gruppe, og omtaler stabile delmængder og undergrupper. Først og fremmest demonstrerer vi, at grupper møder man overalt.

(1.2) Definition. Ved en *gruppe* $(G, *)$ forstås en mængde G med en komposition $G \times G \to G$, betegnet $(x, y) \mapsto x * y$, som opfylder, at kompositionen er *associativ*, at der findes et *neutralt element* $e \in G$, og at der til hvert element x i G findes et *inverst element* x^{-1} i G. Betingelserne kan udtrykkes ved ligningerne, for alle $x, y, z \in G$,

$$(x * y) * z = x * (y * z), \tag{1.2.1}$$

$$e * x = x * e = x, \tag{1.2.2}$$

$$x^{-1} * x = x * x^{-1} = e. \tag{1.2.3}$$

Ligningen (1.2.1) udtrykker, at kompositionen er associativ. Det følger af ligningen, at det i en gruppe ikke er nødvendigt at sætte parenteser ved komposition af flere end to elementer. De to elementer $(x * y) * z$ og $x * (y * z)$ i G er det samme element, og dette element betegnes $x * y * z$.

Ligningerne (1.2.2) udtrykker, at elementet e i G er neutralt element for kompositionen. Det er altså betingelsen, at der i G findes et udvalgt element e således, at ligningerne gælder for alle elementer x i G.

Ligningerne (1.2.3) udtrykker, at der til hvert element $x \in G$ findes et element $x^{-1} \in G$, som er inverst til x i den forstand, at ligningerne gælder.

En gruppe $(G, *)$ kaldes *kommutativ* eller *abelsk*, hvis alle elementer i G *kommuterer*, dvs at der for alle x, y i G gælder ligningen,

$$x * y = y * x. \tag{1.2.4}$$

Elementantallet, $|G|$, for en gruppe G kaldes gruppens *orden*. For en endelig gruppe er ordenen et naturligt tal; for en uendelig gruppe skrives blot $|G| = \infty$.

(1.3) Notation. Kompositionen i en gruppe G er blot en afbildning $G \times G \to G$. I forbindelse med grupper og tilsvarende algebraiske strukturer er det sædvane at betegne en sådan afbildning med et *kompositionstegn*. Fx er der i definitionen i (1.2) brugt tegnet '$*$' for afbildningen: billedet af $(x, y) \in G \times G$ er betegnet $x * y$, og det kaldes *kompositet* af x og y. Andre anvendelige kompositionstegn er '$\circ$', '$\wedge$', '$\cup$', '$\times$', '$\oplus$', og lignende. Der er naturligvis intet i vejen for at en komposition $G \times G \to G$ kan noteres på sædvanlig vis som en afbildning $(x, y) \mapsto f(x, y)$. Kravene til kompositionen får så formen,

$$f(f(x, y), z) = f(x, f(y, z)), \quad f(e, x) = f(x, e) = x, \quad f(x^{-1}, x) = f(x, x^{-1}) = e.$$

De helt dominerende notationer for grupper er den *multiplikative* og den *additive* skrivemåde. Ved den multiplikative skrivemåde bruges tegnet '$\cdot$' for kompositionen, og $x \cdot y$ kaldes *produktet* af x og y. Oftest udelades endda kompositionstegnet, således at man skriver xy for $x \cdot y$. Med denne konvention får de tre krav formen,

$$(xy)z = x(yz), \quad ex = xe = x, \quad x^{-1}x = xx^{-1} = e.$$

Ofte vælger man ved den multiplikative skrivemåde at betegne det neutrale element i gruppen med symbolet 1, der så ikke må forveksles med tallet 1.

Ved den additive skrivemåde bruges tegnet '$+$' for kompositionen, og $x + y$ kaldes *summen* af x og y. Den additive skrivemåde anvendes *kun*, når kompositionen er kommutativ. Yderligere er det sædvane ved den additive skrivemåde at betegne det neutrale element med 0 og det inverse element til x med $-x$. Elementet $-x$ kaldes også det *modsatte* til x. Med den additive skrivemåde får betingelserne formen,

$$(x + y) + z = x + (y + z), \tag{1.3.1}$$
$$0 + x = x + 0 = x, \tag{1.3.2}$$
$$-x + x = x + (-x) = 0, \tag{1.3.3}$$
$$x + y = y + x. \tag{1.3.4}$$

Bemærk, at ligningen (1.3.4) er medtaget, idet den additive notation forudsætter, at gruppen er kommutativ. Det er i øvrigt sædvane at skrive $x - y$ for $x + (-y)$.

Når intet andet anføres, vil vi altid anvende den multiplikative skrivemåde.

(1.4) Invertibelt element. I det følgende vil vi flere gange se eksempler, hvor vi har givet en mængde S med en komposition $(x, y) \mapsto x * y$, som er associativ og har et neutralt element e, men hvor betingelsen (1.2.3) om inverst element ikke nødvendigvis er opfyldt. I denne mere generelle situation siges et element $x \in S$ at være *invertibelt*, hvis der findes et element $x' \in S$ således, at

$$x' * x = x * x' = e. \tag{1.4.1}$$

Der er højst ét sådant element x'. Er nemlig også $x'' * x = e$, så får vi

$$x'' = x'' * e = x'' * (x * x') = (x'' * x) * x' = e * x' = x'.$$

Når x er et invertibelt element i S, siges det entydigt bestemte x' i (1.4.1) at være det *inverse* til x, og det betegnes x^{-1}. Fx viser ligningen $e * e = e$, at vi som e' kan bruge e. Det neutrale element e er altså altid invertibelt, og vi har ligningen,

$$e^{-1} = e. \tag{1.4.2}$$

Lad os understrege, at for at vise, at et element x i S er invertibelt, skal man kunne eftervise eksistensen af det inverse, altså det element x', for hvilke de to ligninger (1.4.1) er opfyldt. Betragt fx for to invertible elementer x og y kompositet $z := x * y$. Vi har da ligningerne,

$$\begin{aligned} \big(y^{-1} * x^{-1}\big) * z &= y^{-1} * x^{-1} * x * y = y^{-1} * e * y = y^{-1} * y = e, \\ z * \big(y^{-1} * x^{-1}\big) &= x * y * y^{-1} * x^{-1} = x * e * x^{-1} = x * x^{-1} = e. \end{aligned}$$

Ligningerne viser, at kompositet $z = x * y$ også er invertibelt, og at det inverse er bestemt ved ligningen,

$$(x * y)^{-1} = y^{-1} * x^{-1}. \tag{1.4.3}$$

De to ligninger (1.4.1) viser i øvrigt, at $x' = x^{-1}$ er invertibel med x som det inverse. Vi har altså ligningen,

$$(x^{-1})^{-1} = x. \tag{1.4.4}$$

I en gruppe er alle elementer invertible. Specielt gælder altså i en gruppe ligningerne (1.4.2), (1.4.3) og (1.4.4).

(1.5) Stabil delmængde. Når der er givet en mængde S med en komposition $(x, y) \mapsto x * y$, kaldes en delmængde $H \subseteq S$ *stabil* under kompositionen, hvis der for alle elementer x og y i H gælder, at kompositet $x * y$ ligger i H. Under denne antagelse definerer kompositionen i S ved *restriktion* en komposition i H: kompositet af to elementer x og y i H er blot $x * y$ opfattet som element i H.

Antag, at kompositionen i S er associativ og har et neutralt element e. Lad S^* være delmængden bestående af de invertible elementer i S. Det fremgår af (1.4), at delmængden S^* er stabil, så den givne komposition i S definerer en komposition i S^*. Yderligere gælder:

Delmængden S^* bestående af de invertible elementer i S er en gruppe.

Ligningen (1.2.1) er nemlig specielt opfyldt når $x, y, z \in S^*$. Videre så vi, at det neutrale element e ligger i S^*, og ligningen (1.2.2) gælder specielt når $x \in S^*$. Og endelig har vi for hvert element $x \in S^*$ bestemt x^{-1} i S^*, så at ligningen (1.2.3) er opfyldt. Følgelig er S^* en gruppe.

(1.6) Undergruppe. For en række af grupperne i de følgende eksempler vil det gælde, at gruppen naturligt er en *undergruppe* af en større gruppe. Hermed menes følgende: Lad der være givet en gruppe $(G, *)$. En delmængde H af G kaldes da en *undergruppe*, hvis følgende betingelse er opfyldt:

(†) Delmængden H er stabil, det neutrale element e ligger i H, og for alle x i H ligger også x^{-1} i H.

Hvis H er en undergruppe, er H specielt en stabil delmængde, og kompositionen i G definerer derfor en komposition i H. Med denne komposition er $(H, *)$ selv en gruppe. Dette følger af, at ligningerne i (1.2) gælder for alle elementer i G og derfor specielt for alle elementer x, y, z i delmængden H.

(1.7) Den trivielle gruppe. Betragt en mængde $G = \{e\}$, der indeholder ét element e. Der er naturligvis præcis én komposition i G, defineret ved $e * e := e$, og det er klart, at med denne komposition er $(G, *)$ en gruppe. Den kaldes den *trivielle gruppe*. Den er øjensynlig kommutativ. I en oplagt forstand er der kun én triviel gruppe, idet kun betegnelsen for det ene element kan variere. Med den multiplikative notation betegnes gruppens eneste element 1, og kompositionen er $1 \cdot 1 = 1$. Med den additive notation betegnes gruppens eneste element 0, og kompositionen er $0 + 0 = 0$. Den trivielle gruppe betegnes ofte C_1.

(1.8) Additive talgrupper. Addition af tal er en fundamental og velkendt komposition. Fx udgør de reelle tal med addition en kommutativ gruppe $\mathbb{R}$, idet betingelserne, i den additive form fra (1.3), er velkendte regler for addition af tal. Når det skal understreges, at vi tænker på systemet af reelle tal som en gruppe med addition, kan vi udførligt skrive $\mathbb{R}^+$ eller $(\mathbb{R}, +)$. Det neutrale element i gruppen $\mathbb{R}^+$ er tallet 0.

De rationale tal med addition udgør en undergruppe $\mathbb{Q}^+$ af $\mathbb{R}^+$, og de hele tal med addition udgør en undergruppe $\mathbb{Z}^+$ af $\mathbb{Q}^+$. Desuden er $\mathbb{R}^+$ en undergruppe af gruppen $\mathbb{C}^+$ af komplekse tal med addition. Systemet $\mathbb{N}$ af naturlige tal er en stabil delmængde af $\mathbb{Z}^+$, men det er ikke en undergruppe, idet tallet 0 ikke tilhører $\mathbb{N}$.

(1.9) Multiplikative talgrupper. Multiplikation er en anden fundamental komposition af reelle tal. Den er som bekendt også kommutativ og associativ, og tallet 1 er neutralt element. Men de reelle tal med multiplikation udgør *ikke* en gruppe, idet tallet 0 ikke har en invers med hensyn til multiplikationen. Som bekendt gælder for to reelle tal x, y forskellige fra 0, at også produktet xy er forskelligt fra 0. Delmængden $\mathbb{R}\backslash\{0\}$ er altså stabil under multiplikation, og vi kan opfatte multiplikation som en komposition i delmængden. Det følger af regnereglerne, at $\mathbb{R}\backslash\{0\}$ med multiplikation er en kommutativ gruppe med tallet 1 som neutralt element. For $x \neq 0$ er det *reciprokke* tal $x^{-1} = 1/x$ det inverse til x. Øjensynlig er tallene forskellige fra 0 netop de invertible mht multiplikation, og gruppen $\mathbb{R}\backslash\{0\}$ betegnes $\mathbb{R}^*$. De positive reelle tal udgør en undergruppe $\mathbb{R}^*_+$ af $\mathbb{R}^*$.

Tilsvarende fås ud fra systemet af rationale tal en multiplikativ gruppe $\mathbb{Q}^* := \mathbb{Q}\backslash\{0\}$ bestående af de rationale tal forskellige fra 0, og fra systemet af komplekse tal fås en multiplikativ gruppe $\mathbb{C}^* := \mathbb{C}\backslash\{0\}$ bestående af de komplekse tal forskellige fra 0. Øjensynlig er $\mathbb{R}^*$ en undergruppe af $\mathbb{C}^*$ og $\mathbb{Q}^*$ er en undergruppe af $\mathbb{R}^*$. De komplekse *enheder*, dvs de komplekse tal u med $|u| = 1$, udgør en undergruppe $\mathbb{U}$ af $\mathbb{C}^*$.

Mængden $\mathbb{Z} \setminus \{0\}$ af hele tal forskellige fra 0 udgør en stabil delmængde af gruppen $\mathbb{Q}^*$, men delmængden er ikke en undergruppe, idet fx det inverse til 2, altså $\frac{1}{2}$, ikke er et helt tal. De eneste hele tal $x \neq 0$, for hvilke det inverse tal x^{-1} igen er et helt tal, er tallene $x = \pm 1$. Det er let at se, at tallene 1 og -1 udgør en undergruppe $\{\pm 1\}$ af $\mathbb{Q}^*$. Gruppen $\{\pm 1\}$ har orden 2. Den betegnes også C_2.

(1.10) Grupper af orden 2. I (1.9) så vi, at tallene ± 1 udgør en gruppe af orden 2. Lad os overveje generelt, hvordan en gruppe $(G, *)$ med to elementer kan se ud. Et af de to elementer i G må være det neutrale element. Lad os betegne det neutrale element l, og lad u være det andet element i G. Da l er neutralt element, får vi af ligningerne (1.2.2), at $l * l = l$, $l * u = u$, og $u * l = u$. Elementet u skal have en invers, og af $u * l = u$ følger specielt, at den inverse til u ikke kan være l. Altså må den inverse til u være u, og følgelig har vi ligningen $u * u = l$. Hermed er kompositionen i G helt bestemt, og givet ved følgende tabel:

$*$	l	u
l	l	u
u	u	l

Analysen viser altså, at der er præcis én gruppe af orden 2 (bortset fra valg af betegnelser for de to elementer). Det er ikke tilfældigt, at betegnelserne l og u for de to elementer er valgt som forbogstaverne i henholdsvis „lige" og „ulige". Tabellen ovenfor svarer jo netop til de regler, der gælder for *paritet*, når man adderer hele tal.

(1.11) Restklassegrupperne. Lad n være et fast naturligt tal. Der er da n restklasser modulo n. Addition af restklasser er kommutativ og associativ, og restklassen $[0]$ er neutralt element for addition. For en given restklasse $[x]$ har vi $[x] + [-x] = [0]$, så restklassen $[-x]$ er den modsatte til $[x]$. Restklasser med addition som komposition udgør derfor en kommutativ gruppe, som vi betegner $\mathbb{Z}/n$ eller $\mathbb{Z}/\mathbb{Z}n$. Gruppens orden, altså antallet af restklasser, er n.

I hver restklasse findes netop ét tal r, som opfylder $0 \leqslant r < n$. De n restklasser er altså klasserne $[0], [1], \dots, [n-1]$. Når n er givet, vil man ofte anvende symbolerne $0, 1, \dots, n-1$ til også at betegne de tilsvarende restklasser.

For $n = 4$ kan restklasserne i $\mathbb{Z}/4$ således betegnes 0, 1, 2, 3. Addition i gruppen $\mathbb{Z}/4$ er så bestemt ved tabellen:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Bemærk, at når vi opfatter 0, 1, 2, 3 som restklasser modulo 4, så har vi ligningerne $-0 = 0$, $-1 = 3$, $-2 = 2$, og $-3 = 1$.

(1.12) Primiske restklasser. Multiplikation af restklasser er en kommutativ og associativ komposition i mængden af restklasser modulo n, og restklassen $[1]$ er neutralt element. Som bekendt er det netop de *primiske restklasser*, der har en invers med hensyn til multiplikation.

De primiske restklasser, dvs restklasser af formen $[r]$, hvor r og n er primiske, udgør altså en multiplikativ gruppe. Denne gruppe betegner vi $(\mathbb{Z}/n)^*$. Dens orden er antallet af tal r med $0 \leqslant r < n$, for hvilke $(r, n) = 1$. Dette antal betegnes $\varphi(n)$. Vi har altså $|(\mathbb{Z}/n)^*| = \varphi(n)$. Funktionen $n \mapsto \varphi(n)$, der er defineret for alle naturlige tal n, kaldes *Euler's φ-funktion*.

For $n = 8$ er det restklasserne svarende til 1, 3, 5, 7, der er de primiske restklasser. Gruppen $(\mathbb{Z}/8)^*$ har altså orden $\varphi(8) = 4$. Multiplikation i gruppen $(\mathbb{Z}/8)^*$ er bestemt ved tabellen,

$\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Bemærk, at enhver af restklasserne 1, 3, 5, 7 modulo 8 har sig selv som den inverse.

(1.13) Enhedsrødder. De komplekse fortegn, altså mængden af komplekse tal z med $|z| = 1$, udgør øjensynlig en undergruppe $\mathbb{U}$ af den multiplikative gruppe $\mathbb{C}^*$. For et givet naturligt tal n er der som bekendt n komplekse tal z, der tilfredsstiller ligningen $z^n = 1$, nemlig tallene $e^{2\pi i a/n}$ for $a = 0, \ldots, n-1$. Disse n komplekse tal kaldes de n'te *enhedsrødder*. Blandt de n'te enhedsrødder har vi specielt tallet 1, svarende til $a = 0$.

De n'te enhedsrødder udgør en undergruppe af $\mathbb{U}$, og dermed en undergruppe af $\mathbb{C}^*$. Hvis nemlig $z^n = 1$ og $w^n = 1$, så finder vi $(zw)^n = z^n w^n = 1 \cdot 1 = 1$. Heraf ses, at de n'te enhedsrødder udgør en stabil delmængde af $\mathbb{C}^*$. Vi har allerede set, at det neutrale element 1 i $\mathbb{C}^*$ er en n'te enhedsrod. Endelig følger af $z^n = 1$, at også $(z^{-1})^n = z^{-n} = 1$. Når z er en n'te enhedsrod, er altså også z^{-1} en n'te enhedsrod.

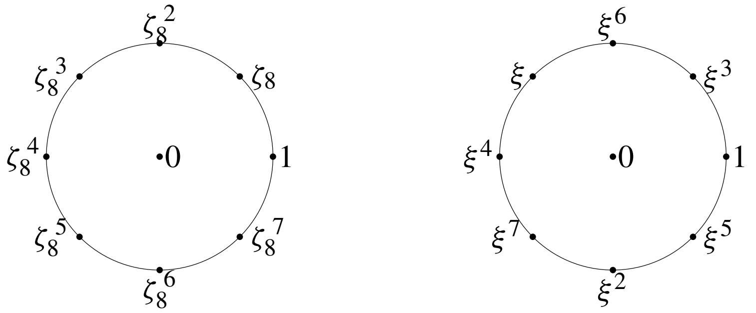
Gruppen af n'te enhedsrødder kaldes den *cykliske gruppe* af orden n, og den betegnes C_n. Blandt de n'te enhedsrødder har vi specielt, for $a = 1$, tallet,

$$\zeta_n := e^{2\pi i/n} = \cos(2\pi/n) + i \sin(2\pi/n),$$

og de n'te enhedsrødder er øjensynlig de n potenser ζ_n^a, for $a = 0, 1, \ldots, n-1$.

Produktet af ζ_n^a og ζ_n^b er potensen ζ_n^{a+b}, og her kan eksponenten $a + b$ erstattes med sin principale rest modulo n, idet $\zeta_n^n = 1$. Multiplikation i gruppen C_n svarer altså til addition modulo n af eksponenterne.

Fx består gruppen C_8 af de 8 første potenser af enhedsroden ζ_8. Bemærk, at C_8 også består af de første 8 potenser af enhedsroden $\xi := \zeta_8^3$.



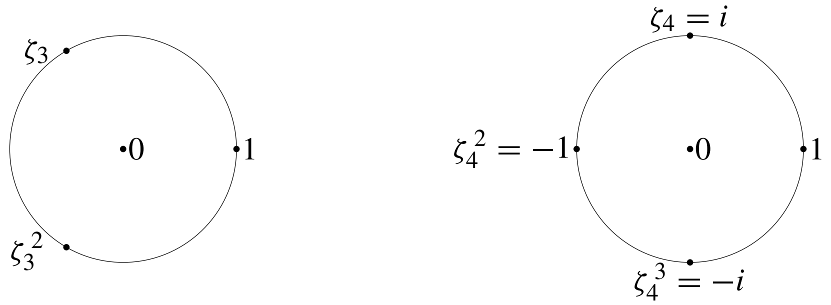
(1.14) Eksempel. For $n = 1$ har vi øjensynlig $\mathrm{C}_1 = \{1\}$. Den cykliske gruppe C_1 er altså den trivielle gruppe, i overensstemmelse med notationen i (1.7). For $n = 2$ har vi $\mathrm{C}_2 = \{\pm 1\}$, i overensstemmelse med notationen i (1.9).

De 3'die enhedsrødder er de tre løsninger til ligningen $z^3 = 1$. Ligningen kan skrives $(z-1)(z^2+z+1) = 0$. Den ene løsning er $z = 1$, og de to andre løsninger er de to rødder i andengradspolynomiet $z^2 + z + 1$, altså tallene

$$-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}\,.$$

Disse tre tal udgør altså gruppen C_3.

Gruppen C_4 består øjensynlig af de fire tal ± 1 og $\pm i$.



(1.15) Vektorrum. Lad V være et reelt vektorrum. Addition af vektorer er så en komposition i mængden V. Det er en del af betingelserne for et vektorrum, at V med denne komposition er en kommutativ gruppe. Specielt gælder, at talrummet $\mathbb{R}^n$ er en kommutativ gruppe. Additionen er koordinatvis addition af n-sæt,

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n).$$

Det er klart, at vi ved en tilsvarende koordinatvis addition får kommutative grupper $\mathbb{Z}^n$, $\mathbb{Q}^n$ og $\mathbb{C}^n$ af n-sæt med henholdsvis hele, rationale, og komplekse koordinater.

(1.16) Permutationsgrupper. Sammensætning af afbildninger er som bekendt associativ: hvis vi kan danne de sammensatte afbildninger $(f \circ g) \circ h$ og $f \circ (g \circ h)$, så er de den samme afbildning, nemlig afbildningen givet ved

$$x \mapsto f(g(h(x))).$$

Det ses specielt, at hvis X er en given mængde, så kan vi opfatte sammensætning af afbildninger som en associativ komposition, $(f, g) \mapsto f \circ g$, i mængden af alle afbildninger af X ind i sig selv. Den *identiske afbildning* id_X, bestemt ved $\mathrm{id}_X(x) = x$ for alle $x \in X$, er neutralt element for denne komposition.

Betragt specielt de bijektive afbildninger af mængden X på sig selv. Hvis $f\colon X \to X$ og $g\colon X \to X$ er bijektive afbildninger, så er den sammensatte afbildning $f \circ g\colon X \to X$ igen bijektiv. Sammensætning kan altså opfattes som en associativ komposition i mængden af bijektive afbildninger. Den identiske afbildning id_X er bijektiv, og den er neutralt element for kompositionen. For enhver bijektiv afbildning $f\colon X \to X$ eksisterer den inverse bijektive afbildning $f^{-1}\colon X \to X$, og vi har ligningerne

$$f(f^{-1}(x)) = x \text{ og } f^{-1}(f(x)) = x.$$

De to ligninger udsiger, at $f \circ f^{-1} = \mathrm{id}_X$ og $f^{-1} \circ f = \mathrm{id}_X$.

Det følger af disse overvejelser, at de bijektive afbildninger af X på sig selv, med sammensætning som komposition, udgør en gruppe med den identiske afbildning id_X som neutralt element. En bijektiv afbildning af X på sig selv kaldes også en *transformation* af X eller en *permutation* af X, og gruppen af bijektive afbildninger kaldes den fulde *transformationsgruppe* eller den fulde *permutationsgruppe* for X. Vi betegner den $\mathrm{Perm}(X)$ eller S_X.

Det er sædvane at skrive permutationsgruppen multiplikativt, altså blot at skrive fg for den sammensatte afbildning $f \circ g$. Den identiske afbildning id_X betegnes også 1_X, eller blot id eller 1.

Alle interessante grupper i matematik er naturligt født som undergrupper af transformationer af en passende mængde X. Som vi senere skal se, gælder der faktisk, at enhver gruppe kan opfattes som en gruppe af transformationer.

(1.17) Additive matrixgrupper. Matricer af samme størrelse kan adderes (pladsvis), og addition er en kommutativ og associativ komposition i mængden af $m \times p$-matricer. Det er klart, at de reelle $m \times p$-matricer udgør en kommutativ gruppe. Vi betegner den $\mathrm{Mat}_{m,p}(\mathbb{R})$, og skriver blot $\mathrm{Mat}_m(\mathbb{R})$ når $p = m$. Det neutrale element for additionen er nul-matricen 0, og den modsatte til en matrix A er matricen $-A$, der fås ved at erstatte alle koefficienter i A med deres modsatte. Tilsvarende har vi additive grupper $\mathrm{Mat}_{m,p}(\mathbb{C})$, $\mathrm{Mat}_{m,p}(\mathbb{Q})$ og $\mathrm{Mat}_{m,p}(\mathbb{Z})$ af matricer med henholdsvis komplekse, rationale, og hele koefficienter.

Disse additive grupper af matricer udgør ikke noget essentielt nyt i forhold til talrummene behandlet i (1.15). En $m \times p$-matrix er jo blot et sæt af mp reelle tal, opskrevet på særlig måde i et rektangulært skema, og addition af matricer svarer til koordinatvis addition. Vi kan altså umiddelbart identificere gruppen $\mathrm{Mat}_{m,p}(\mathbb{R})$ med talrummet $\mathbb{R}^{mp}$, idet opskrivningen i en matrix blot er en særlig måde at skrive mp-sæt på.

(1.18) Den generelle lineære gruppe. Matrixmultiplikation er fra et gruppeteoretisk synspunkt mere interessant. Som bekendt er multiplikationen associativ: hvis vi kan danne matrixprodukterne $(AB)C$ og $A(BC)$, så er de den samme matrix. Specielt kan vi opfatte matrixmultiplikation som en associativ komposition i mængden $\mathrm{Mat}_n(\mathbb{R})$ af kvadratiske $n \times n$-matricer. Enhedsmatricen, betegnet 1_n eller blot 1, er neutralt element for multiplikationen.

En matrix $A \in \mathrm{Mat}_n(\mathbb{R})$ kaldes som bekendt invertibel, hvis der findes en invers matrix, dvs netop når A er invertibel som beskrevet i (1.4). Det følger, at de invertible matricer udgør en multiplikativ gruppe. Denne gruppe kaldes den *generelle lineære gruppe af grad n*, og den betegnes $\mathrm{GL}_n(\mathbb{R})$. Som bekendt består $\mathrm{GL}_n(\mathbb{R})$ af de matricer $A \in \mathrm{Mat}_n(\mathbb{R})$, for hvilke $\det A \neq 0$.

Tilsvarende kan vi definere den komplekse generelle lineære gruppe $\mathrm{GL}_n(\mathbb{C})$ bestående af invertible $n \times n$-matricer med komplekse koefficienter.

Det er klart, at i gruppen $\mathrm{GL}_n(\mathbb{R})$ udgør delmængden bestående af matricer med rationale koefficienter en stabil delmængde. Øjensynlig ligger enhedsmatricen 1_n i delmængden. Hvis en kvadratisk matrix A har rationale koefficienter, så er dens determinant et rationalt tal. Hvis dette tal er forskelligt fra 0, så følger det af de sædvanlige formler for den inverse matrix A^{-1}, at også A^{-1} har rationale koefficienter. Heraf ses, at matricerne med rationale koefficienter udgør en undergruppe $\mathrm{GL}_n(\mathbb{Q})$ af $\mathrm{GL}_n(\mathbb{R})$.

Matricerne i $\mathrm{GL}_n(\mathbb{R})$ med heltalskoefficienter udgør ligeledes en stabil delmængde, der indeholder 1_n. Men for en invertibel matrix A med heltalskoefficienter vil den inverse matrix A^{-1} i almindelighed ikke have heltalskoefficienter. Antag, at A^{-1} har koefficienter i $\mathbb{Z}$. Da er $\det A$ og $\det(A^{-1})$ hele tal, og $\det A \det(A^{-1}) = 1$. Følgelig er $\det A = \pm 1$. Antag omvendt, at $\det A = \pm 1$. Da følger det af de sædvanlige formler for den inverse matrix, at også A^{-1} har hele koefficienter. For en heltalsmatrix A med determinant forskellig fra 0 gælder altså, at den inverse matrix har heltalskoefficienter, hvis og kun hvis $\det A = \pm 1$. Det følger let, at heltalsmatricer med determinant ± 1 udgør en undergruppe i gruppen $\mathrm{GL}_n(\mathbb{R})$. Denne undergruppe betegnes $\mathrm{GL}_n(\mathbb{Z})$.

(1.19) Den specielle lineære gruppe. For kvadratiske $n \times n$-matricer A og B gælder som bekendt ligningen $\det(AB) = \det A \det B$. Matricerne med determinant 1 udgør en delmængde af $\mathrm{GL}_n(\mathbb{R})$. Af ligningen følger let, at delmængden er stabil. Videre har enhedsmatricen determinant 1. Og endelig, hvis A har determinant 1, så har også A^{-1} determinant 1. Heraf ses, at matricerne med determinant 1 udgør en undergruppe af den generelle lineære gruppe $\mathrm{GL}_n(\mathbb{R})$. Denne gruppe kaldes den *specielle lineære gruppe af grad n*, og den betegnes $\mathrm{SL}_n(\mathbb{R})$. Den består altså af de matricer $A \in \mathrm{Mat}_n(\mathbb{R})$, for hvilke $\det A = 1$.

Tilsvarende defineres grupperne $\mathrm{SL}_n(\mathbb{C})$ og $\mathrm{SL}_n(\mathbb{Q})$. Gruppen $\mathrm{SL}_n(\mathbb{Z})$ består af $n \times n$-matricer med heltalskoefficienter og determinant 1. Den er en undergruppe i $\mathrm{GL}_n(\mathbb{Z})$.

(1.20) Den ortogonale gruppe. Betragt vektorrummet $\mathbb{R}^n$ med den sædvanlige (euklidiske) afstand. En afbildning $f : \mathbb{R}^n \to \mathbb{R}^n$ kaldes *ortogonal*, hvis f er afstandsbevarende, dvs en isometri, og lineær. Vi skal senere se nærmere på ortogonale afbildninger. Her vil vi blot bemærke, at de ortogonale afbildninger udgør en undergruppe i den fulde transformationsgruppe for $\mathbb{R}^n$. De lineære afbildninger $\mathbb{R}^n \to \mathbb{R}^n$ har formen $x \mapsto Ax$ med en $n \times n$-matrix A. Matricer A, for hvilke afbildningen $x \mapsto Ax$ er ortogonal, kaldes *ortogonale matricer*. Sammensætning af lineære afbildninger svarer til multiplikation af de tilsvarende matricer. Det følger, at gruppen af ortogonale afbildninger svarer til undergruppen af ortogonale matricer i $\mathrm{GL}_n(\mathbb{R})$. Denne undergruppe kaldes den *ortogonale gruppe af grad n*, og den betegnes $\mathrm{O}_n(\mathbb{R})$ eller blot $\mathrm{O}(n)$. De ortogonale matricer med determinant 1 udgør den *specielle ortogonale* undergruppe $\mathrm{SO}_n(\mathbb{R}) = \mathrm{O}^+(n)$; de beskriver de ortogonale, orienteringsbevarende afbildninger.

For $n = 2$, altså for ortogonale afbildninger i planen $\mathbb{R}^2$, er situationen specielt simpel. Betragt en ortogonal afbildning $f : \mathbb{R}^2 \to \mathbb{R}^2$, svarende til en ortogonal 2×2-matrix,

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Lad (e_1, e_2) være den kanoniske basis for $\mathbb{R}^2$. Vektoren e_i er en enhedsvektor, dvs afstanden mellem nul-vektoren og e_i er lig med 1, og afstanden mellem e_1 og e_2 er lig med $\sqrt{2}$. Den første søjle i A er koordinatsæt for billedvektoren $f(e_1)$. Da f er en isometri, er $f(e_1)$ en enhedsvektor. Altså er $a^2 + b^2 = 1$, og følgelig findes et tal θ således, at $(a, b) = (\cos\theta, \sin\theta)$. Tilsvarende er $f(e_2)$ en enhedsvektor. Videre er afstanden mellem $f(e_1)$ og $f(e_2)$ lig med $\sqrt{2}$. Det følger, at $f(e_2)$ er en enhedsvektor vinkelret på $f(e_1)$. Altså er $(c, d) = (-b, a)$ eller $(c, d) = (b, -a)$. Matricen A har derfor en af følgende to former:

$$D_\theta := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \qquad S_\theta := \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

De to former har, henholdsvis, determinant 1 og -1. Det er altså matricerne af den første form, der udgør den specielle ortogonale gruppe $\mathrm{SO}_2(\mathbb{R})$. Matricen D_θ af den første form beskriver en *drejning* med vinklen θ omkring nul-vektoren.

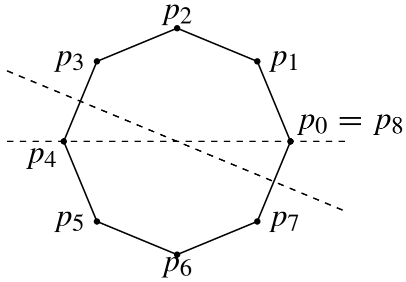
Matricen S_θ af den anden form beskriver en *spejling* i linien bestemt ved enhedsvektoren $e := (\cos\frac{1}{2}\theta, \sin\frac{1}{2}\theta)$. Linien kaldes *spejlingsaksen*. Vektoren e er egenvektor for S_θ med egenværdien 1 og *tværvektoren* $\hat{e} := (-\sin\frac{1}{2}\theta, \cos\frac{1}{2}\theta)$ er egenvektor hørende til egenværdien -1. I basen $(e, \hat{e})$ beskrives afbildningen derfor ved matricen,

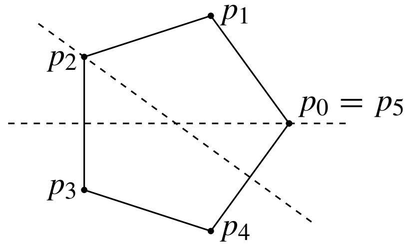
$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Det tilsvarende resultat er $\mathbb{R}^3$ er følgende: *Matricerne i* $\mathrm{SO}_3(\mathbb{R})$ *beskriver rotationerne omkring en linie gennem nul-vektorern i* $\mathbb{R}^3$.

(1.21) Diedergruppen. Betragt, for $n \geqslant 3$, en *regulær n-kant* i planen, fx bestemt ved at de n hjørner p_j er de n vektorer med koordinater $(\cos 2j\pi/n, \sin 2j\pi/n)$ for $j = 1, 2, \dots, n$. Det er naturligt at regne indices modulo n. Specielt er $p_0 = p_n$.

Ved en *symmetri* af n-kanten forstås en ortogonal afbildning af planen, som afbilder mængden $\{p_1, \dots, p_n\}$ af hjørner på sig selv. Det er klart, at n-kantens symmetrier udgør en undergruppe i gruppen af ortogonale afbildninger. Denne gruppe af symmetrier svarer til en undergruppe af ortogonale matricer i $\mathrm{O}(2)$. Gruppen af symmetrier af n-kanten kaldes *diedergruppen* af grad n, og den betegnes D_n.





Vi kan umiddelbart bestemme $2n$ symmetrier i gruppen D_n. For det første er det klart, at de n drejninger med vinkler $2j\pi/n$ for $j = 0, 1, \dots, n-1$ er symmetrier af n-kanten. For det

andet er det klart, at enhver spejling i en akse, der enten går gennem nul-vektoren og et hjørne eller gennem nul-vektoren og midtpunktet af en kant, er en symmetri af n-kanten. Hvis n er ulige, så går hver akse gennem et hjørne også gennem midtpunktet af den modstående kant; der er altså lige så mange akser som hjørner, dvs n spejlingsakser. Hvis n er lige, så går hver akse gennem et hjørne også gennem det modstående hjørne og hver akse gennem midtpunktet af en kant går gennem midtpunktet af den modstående kant; antallet af spejlingsakser er altså $n/2 + n/2 = n$.
Både når n er lige og ulige er der således bestemt n drejninger (heriblandt den identiske afbildning) og n spejlinger i symmetrigruppen D_n. Disse i alt $2n$ symmetrier udgør hele diedergruppen D_n. Lad nemlig $f : \mathbb{R}^2 \to \mathbb{R}^2$ være en symmetri af n-kanten. De to vektorer p_0 og p_1 udgør en basis for vektorrummet $\mathbb{R}^2$. Da f er lineær, er f helt bestemt ved de to billedvektorer $f(p_0)$ og $f(p_1)$. Billedvektoren $f(p_0)$ skal være et af de n hjørner p_j, så der er n muligheder for $f(p_0)$. Da f er en isometri, må $f(p_1)$ være et af de to nabohjørner til p_j. For hver af de n muligheder for $f(p_0)$ er der derfor 2 muligheder for $f(p_1)$. Der er følgelig højst $2n$ mulige symmetrier af n-kanten.

Det følger, at diedergruppen D_n består af de n drejninger og de n spejlinger. Specielt har diedergruppen D_n orden $2n$.

En oversigt over de $2n$ symmetrier af n-kanten kan fås som følger. Lad S være spejlingen i førsteaksen (bestemt ved enhedsvektoren p_0), og lad D betegne drejningen med vinklen $2\pi/n$. Da består diedergruppen af de $2n$ symmetrier i listen,

$$\mathrm{id} = D^0, D^1, \dots, D^{n-1}, S, DS, \dots, D^{n-1}S. \tag{1.21.1}$$

Yderligere gælder for D og S ligningerne,

$$D^n = \mathrm{id}, \quad S^2 = \mathrm{id}, \quad SD = D^{-1}S. \tag{1.21.2}$$

Lad nemlig f være en symmetri af n-kanten. Billedet af p_0 er da et af de n hjørner, så vi har $f(p_0) = p_i$ hvor $0 \leqslant i < n$. Billedet af p_1 er så et af de to nabohjørner p_{i+1} og p_{i-1}, idet p_j naturligt defineres for alle hele tal j ved at regne modulo n. I det første tilfælde har vi de to ligninger $f(p_0) = p_i$ og $f(p_1) = p_{i+1}$. De samme ligninger gælder øjensynlig for afbildningen D^i. Følgelig er $f = D^i$, idet begge afbildninger er lineære. I det andet tilfælde har vi de to ligninger $f(p_0) = p_i$ og $f(p_1) = p_{i-1}$. De samme ligninger gælder for afbildningen D^iS, idet $S(p_0) = p_0$ og $S(p_1) = p_{-1}$. Det følger som før, at $f = D^iS$. Hermed er bevist, at enhver symmetri f i D_n er lig med en af symmetrierne i listen (1.21.1). Da der er $2n$ symmetrier i D_n, og $2n$ symmetrier i listen, må symmetrierne i listen netop være de $2n$ forskellige symmetrier i D_n.

De to første ligninger i (1.21.2) er oplagte. Den tredie ligning indses ved at bemærke, at de to sider af ligningen er lineære afbildninger. De afbilder begge p_0 på p_{n-1} og p_{n-1} på p_0, og følgelig er de to afbildninger ens.

Bemærk, at ligningerne (1.21.2) tillader os at „regne“ i gruppen D_n uden at tænke på at gruppens elementer er symmetrier af n-kanten. To elementer i gruppen er to elementer i listen

(1.21.1). At bestemme deres produkt er at afgøre hvor i listen produktet befinder sig. Fx finder vi, for $n = 4$, at

$$(DS)(D^2S) = DSDDS = DD^{-1}SDS = DD^{-1}D^{-1}SS = D^{-1} = D^3.$$

I det foregående er antaget, at $n \geqslant 3$. Definitionen af diedergruppen D_n som gruppen af ortogonale afbildninger, der afbilder mængden af de n hjørner på sig selv, har imidlertid god mening også for $n = 1$ og $n = 2$. For $n = 1$ er der kun ét hjørne p_0, og p_0 er enhedsvektoren e_1 med koordinater $(1, 0)$. En symmetri skal afbilde dette ene hjørne på sig selv. Symmetrien må derfor enten være den identiske afbildning eller spejlingen i linien bestemt ved enhedsvektoren e_1. Diedergruppen D_1 består altså af den identiske afbildning og denne spejling.

For $n = 2$ er der 2 hjørner, e_1 og $-e_1$. En symmetri må derfor enten afbilde e_1 på e_1 (og dermed $-e_1$ på $-e_1$), eller den må ombytte e_1 og $-e_1$. I det første tilfælde må symmetrien være en af de to symmetrier i D_1, altså enten den identiske afbildning eller spejlingen i linien bestemt ved vektoren e_1. I det andet tilfælde må symmetrien enten være halvdrejningen, dvs drejningen med vinklen π, eller spejlingen i linien vinkelret på e_1, dvs spejlingen i linien bestemt ved vektoren e_2. Diedergruppen D_2 består altså af identiteten, halvdrejningen, og spejlingerne i de to koordinatakser, dvs linierne bestemt ved vektorerne e_1 og e_2.

Det ses, at diedergruppen D_n i alle tilfælde har orden $2n$.

(1.22) Kvaterniongruppen. Betragt de 4 komplekse 2×2-matricer:

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{i} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \mathbf{j} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Matricerne har alle determinant 1. En let udregning viser ligningerne,

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}, \quad \mathbf{i}\,\mathbf{j} = \mathbf{k}.$$

Heraf følger let, at

$$-\mathbf{j}\,\mathbf{i} = \mathbf{k}, \quad \mathbf{j}\,\mathbf{k} = -\mathbf{k}\,\mathbf{j} = \mathbf{i}, \quad \mathbf{k}\,\mathbf{i} = -\mathbf{i}\,\mathbf{k} = \mathbf{j}.$$

Fx følger ligningen $-\mathbf{j}\,\mathbf{i} = \mathbf{k}$ ved at transponere ligningen $\mathbf{i}\,\mathbf{j} = \mathbf{k}$, og de resterende følger ved multiplikation af de foregående med $\mathbf{i}$ eller $\mathbf{j}$. Matricen $\mathbf{1}$ er blot enhedsmatrix. Specielt er $\mathbf{1}^2 = (-\mathbf{1})^2 = \mathbf{1}$, og $\mathbf{1}$ og $-\mathbf{1}$ kommuterer med alle matricer.

Lad nu Q være mængden bestående af de 8 matricer $\pm\mathbf{1}$, $\pm\mathbf{i}$, $\pm\mathbf{j}$, $\pm\mathbf{k}$. Af de viste ligninger fremgår, at et produkt af 2 matricer i Q igen er en matrix i Q. Matrixmultiplikation er associativ, og enhedsmatricen $\mathbf{1}$ tilhører Q. De to matricer $\pm\mathbf{1}$ er deres egen inverse, og det fremgår af de viste ligninger, at for hver af de øvrige 6 matricer $\mathbf{x}$ i Q gælder $\mathbf{x}^{-1} = -\mathbf{x} \in Q$. Mængden Q af de 8 matricer er derfor en undergruppe af $\mathrm{GL}_2(\mathbb{C})$. Den kaldes *kvaterniongruppen*, og betegnes Q_8.

(1.23) Opgaver.

1. Vis, at $a * b := a + b - ab$ er en komposition i mængden $G := \mathbb{R}\backslash\{1\}$. Vis, at $(G, *)$ er en kommutativ gruppe.

2. Lad $\mathcal{P}(X)$ være mængden af delmængder af X. Vis, at med kompositionen $A + B := (A \cup B) \setminus (A \cap B)$ er $(\mathcal{P}(X), +)$ en kommutativ gruppe. Hvad er det neutrale element? Og det modsatte $-A$ til A? Beskriv, når $A \subseteq B$, mængden $B - A$.

3. En (multiplikativ) gruppe har tre elementer e, a, b, hvor e er det neutrale element. Beskriv kompositionen.

4. Lad G være en endelig gruppe, og lad $H \subseteq G$ være en ikke-tom, stabil delmængde. Vis, at H er en undergruppe.

5. Ved *gruppetavlen*, også kaldet *Cayley-tabellen*, for en endelig gruppe G forstås det kvadratiske skema, der på plads (i, j) har produktet af gruppens i'te og j'te element (i en given rækkefølge af gruppens elementer). Vis, at gruppetavlen i hver række og hver søjle indeholder samtlige gruppens elementer. Bestem gruppetavlen for den additive gruppe $\mathbb{Z}/6$ og for den multiplikative gruppe $(\mathbb{Z}/9)^*$.

6. Vis, at $\mathrm{C}_d \subseteq \mathrm{C}_n$, hvis og kun hvis d er divisor i n.

7. Vis, at et underrum i et vektorrum V er en undergruppe, når vektorrummet opfattes som additiv gruppe. Er enhver undergruppe af V et underrum?

8. En matrix A kaldes en *skalarmatrix*, hvis A er en (kvadratisk) diagonalmatrix og alle diagonalelementerne er ens. Vis, at skalarmatricerne forskellige fra nul-matricen udgør en undergruppe af $\mathrm{GL}_n(\mathbb{R})$.

9. I $\mathbb{R}^3$ med de 3 koordinatakser betegnes med δ_i drejningen med vinklen π omkring den i'te koordinatakse. Angiv matricerne, der beskriver de tre drejninger. Vis, at sammensætning af to forskellige af disse drejninger altid er den tredie, eller, ækvivalent, at produkt af to forskellige af matricerne altid er lig med den tredie. Slut heraf, at de tre matricer og enhedsmatricen udgør en undergruppe af orden 4 i den ortogonale gruppe $\mathrm{O}_3(\mathbb{R})$. Den kaldes *Klein's Vierer-gruppe*.

10. Vis, at gruppen D_3 ikke er kommutativ. Vis, at gruppen $\mathrm{SL}_2(\mathbb{R})$ ikke er kommutativ.

11. Bestem gruppetavlen for diedergruppen D_4, idet de 8 elementer skrives i rækkefølgen id, D, D^2, D^3, S, DS, D^2S, D^3S, jfr (1.21).

12. Lad G være en gruppe, og lad H være delmængden bestående af de elementer h for hvilke $gh = hg$ for alle $g \in G$. Vis, at H er en undergruppe af G. Den kaldes G's *centrum*.

13. Antag for alle elementer g i gruppen G, at $g^2 = e$. Vis, at G er kommutativ.

14. Vis, at hvis d er divisor i n, så er D_d en undergruppe af D_n.

15. Vis, at mængden $\mathrm{UT}_n(\mathbb{R})$ af *uni-triangulære* $n \times n$-matricer, dvs matricer der har 0 under diagonalen og 1 i diagonalen, er en undergruppe af $\mathrm{SL}_n(\mathbb{R})$. Vis, at $\mathrm{UT}_n(\mathbb{R})$ er kommutativ for $n = 2$ og ikke-kommutativ for $n \geqslant 3$. Den kaldes *Heisenberg-gruppen*, når $n = 3$.

16. Lad H være en delmængde af en gruppe G. Vis, at H er en undergruppe, hvis og kun hvis H ikke er tom og $hk^{-1} \in H$ for alle $h, k \in H$.

17. Lad $G = \mathrm{Perm}(\mathbb{C})$ være den fulde permutationsgruppe for $\mathbb{C}$, altså gruppen af alle bijektive afbildninger af $\mathbb{C}$ på sig selv. Idet n er et givet naturligt tal ligger afbildningerne $\delta(z) := e^{2\pi i/n}z$ og $\sigma(z) := \overline{z}$ i G. Vis, at de $2n$ afbildninger: id, $\delta, \dots, \delta^{n-1}, \sigma, \delta\sigma, \dots, \delta^{n-1}\sigma$ udgør en undergruppe af G.

18. For en matrix $A \in \mathrm{Mat}_n(\mathbb{C})$ betegnes med A^* den komplekst konjugerede af den transponerede til A (den *Hermitisk konjugerede* eller den *adjungerede matrix*). Lad $\mathrm{U}_n(\mathbb{C})$ betegne mængden af matricer A for hvilke $AA^* = 1_n$. Vis, at $\mathrm{U}_n(\mathbb{C})$ er en undergruppe af $\mathrm{GL}_n(\mathbb{C})$. Gruppen $\mathrm{U}_n(\mathbb{C})$ kaldes den *unitære gruppe* af grad n.

19. For en delmængde M af en gruppe G betegnes med $\langle M \rangle$ delmængden bestående af alle produkter $g_1 \cdots g_r$ (med $r \geqslant 0$ faktorer), hvor der for hver faktor g_i gælder $g_i \in M$ eller $g_i^{-1} \in M$. Vis, at $\langle M \rangle$ er en undergruppe af G (Du må gerne antage, at $M \neq \emptyset$). Den kaldes den af delmængden M *frembragte undergruppe*.

20. Vis, fx ved hjælp af gruppetavler, at der er præcis 2 grupper af orden 4.

21. *Vis, at en ikke-tom mængde G med en associativ komposition '$*$' er en gruppe, hvis og kun hvis der for alle $a, b \in G$ gælder, at ligningerne $a * x = b$ og $y * a = b$ har løsninger $x, y \in G$.

22. *Antag, at G er en mængde med en associativ komposition '$*$', som har et *venstreneutralt* element e, dvs $e * x = x$ for alle $x \in G$. Vis, at hvis hvert element $x \in G$ har et *venstreinverst* x', dvs $x' * x = e$, så er G en gruppe.

Vis, at hvis hvert element x har et *højreinverst* x', dvs $x * x' = e$, så er G ikke nødvendigvis en gruppe.

Vis, at hvis man ud over eksistensen af højreinverse elementer antager følgende: Af $a * x = b * x$ for alle x følger $a = b$, så er G en gruppe.

2. Permutationer.

(2.1) Indledning. Lad X være en mængde. En bijektiv afbildning $\sigma\colon X \to X$, af X på sig selv, kaldes som nævnt i (1.16) en *transformation* eller en *permutation* af X. Med sammensætning som komposition udgør disse bijektive afbildninger en gruppe, kaldet den fulde *transformations-* eller *permutationsgruppe* for X, betegnet $\mathrm{Perm}(X)$ eller S_X.

Komposition i gruppen S_X er sammensætning. Vi skriver altid kompositionen *multiplikativt*, dvs vi skriver $\sigma\tau$ for den sammensatte afbildning $\sigma \circ \tau$. Det neutrale element i gruppen S_X er den identiske afbildning $\mathrm{id} = \mathrm{id}_X$, kaldet *identiteten*, bestemt ved $\mathrm{id}(x) = x$ for alle $x \in X$.

I dette kapitel vil vi udelukkende betragte tilfældet, hvor X er en endelig mængde. De bijektive afbildninger af X på sig selv vil blive kaldt permutationer. Grupper af permutationer, dvs undergrupper af gruppen S_X for en given endelig mængde X, var blandt de først betragtede grupper. De spiller en vigtig rolle, både i den abstrakte gruppeteori og i en række kombinatoriske anvendelser. Vi gennemgår en række begreber knyttet til permutationsgruppen S_X, herunder permutationers cykelfremstilling, og fortegn.

Når X er mængden $\{1, \dots, n\}$, bruger vi altid betegnelsen S_n for permutationsgruppen. Gruppen S_n kaldes den *symmetriske gruppe af grad n*. Den består af alle permutationer af mængden $\{1, \dots, n\}$. For en permutation σ i S_n er der n muligheder for billedet $\sigma(1)$, herefter er der $n-1$ muligheder for billedet $\sigma(2)$, og $n-2$ muligheder for billedet $\sigma(3)$, osv. Der er således i alt $n!$ permutationer. Den symmetriske gruppe S_n har altså orden $n!$.

I almindelighed, når X er en endelig mængde med n elementer, kan vi nummerere elementerne i X, altså skrive $X = \{x_1, \dots, x_n\}$. Efter en sådan fast nummerering kan vi identificere elementerne i X med tallene $1, 2, \dots, n$, idet tallet i svarer til elementet x_i i X. Under denne identifikation er det klart, at permutationer af X svarer til permutationer af mængden $\{1, 2, \dots, n\}$. Permutationsgruppen S_X kan herefter identificeres med den symmetriske gruppe S_n.

(2.2) Tabelnotation. Hvis X har n elementer, kan en permutation σ af X angives ved en tabel med to rækker, hvor den øverste række indeholder samtlige n elementer i X og hvert element i nederste række er billede af det element, der står oven over i øverste række. Permutationen,

$$\sigma = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ y_1 & y_2 & \dots & y_n \end{pmatrix}, \tag{2.2.1}$$

er altså den bijektive afbildning σ bestemt ved at $\sigma(x_i) = y_i$ for $i = 1, \dots, n$. Bemærk, at *tabelnotationen* kun fastlægger en permutation, når elementerne i begge rækker er samtlige n elementer i X.

Er X for eksempel en mængde med 2 elementer, $X = \{a, b\}$, er der præcis 2 permutationer af X, nemlig

$$\mathrm{id} = \begin{pmatrix} a & b \\ a & b \end{pmatrix} \text{ og } \tau = \begin{pmatrix} a & b \\ b & a \end{pmatrix}.$$

Hvis X har 3 elementer, $X = \{a, b, c\}$, har vi 6 permutationer,

$$\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}.$$

Rækkefølgen af søjlerne i matricen er underordnet. Fx har vi i den symmetriske gruppe S_8 ligningen,

$$\sigma = \begin{pmatrix} 4 & 7 & 2 & 5 & 8 & 3 & 6 & 1 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 2 & 5 & 8 & 3 & 6 & 1 \end{pmatrix}, \tag{2.2.2}$$

idet begge matricer fastlægger permutationen $\sigma \in S_8$ bestemt ved $\sigma(1) = 4$, $\sigma(2) = 7$, $\sigma(3) = 2$, $\sigma(4) = 5$, $\sigma(5) = 8$, $\sigma(6) = 3$, $\sigma(7) = 6$, $\sigma(8) = 1$.

Når en permutation σ er beskrevet ved matricen (2.2.1), fås en tabel for den inverse permutation σ^{-1} blot ved at ombytte første og anden række. Når $\sigma(x_i) = y_i$ har vi nemlig $\sigma^{-1}(y_i) = x_i$. Fx finder vi for permutationen i (2.2.2), at den inverse er bestemt ved ligningen,

$$\sigma^{-1} = \begin{pmatrix} 4 & 7 & 2 & 5 & 8 & 3 & 6 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 6 & 1 & 4 & 7 & 2 & 5 \end{pmatrix}.$$

Ved et produkt $\tau\sigma$ af to permutationer er det bekvemt at ordne matricen for τ således, at dens øverste række er den nederste række for σ. En tabel for $\tau\sigma$ fås så ved øverst at tage den første række i matricen for σ og nederst den anden række i matricen for τ. Med andre ord har vi ligningen,

$$\tau\sigma = \begin{pmatrix} y_1 & y_2 & \dots & y_n \\ z_1 & z_2 & \dots & z_n \end{pmatrix} \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ y_1 & y_2 & \dots & y_n \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ z_1 & z_2 & \dots & z_n \end{pmatrix},$$

idet τ er bestemt ved $\tau(y_i) = z_i$.

Fx bestemmer de to matricer i (2.2.2) den samme permutation σ i S_8. Den øverste række i den første tabel er den nederste række i den anden tabel. Det er herefter umiddelbart at opskrive en tabel for σ^2:

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

(2.3) Observation. To permutationer σ og τ af X siges at *kommutere*, hvis $\sigma\tau = \tau\sigma$. I almindelighed vil permutationer *ikke* kommutere. Gruppen af permutationer er altså i almindelighed ikke en kommutativ gruppe.

Antag for eksempel, at X indeholder 3 elementer, $X = \{a, b, c\}$, og betragt permutationerne,

$$\sigma = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \text{ og } \tau = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}.$$

Her er $\sigma\tau \neq \tau\sigma$, idet

$$\sigma\tau = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \qquad \tau\sigma = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}.$$

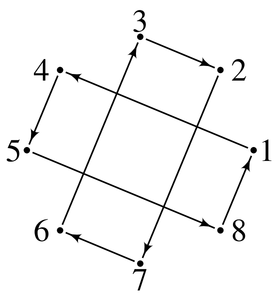
Det er let at vise, essentielt ved det samme argument, at permutationsgruppen S_X er ikke-kommutativ, når blot X indeholder mindst 3 elementer. Når X indeholder præcis to elementer, har vi set i (2.2), at S_X er en gruppe af orden 2, og den er derfor kommutativ. Hvis X kun indeholder ét element, er identiteten naturligvis den eneste afbildning af X ind i sig selv, og S_X er altså den trivielle gruppe.

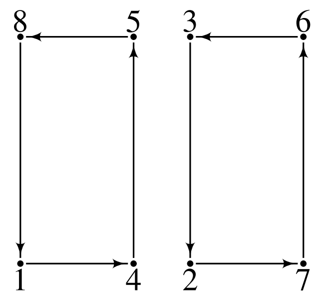
Bemærk, at også for $X = \emptyset$ gælder, at identiteten er den eneste afbildning af X ind i sig selv. For den tomme mængde er permutationsgruppen $\mathrm{S}_\emptyset$ altså også den trivielle gruppe.

(2.4) Direkte notation. Når mængden X består af tallene $1, 2, \dots, n$ er det af og til bekvemt at bruge den *direkte notation*. En afbildning $\sigma\colon \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ kan opfattes som et n-sæt $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n)$, hvor hvert $\sigma_i = \sigma(i)$ er et af tallene $1, 2, \dots, n$. Et sådant n-sæt definerer en permutation i gruppen S_n, når tallene σ_i er forskellige.

Fx kan permutationen σ i S_8 bestemt ved matricerne i (2.2.2) i den direkte notation angives som $\sigma = (4, 7, 2, 5, 8, 3, 6, 1)$ og identiteten i S_8 kan angives som $\mathrm{id} = (1, 2, 3, 4, 5, 6, 7, 8)$.

(2.5) Notation. Et *grafisk billede* af permutationer kan fås på følgende måde: De n elementer i X afsættes som n forskellige punkter i planen $\mathbb{R}^2$. En given permutation σ af X kan så anskueliggøres ved at der for hvert punkt x i X tegnes en pil fra punktet til billedpunktet $\sigma(x)$. Hvis $\sigma(x) = x$, kan pilen undværes, eller afsættes som en cirkulær pil, der begynder og slutter i x. Fx kan permutationen i (2.2.2) anskueliggøres ved et af billederne,

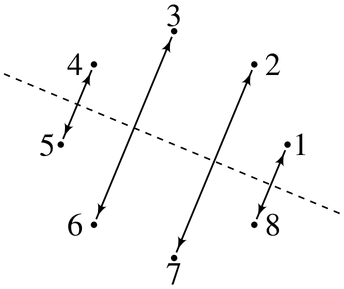




(2.6) Eksempel. Visse permutationer kan angives ved regneudtryk. Fx defineres for et givet tal n en permutation ω i S_n ved forskriften $\omega(i) = n - i + 1$, for $i = 1, \dots, n$. Med tabelnotationen fra (2.2) og den direkte notation fra (2.4) har vi,

$$\omega = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ n & n-1 & \dots & 2 & 1 \end{pmatrix} = (n, n-1, \dots, 2, 1).$$

Hvis de n tal $1, 2, \dots, n$ opfattes som hjørnerne i en regulær n-kant, så kan permutationen ω anskueliggøres som den symmetri af n-kanten, der fås ved spejling i linien gennem nulvektoren og midtpunktet af kanten, der forbinder det første hjørne 1 med det sidste hjørne n. Fx, for $n = 8$,



(2.7) Eksempel. Modulo n gælder, at restklasserne af tallene $1, 2, \dots, n$ netop er samtlige restklasser. I forbindelse med permutationer vil vi altid, når n er givet, identificere tallene $1, 2, \dots, n$ med deres restklasser modulo n. Under identifikationen er restklassen af n lig med nul-elementet i gruppen $\mathbb{Z}/n$. Med denne identifikation kan vi opfatte permutationer af mængden $\mathbb{Z}/n$ som permutationer i den symmetriske gruppe S_n.

Under identifikationen kan vi fx for hvert helt tal a betragte translationen $\rho_a : x \mapsto x + a$, hvor der regnes modulo n. Den er en bijektiv afbildning af mængden af restklasser $\mathbb{Z}/n$, idet den inverse afbildning er translationen ρ_{-a}. Følgelig kan ρ_a opfattes som permutation i gruppen S_n. For $a = 1$ har vi i den direkte notation, at $\rho_1 = (2, 3, \dots, n-1, n, 1)$.

Som et andet eksempel kan vi modulo 8 betragte afbildningen $x \mapsto 3x + 1$. Den er sammensat af afbildningen $x \mapsto 3x$, som er bijektiv da 3 er primisk med 8, og translationen $y \mapsto y + 1$, som altid er bijektiv. Afbildningen $x \mapsto 3x + 1$ er altså en permutation af $\mathbb{Z}/8$, og dermed en permutation i S_8. Det er let at se, at $x \mapsto 3x + 1$ som permutation i S_8 netop er permutationen i (2.2.2).

(2.8) Definition. Lad σ være en permutation af X. Et element $x \in X$ vil da enten blive *flyttet* af σ, dvs opfylde $\sigma(x) \neq x$, eller også vil det være *fixpunkt* for σ, dvs opfylde $\sigma(x) = x$.

To permutationer σ og μ af X kaldes *disjunkte*, hvis mængden af elementer, der flyttes af σ, er disjunkt med mængden af elementer, der flyttes af μ. Ækvivalent er betingelsen, at hvert element i X er fixpunkt for mindst en af permutationerne σ og μ.

Lad os vise, at disjunkte permutationer kommuterer. Hertil bemærkes først, at hvis x flyttes af en permutation σ, så flyttes også $\sigma(x)$ af σ. Da σ er en injektiv afbildning, følger det nemlig af $\sigma(x) \neq x$, at $\sigma^2(x) \neq \sigma(x)$.

Antag nu, at σ og μ er disjunkte. Det skal vises, at $\sigma\mu = \mu\sigma$, altså at der for alle $x \in X$ gælder ligningen,

$$\sigma(\mu(x)) = \mu(\sigma(x)). \tag{1}$$

Betragt et givet element x. Ifølge antagelsen er x fixpunkt for en af de to permutationer. Vi kan antage, at x er fixpunkt for μ. Hvis x også er fixpunkt for σ, er ligningen (1) opfyldt: begge sider er lig med x. Antag derfor, at x flyttes af σ. Som nævnt ovenfor gælder så, at også $\sigma(x)$ flyttes af σ. Elementet $\sigma(x)$ er altså ikke fixpunkt for σ. Af antagelserne følger så, at $\sigma(x)$ må være fixpunkt for μ. Herefter er ligningen (1) igen opfyldt: begge sider er lig med $\sigma(x)$.

(2.9) Cykler. Lad der være givet p forskellige elementer $a_1, \dots, a_p$ i X. Vi kan da definere en permutation γ af X ved ligningerne,

$$\gamma(a_1) = a_2, \quad \gamma(a_2) = a_3, \quad \dots, \quad \gamma(a_{p-1}) = a_p, \quad \gamma(a_p) = a_1 \quad \text{og}$$
$$\gamma(x) = x, \ \text{ når } x \notin \{a_1, \dots, a_p\}.$$

En permutation af denne form kaldes en *p-cykel* eller en *cykel af længde p*.

For p-cyklen γ beskrevet ovenfor bruger vi altid den såkaldte *cykelnotation*,

$$\gamma = (a_1 \ \dots \ a_p),$$

hvor vi ikke har sat komma mellem elementerne for at undgå forveksling med den direkte notation.

Bemærk, at definitionen også har mening for $p = 1$. Er der givet ét element a_1 reduceres ligningerne til $\gamma(a_1) = a_1$ og $\gamma(x) = x$ for $x \neq a_1$. Ligningerne fastlægger altså identiteten. I cykelnotationen betegner (a_1) altså den identiske afbildning, og den er en 1-cykel.

I cykelnotationen kan hvert af de p elementer a_i optræde på førstepladsen, idet vi øjensynlig har ligningen,

$$\gamma = (a_1\, a_2 \ \dots \ a_p) = (a_i\, a_{i+1} \ \dots \ a_p\, a_1 \ \dots \ a_{i-1}). \tag{2.9.1}$$

Den inverse til en p-cykel er igen en p-cykel, idet vi har ligningen,

$$(a_1\, a_2 \ \dots \ a_p)^{-1} = (a_p\, a_{p-1} \ \dots \ a_1). \tag{2.9.2}$$

En cykel af længde 2 kaldes også en *transposition*. En transposition $\tau = (a_1\, a_2)$ ombytter altså a_1 og a_2 og har alle resterende elementer i X som fixpunkter. En transposition er sin egen inverse: $(a_1\, a_2) = (a_2\, a_1)$, idet begge transpositioner ombytter a_1 og a_2.

En p-cykel er et produkt af $p - 1$ transpositioner, idet der gælder ligningen,

$$(a_1 \ \dots \ a_p) = (a_1\, a_p)(a_1\, a_{p-1}) \cdots (a_1\, a_2). \tag{2.9.3}$$

Lad os understrege at ligningen (2.9.3), såvel som en række af de følgende ligninger, er en ligning mellem (bijektive) afbildninger af X ind i sig selv. Det er påstanden, at ligningens to sider er den samme afbildning, altså at de to sider har samme værdi for ethvert element x i X. Højresiden er produktet $\tau_p \cdots \tau_2$ af de $p - 1$ transpositioner $\tau_j := (a_1\, a_j)$ for $j = 2, \dots, p$. Betragt værdien i x. Antag først, at x ikke er et af elementerne a_i. Da er x fixpunkt for cyklen på venstresiden. På højresiden er x fixpunkt for alle transpositionerne τ_j, og dermed også for produktet. Altså har begge sider værdien x i x. Antag dernæst, at $x = a_i$, hvor $i < p$. Venstresidens værdi i x er da a_{i+1}. På højresiden er $x = a_i$ fixpunkt for transpositionerne $\tau_2, \dots, \tau_{i-1}$. Videre er $\tau_i(x) = a_1$ og $\tau_{i+1}(a_1) = a_{i+1}$. Endelig er a_{i+1} fixpunkt for transpositionerne $\tau_{i+2}, \dots, \tau_p$. Højresidens værdi i x er altså ligeledes a_{i+1}. Antag endelig, at $x = a_p$. Venstresidens værdi i x er da a_1. På højresiden er $x = a_p$ fixpunkt for transpositionerne $\tau_2, \dots, \tau_{p-1}$, og $\tau_p(x) = a_1$. Højresidens værdi i x er derfor også lig med a_1. Det er således vist, at de to sider af (2.9.3) har samme værdi i ethvert element x af X. Altså gælder ligningen (2.9.3).

(2.10) Eksempel. Bemærk, at det kun er de elementer, der flyttes af p-cyklen γ, der indgår i notationen; de øvrige elementer i X er fixpunkter for γ. Specielt skal det altid af sammenhængen fremgå, hvilken mængde, der er X. Fx betegner 3-cyklen $(1\,2\,3)$ den permutation i

S_3, der er bestemt ved $1 \mapsto 2$, $2 \mapsto 3$, og $3 \mapsto 1$, men den samme betegnelse definerer den tilsvarende permutation i S_4, der har 4 som fixpunkt. Som permutation i S_4 har vi ligningen,

$$(1\,2\,3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}.$$

(2.11) Definition. Lad σ være en given permutation af den endelige mængde X. For hvert element $a \in X$ kan vi betragte følgen af billeder: $a_1 := a$, $a_2 := \sigma(a_1)$, og, induktivt, $a_{i+1} = \sigma(a_i)$. Delmængden,

$$B_a = B_a(\sigma) := \{a_1, a_2, \dots\},$$

kaldes *banen* bestemt ved a. Da X er endelig, har følgen $a_1, a_2, \dots$ gentagelser. Der findes derfor et entydigt bestemt naturligt tal p således, at elementerne $a_1, \dots, a_p$ er forskellige og $a_{p+1} = a_q$ med $1 \leqslant q \leqslant p$. Her er nødvendigvis $q = 1$. Antog vi nemlig, at $q > 1$, ville vi have $\sigma(a_p) = a_{p+1} = a_q = \sigma(a_{q-1})$, og da σ er injektiv, ville vi få $a_p = a_{q-1}$ og $1 \leqslant q - 1 < p$, i modstrid med at elementerne $a_1, \dots, a_p$ var forskellige. Vi har altså $\sigma(a_p) = a_1$. Nu følger det, at $a_{p+2} = \sigma(a_1) = a_2$, $a_{p+3} = \sigma(a_{p+2}) = a_3$, osv. Banen B_a for σ består altså af de p forskellige elementer $a_1, \dots, a_p$:

$$B_a = \{a_1, \dots, a_p\}, \text{ og } \sigma(a_p) = a_1.$$

Tallet p er altså netop antallet af elementer i banen. Det kaldes også banens *længde*.

Hvis a er fixpunkt for σ, har vi $a = a_1 = a_2 = \cdots$. Banen B_a består altså alene af elementet a. Hvis a ikke er fixpunkt for σ, har vi $a_2 \neq a_1$, så banen B_a indeholder mere end ét element. Fixpunkterne for σ er altså netop de elementer $a \in X$, for hvilke banen B_a er en *et-punkts-bane*, dvs har længde 1.

Et vilkårligt element b i banen B_a bestemmer den samme bane, thi er $b = a_i$ finder vi

$$b_1 = a_i,\ b_2 = a_{i+1},\ \dots,\ b_{p-i+1} = a_p,\ b_{p-i+2} = a_1,\ \dots,\ b_p = a_{i-1},\ b_{p+1} = a_i$$

og følgelig er $B_b = B_a$.

Det følger nu, at banerne for σ udgør en klassedeling af X. Hver bane er nemlig ikke-tom, hvert element a i X ligger i en bane (nemlig i banen B_a), og hvis to baner har et element b fælles, så er de ens, nemlig lig med banen B_b.

Til en bane B af længde p for σ er der naturligt en *tilhørende p*-cykel,

$$\gamma := (a_1\ \dots\ a_p),$$

hvor $a = a_1$ er et element i B, og $a_{i+1} = \sigma(a_i)$. Cyklen γ afhænger ikke af hvilket element a, der er valgt i B. Øjensynlig gælder for alle $x \in B$, at $\sigma(x) = \gamma(x)$. Hvis $x \notin B$ er x fixpunkt for γ (men ikke nødvendigvis for σ). Da banerne udgør en klassedeling af X, er de tilhørende cykler disjunkte. Specielt kommuterer cyklerne hørende til banerne for σ.

(2.12) Cykelsætningen. *Lad σ være en permutation af X, lad $B_1, \dots, B_m$ være banerne for σ, og lad $\gamma_1, \dots, \gamma_m$ være de tilhørende cykler. Da gælder ligningen,*

$$\sigma = \gamma_1 \cdots \gamma_m. \tag{2.12.1}$$

Bevis. Ligningens to sider er (bijektive) afbildninger $X \to X$. Det er påstanden, at de to afbildninger er den samme, altså at de har samme værdi for hvert element $x \in X$. Venstresidens værdi i x er $\sigma(x)$. Da banerne udgør en klassedeling, ligger x i én bane, fx i B_j. Vi har da $\gamma_j(x) = \sigma(x)$. Elementerne x og $\gamma_j(x)$ ligger begge i banen B_j, og de er derfor fixpunkter for alle de øvrige cykler γ_i. Højresidens værdi i x er derfor $\gamma_j(x) = \sigma(x)$, altså lig med venstresidens. Hermed er ligningen bevist. □

(2.13) Eksempel. Fremstillingen (2.12.1) af σ som et produkt af disjunkte cykler hørende til banerne, kaldes også *cykelfremstillingen* af σ. Bemærk, at cyklen hørende til en et-punkts-bane (svarende til et fixpunkt for σ) er en 1-cykel, og altså identiteten. Fjernes 1-cyklerne fås en fremstilling af σ som produkt af disjunkte cykler af længde større end 1.

Det skal understreges, at når σ selv er identiteten, så er alle cyklerne 1-cykler, og der er ingen cykler tilbage, når de fjernes. Det er her, og i almindelighed, konventionen, at et produkt med *ingen* faktorer siges at fremstille identiteten.

Det er umiddelbart at bestemme cykelfremstillingen af en given permutation. Betragt fx permutationen $\sigma \in S_8$ i (2.2.2). Vælg et tal z, der flyttes af σ. Vi kan for eksempel vælge tallet $z = 4$. Af tabelnotationen for σ fremgår, at $4 \mapsto 5$, og videre, at $5 \mapsto 8$, og videre, at $8 \mapsto 1$, og endelig at $1 \mapsto 4$. Hermed er den første bane bestemt, og den tilhørende cykel er 4-cyklen $(4\,5\,8\,1)$. Vælg nu et nyt tal, der flyttes af σ og ikke er et af de allerede berørte. Vi kan for eksempel vælge tallet 2. Det ses, at $2 \mapsto 7$, at $7 \mapsto 6$, at $6 \mapsto 3$, og endelig, at $3 \mapsto 2$. Hermed er den anden bane bestemt, og den tilhørende cykel er 4-cyklen $(2\,7\,6\,3)$. Nu er der ikke flere tal blandt de 8, og vi har fremstillingen af σ som produkt af to disjunkte 4-cykler,

$$\sigma = \begin{pmatrix} 4 & 7 & 2 & 5 & 8 & 3 & 6 & 1 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \end{pmatrix} = (4\,5\,8\,1)(2\,7\,6\,3).$$

(2.14) Hovedsætning. *Lad X være en endelig mængde. Da gælder:*

(1) *Enhver permutation σ af X kan fremstilles som et produkt af transpositioner.*

(2) *Er $a \in X$ et givet element, kan der i fremstillingen vælges transpositioner af formen $(a\,x)$ for $x \in X \setminus \{a\}$.*

(3) *Er $X = \{x_1, \dots, x_n\}$ en nummerering af elementerne i X, kan der i fremstillingen vælges transpositioner af formen $(x_j\,x_{j+1})$ for $j = 1, \dots, n-1$ („transposition af naboer“).*

Bevis. Det følger af Cykelsætningen, at σ kan fremstilles som produkt af cykler. Hver af disse cykler kan ifølge Ligning (2.9.3) fremstilles som produkt af transpositioner. Herved fås en fremstilling af σ som produkt af transpositioner. Hermed er (1) bevist.

En transposition $(x_1\, x_2)$ er af formen $(a\, x)$, hvis enten x_1 eller x_2 er lig med a. Hvis både x_1 og x_2 er forskellige fra a, så følger det let, at

$$(x_1\, x_2) = (a\, x_1)(a\, x_2)(a\, x_1); \tag{2.14.1}$$

transpositionen $(x_1\, x_2)$ er altså et produkt af tre transpositioner af formen $(a\, x)$. Påstanden (2) følger derfor af (1).

Antag, at X er nummereret, $X = \{x_1, \dots, x_n\}$. Det følger da af (2), at σ kan skrives som produkt af transpositioner af formen $(x_1\, x_i)$. For at vise (3) er det derfor nok at vise, at hver af transpositionerne $(x_1\, x_i)$, for $i = 2, \dots, n$, kan skrives som produkt af transpositioner af naboer, dvs transpositioner af formen $(x_j\, x_{j+1})$. Denne påstand vises ved induktion efter i. For $i = 2$ er påstanden triviel, idet $(x_1\, x_2)$ selv er en transposition af naboer. For $i \geqslant 2$ følger det af (2.14.1), at

$$(x_1\, x_{i+1}) = (x_i\, x_{i+1})(x_1\, x_i)(x_i\, x_{i+1}).$$

På højresiden er $(x_i\, x_{i+1})$ en transposition af naboer, og induktivt er transpositionen $(x_1\, x_i)$ et produkt af transpositioner af naboer. Altså er venstresiden, $(x_1\, x_{i+1})$, et produkt af transpositioner af naboer.

Hermed er også (3) bevist. $\square$

(2.15) Eksempel. Fremstillingen af en permutation σ som produkt af transpositioner er ikke entydig. Fx finder vi for transpositionen $\tau = (1\,2)$ i S_3 ligningerne,

$$\tau = (1\,2) = (1\,3)(2\,3)(1\,3) = (2\,3)(1\,3)(2\,3).$$

Permutationen τ kan altså fremstilles som et produkt af én transposition („sig selv“) og den har to fremstillinger som et produkt af 3 transpositioner.

Betragt permutationen ω i S_9, jfr (2.6). Den er bestemt ved $\omega(i) = 10 - i$ for $i = 1, \dots, 9$. Cykelfremstillingen er

$$\omega = (1\,9)(2\,8)(3\,7)(4\,6)(5). \tag{2.15.1}$$

Tallet 5 er fixpunkt, og ser vi bort fra identiteten (5), er (2.15.1) en fremstilling af ω som produkt af 4 transpositioner. Det følger af beviset for Sætning (2.14), at vi herfra kan få en fremstilling af ω som produkt af 10 transpositioner af formen $(1\, i)$, for $i = 2, \dots, 9$. I (2.15.1) er $(4\,6) = (5\,6)(4\,5)(5\,6)$ et produkt af tre transpositioner af naboer. Tilsvarende, jfr beviset for (2.14), kan de 3 andre transpositioner skrives som produkter af transpositioner af naboer. Herved fås en fremstilling af ω som produkt af mindst 36 transpositioner af naboer.

(2.16) Cykeltype. Lad σ være en permutation i den endelige mængde X. Som nævnt i (2.11) udgør banerne for σ en klassedeling af X. En række vigtige invarianter for σ er knyttet til denne klassedeling. Med $m(\sigma)$ betegner vi antallet af baner for σ. Mere præcist betegner vi med $m_p(\sigma)$ antallet af baner af længde p for σ. Specielt er $m_1(\sigma)$ antallet af fixpunkter for σ. Længden af en bane kan jo højst være elementantallet i X, så vi har $m_p(\sigma) = 0$, når $p > |X|$. Følgen $m_1(\sigma), m_2(\sigma), m_3(\sigma) \dots$ kaldes også *typen* af σ. Typen angiver altså hvor mange et-punkts-baner, 2-punkts-baner osv, der indgår i klassedelingen. Ofte angives typen mere kompakt som et „formelt produkt" $1^{m_1}2^{m_2}3^{m_3}\cdots$; at en permutation har typen $1^3 3^2 5^1$ betyder altså, at den har 3 fixpunkter, der er 2 baner af længde 3 og 1 bane af længde 5. For en permutation σ af typen $1^{m_1}2^{m_2}\cdots$ giver cykelsætningen en fremstilling af σ som et produkt af disjunkte cykler, og m_p er antallet af p-cykler i fremstillingen. Skrives i fremstillingen først 1-cyklerne, dernæst 2-cyklerne osv, så fås en fremstilling, der matcher følgende billede,

$$\overbrace{(*)\cdots(*)}^{m_1}\ \overbrace{(**)\cdots(**)}^{m_2}\ \overbrace{(***)\cdots(***)}^{m_3}\ \cdots .$$

Typen af σ kaldes også *cykeltypen*. Den kan alternativt angives ved et billede som ovenstående.

Et simpelt tælleargument viser formlerne,

$$m(\sigma) = \sum m_p(\sigma), \qquad |X| = \sum p\, m_p(\sigma), \tag{2.16.1}$$

hvor der summeres over $p = 1, 2, \dots$; der er kun endelig mange led forskellige fra 0 i summerne, idet $m_p(\sigma) = 0$ for $p > |X|$. Den første formel udsiger blot, at vi kan tælle antallet $m(\sigma)$ af baner ved at tælle antallet af baner af længde p og lægge antallene sammen. Den anden formel udsiger, at vi kan tælle antallet af elementer i X ved at tælle elementerne i hver bane og lægge antallene sammen: i hver bane af længde p er der p elementer, så de $m_p(\sigma)$ baner af længde p bidrager med $p{\cdot}m_p(\sigma)$ til summen.

For en given mængde X afhænger de mulige typer kun af elementantallet $n = |X|$. Hver type svarer til en *partition* af n som en sum af et antal 1-taller, et antal 2-taller osv. For $n = 4$ er partitionerne:

$$1+1+1+1 = 2+2 = 1+3 = 1+1+2 = 4$$

svarende til de 5 typer 1^4, 2^2, $1^1 3^1$, $1^2 2^1$, 4^1.

(2.17) Eksempel. De 24 permutationer i S_4 deles i 5 typer:

cykelbillede	type	baneantal	antal
$(*)(*)(*)(*)$	1^4	4	1
$(**)(**)$	2^2	2	3
$(*)(***)$	$1^1 3^1$	2	8
$(*)(*)(**)$	$1^2 2^1$	3	6
$(****)$	4^1	1	6

Typen 1^4 fastlægger øjensynlig identiteten. Typen 2^2 fastlægger en *dobbelttransposition*, dvs et produkt af to disjunkte transpositioner. Ved en dobbelttransposition i S_4 skal tallet 1 ombyttes med et af tallene 2, 3, 4, og de to resterende tal skal ombyttes. Dobbelttranspositioner er altså helt bestemt ved det tal, som 1 ombyttes med; der er altså 3 dobbelttranspositioner i S_4. Typen $1^1 3^1$ fastlægger 3-cyklerne. For en 3-cykel i S_4 er der 4 muligheder for fixpunktet, og når fixpunktet er fastlagt, er der to 3-cykler, som permuterer de tre øvrige tal; der er altså $4 \cdot 2 = 8$ cykler af længde 3 i S_4. Typen $1^2 2^1$ fastlægger en transposition. En transposition er bestemt ved fastlæggelsen af de to tal, der ombyttes; der er altså $\binom{4}{2} = 6$ transpositioner i S_4. Endelig fastlægger typen 4^1 en 4-cykel. Notationen for en 4-cykel kan vælges med et bestemt tal, fx 1, på førstepladsen; der er altså $3 \cdot 2 \cdot 1 = 6$ cykler af længde 4 i S_4.

(2.18) Fortegn. For en permutation σ af en endelig mængde X defineres *fortegnet*, $\operatorname{sign}(\sigma)$, som tallet,

$$\operatorname{sign}(\sigma) := (-1)^k, \quad \text{hvor } k = |X| - m(\sigma) = \sum (p-1)m_p(\sigma). \tag{2.18.1}$$

Her er $m(\sigma)$ antallet af baner for σ, og $m_p(\sigma)$ er antallet af baner af længde p. De to udtryk for $k = k(\sigma)$ er ens ifølge (2.16.1).

Antag at X har n elementer. Identiteten har alle elementer i X som fixpunkter, så alle baner er et-punkts-baner. For identiteten har vi altså $m_1 = n$, og $m_2 = m_3 = \cdots = 0$. Typen er altså 1^n, og baneantallet er $m = n$. Fortegnet for identiteten er $(-1)^{n-m} = 1$.

Betragt en p-cykel γ, hvor $p > 1$. Da er der én bane, som indeholder p elementer, og de øvrige $n-p$ elementer er fixpunkter. Vi har altså $m_1(\gamma) = n-p$, $m_p(\gamma) = 1$, og $m_q(\gamma) = 0$ for $q \neq 1, p$. Typen er altså $1^{n-p}p^1$ og baneantallet er $m = n - p + 1$. Specielt er fortegnet for en p-cykel lig med $(-1)^{n-m} = (-1)^{p-1}$.

Bemærk specielt, at en transposition har fortegnet -1.

For en given permutation σ er tallet $m_p(\sigma)$ antallet af p-cykler, der indgår i cykelfremstillingen af σ. Enhver p-cykel kan skrives som produkt af $p-1$ transpositioner, jfr (2.9.3). Summen $k := \sum(p-1)m_p(\sigma)$ i (2.18.1) er derfor det antal transpositioner, der fremkommer, når man i cykelfremstillingen skriver hver p-cykel som produkt af $p-1$ transpositioner. Det følger specielt, at σ kan skrives som produkt af k transpositioner.

(2.19) Lemma. *Lad τ være en transposition og lad σ være en vilkårlig permutation af den endelige mængde X. Da gælder for baneantallene ligningen,*

$$m(\tau\sigma) = m(\sigma) \pm 1. \tag{2.19.1}$$

Bevis. Lad a og b være de to elementer, der ombyttes af τ. Som nævnt i (2.11) udgør banerne for σ en klassedeling af X. Der er to tilfælde: Banerne $B_a(\sigma)$ og $B_b(\sigma)$ er disjunkte eller de er ens.

Betragt det første tilfælde, hvor banerne $B_a(\sigma)$ og $B_b(\sigma)$ er disjunkte. Lad deres længder være p og q. Vi har altså

$$B_a(\sigma) = \{a = a_1, a_2, \ldots, a_p\} \text{ og } B_b(\sigma) = \{b = b_1, b_2, \ldots, b_q\},$$

hvor $\sigma(a_p) = a$ og $\sigma(b_q) = b$. Det påstås, at

$$B_a(\tau\sigma) = \{a_1, \ldots, a_p, b_1, \ldots, b_q\}. \tag{1}$$

Hertil skal vi betragte billederne $(\tau\sigma)^i(a)$. Vi har $a = a_1$. For $1 \leqslant i < p$ har vi $\sigma(a_i) = a_{i+1}$, og da a_{i+1} ikke flyttes af τ, er $\tau\sigma(a_i) = a_{i+1}$. For $i = p$ har vi $\sigma(a_p) = a_1$ og dermed $\tau\sigma(a_p) = \tau(a) = b = b_1$. Videre følger det for $1 \leqslant j < q$, at vi har $\tau\sigma(b_j) = b_{j+1}$. Endelig får vi for $j = q$, at $\tau\sigma(b_q) = \tau(b) = a = a_1$. Hermed har vi vist ligningen (1). De to baner $B_a(\sigma)$ og $B_b(\sigma)$ for σ er altså forenet til én bane for $\tau\sigma$. De øvrige baner for σ

består af elementer, der ikke flyttes af τ, og de er derfor også baner for $\tau\sigma$. Altså får vi, i det første tilfælde, ligningen,

$$m(\tau\sigma) = m(\sigma) - 1.$$

Betragt det andet tilfælde, hvor $B_a(\sigma)$ og $B_b(\sigma)$ er samme bane. Da $b \in B_a(\sigma)$, har vi $b = a_{p+1}$ med et passende $p \geqslant 1$, og kan antage, at banen har længden $p + q$. Da er

$$B_a(\sigma) = \{a_1, \ldots, a_p, b_1, \ldots, b_q\},$$

hvor $\sigma(a_p) = b_1 = b$ og $\sigma(b_q) = a_1$. For $1 \leqslant i < p$ får vi $\tau\sigma(a_i) = a_{i+1}$, og for $i = p$ har vi $\tau\sigma(a_p) = \tau(b_1) = a_1$. Altså er $B_a(\tau\sigma) = \{a_1, \ldots, a_p\}$. Tilsvarende er $B_b(\tau\sigma) = \{b_1, \ldots, b_q\}$. Den ene bane $B_a(\sigma)$ splittes altså i to baner for $\tau\sigma$. De øvrige baner for σ består af elementer, der ikke flyttes af τ, og de er derfor også baner for $\tau\sigma$. Altså får vi, i det andet tilfælde, ligningen,

$$m(\tau\sigma) = m(\sigma) + 1.$$

Følgelig gælder (2.19.1) i begge tilfælde. ∎

(2.20) Hovedsætning. *For permutationer μ og σ af den endelige mængde X gælder ligningen for fortegnene,*

$$\operatorname{sign}(\mu\sigma) = \operatorname{sign}(\mu)\operatorname{sign}(\sigma). \tag{2.20.1}$$

Bevis. For en transposition τ har vi ifølge Lemma (2.19), at $m(\tau\sigma) = m(\sigma) \pm 1$. Altså er $|X| - m(\tau\sigma) = |X| - m(\sigma) \mp 1$. Heraf fås ligningen for fortegnene,

$$\operatorname{sign}(\tau\sigma) = (-1)\operatorname{sign}(\sigma). \tag{1}$$

For et produkt $\tau_1 \cdots \tau_k$ af k transpositioner følger det, ved gentagen anvendelse af (1), at

$$\operatorname{sign}(\tau_1 \cdots \tau_k) = (-1)^k.$$

Ifølge Hovedsætning (2.14)(1) kan μ og σ fremstilles som produkter af transpositioner. Antag, at der indgår k transpositioner i en fremstilling af μ og l transpositioner i en fremstilling af σ. Af fremstillingerne fås en fremstilling af $\mu\sigma$ som produkt af $k+l$ transpositioner. Altså er

$$\operatorname{sign}(\mu\sigma) = (-1)^{k+l} = (-1)^k(-1)^l = \operatorname{sign}(\mu)\ \operatorname{sign}(\sigma).$$

Hermed er (2.20.1) bevist. ∎

(2.21) Definition. En permutation σ af den endelige mængde X kaldes *lige*, hvis den kan skrives som et produkt af et lige antal transpositioner, og *ulige*, hvis den kan skrives som et produkt af et ulige antal transpositioner. Her medregnes fremstillingen af identiteten som et produkt af ingen transpositioner (hvor antallet er 0), så identiteten er en lige permutation.

Ifølge Hovedsætning (2.14)(1) kan enhver permutation skrives som et produkt af transpositioner. Enhver permutation er altså lige eller ulige. Men på forhånd er det ikke klart, at en permutation σ ikke kan være både lige og ulige. Det kunne jo tænkes, at σ både kunne fremstilles som et produkt af et lige antal transpositioner og som et produkt af et ulige antal. At dette ikke kan være tilfældet, fremgår af det følgende resultat.

(2.22) Korollar. *En permutation μ af en endelig mængde er lige, hvis og kun hvis den har fortegnet* 1, *og ulige, hvis og kun hvis den har fortegnet* -1. *De lige permutationer udgør en undergruppe i gruppen af alle permutationer. Hvis X har mindst* 2 *elementer, er det præcis halvdelen af permutationerne, der er lige.*

Bevis. En transposition har fortegnet -1. Ved gentagen anvendelse af (2.20.1) følger derfor, at hvis μ er et produkt af k transpositioner, så har μ fortegnet $(-1)^k$. Heraf følger den første påstand.

Af en fremstilling af μ som produkt af k transpositioner og en fremstilling af σ som et produkt af l transpositioner får vi umiddelbart en fremstilling af $\mu\sigma$ som et produkt af $k+l$ transpositioner. Specielt følger det, at hvis μ og σ er lige permutationer, så er også $\mu\sigma$ en lige permutation. Heraf fremgår, at de lige permutationer udgør en stabil delmængde af gruppen S_X af alle permutationer. Som nævnt er identiteten en lige permutation. Hvis permutationen μ er skrevet som produkt af k transpositioner,

$$\mu = \tau_1 \cdots \tau_k,$$

så får vi fremstillingen for den inverse permutation,

$$\mu^{-1} = \tau_k^{-1} \cdots \tau_1^{-1} = \tau_k \cdots \tau_1,$$

hvor det sidste lighedstegn følger af at en transposition er sin egen inverse. Det fremgår specielt, at hvis μ er lige, så er også μ^{-1} lige. Hermed er vist, at de lige permutationer udgør en undergruppe.

Hvis X indeholder mindst to elementer, så findes der en ulige permutation τ af X, fx en transposition. Det fremgår af overvejelserne ovenfor, at en permutation μ er lige, hvis og kun hvis $\tau\mu$ er ulige. Ved $\mu \mapsto \tau\mu$ defineres altså en afbildning fra mængden L af lige permutationer til mængden U af ulige permutationer. Afbildningen er bijektiv. Den inverse afbildning er nemlig givet ved den samme forskrift $\nu \mapsto \tau\nu$, idet $\tau\tau\mu = \mu$. Der er derfor samme antal permutationer i L og U, og da summen af de to antal er lig med antallet af alle permutationer, må de hver for sig være det halve af antallet af alle permutationer.

Hermed er alle korollarets påstande bevist. □

(2.23) Definition. De lige permutationer i den symmetriske gruppe S_n udgør ifølge korollaret en undergruppe. Denne undergruppe kaldes den *alternerende gruppe af grad n*, og den betegnes A_n.

For $n = 1$, består den symmetriske gruppe S_1 kun af identiteten, som er en lige permutation. Vi har altså, at $\mathrm{A}_1 = \mathrm{S}_1$ er den trivielle gruppe med ét element, som vi også betegner C_1.

For $n \geqslant 2$ følger det af korollaret, at A_n består af halvdelen af permutationerne i S_n. Gruppen A_n har altså orden $\frac{1}{2}n!$.

(2.24) Sætning. *Lad X være en endelig mængde. Da gælder:*

(1) *Enhver lige permutation σ af X kan fremstilles som et produkt af* 3*-cykler.*
(2) *Er der givet to forskellige elementer $a, b \in X$, kan der i fremstillingen vælges* 3*-cykler af formen $(a\,b\,x)$ for $x \in X \setminus \{a, b\}$,*
(3) *Er $X = \{x_1, \dots, x_n\}$ en nummerering af elementerne i X, kan der i fremstillingen vælges* 3*-cykler af formen $(x_i\, x_{i+1}\, x_{i+2})$ for $i = 1, \dots, n-2$.*

Bevis. Det følger af Hovedsætning (2.14)(2), at σ kan skrives som produkt af et antal transpositioner af formen $(a\,x)$ med et fast element a. Antallet er lige, da σ er en lige permutation. Vi kan derfor multiplicere faktorerne to og to. Betragt et produkt $(a\,x)(a\,y)$. Hvis $x = y$, er produktet blot identiteten. Hvis a, x, y er forskellige, finder vi $(a\,x)(a\,y) = (a\,y\,x)$, så produktet er en 3-cykel. Hermed er (1) bevist.

Ifølge beviset for (1) kan σ skrives som produkt af 3-cykler af formen $(a\,y\,x)$. Det er derfor nok at vise, at enhver sådan 3-cykel kan skrives som produkt af 3-cykler af formen $(a\,b\,x)$. Hvis $y = b$ er dette naturligvis oplagt. Hvis $x = b$, følger påstanden af ligningen,

$$(a\,y\,b) = (a\,b\,y)(a\,b\,y).$$

Endelig, hvis både x og y er forskellige fra b, så følger påstanden af ligningen,

$$(a\,y\,x) = (a\,b\,x)(a\,b\,y)(a\,b\,y).$$

Hermed er (2) bevist.

Ifølge (2) kan σ skrives som produkt af 3-cykler af formen $(x_1\,x_2\,x_i)$, for $i = 3, \dots, n$. Vi viser, ved induktion efter i, at enhver sådan 3-cykel kan skrives som et produkt af 3-cykler, der cykler naboer. For $i = 3$ har vi cyklen $(x_1\,x_2\,x_3)$, som selv er en 3-cykel af naboer. For $i = 4$ fremgår påstanden af ligningen,

$$(x_1\,x_2\,x_4) = (x_1\,x_2\,x_3)(x_2\,x_3\,x_4)^2,$$

som let eftervises. I induktionsskridtet bruges for $i \geqslant 4$ ligningen,

$$(x_1\,x_2\,x_{i+1}) = (x_{i-1}\,x_i\,x_{i+1})(x_1\,x_2\,x_i)(x_{i-1}\,x_i\,x_{i+1})^2,$$

som let eftervises. På højresiden er den anden 3-cykel induktivt et produkt af 3-cykler af naboer, og de øvrige 3-cykler er selv 3-cykler af naboer. Hermed er også (3) bevist. $\square$

(2.25) Eksempel. 15-spillet er et velkendt puslespil. Det spilles med 15 brikker placeret på et bræt med $4 \times 4 = 16$ felter. Et af felterne er altså tomt. Et (tilladt) træk består i at en brik kan skubbes hen på nabofeltet, såfremt dette er tomt. Felterne er naturligt nummereret fra 1 til 16; rækkefølgen fremgår af den første figur, hvor der er placeret en brik mærket med i på felt nummer i. Felt nummer 16 er tomt. På den næste figur er der flyttet rundt på de 15 brikker. Kan man med tilladte træk komme fra den første figur til den anden?

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

4	8	12	15
3	7	11	14
2	6	10	13
1	5	9	

g	o	s	å
s	v	æ	r
u	d	e	n
t	a	l	

Det er bekvemt at tænke sig, at en „tom brik“ er placeret på det tomme felt. Et tilladt træk består så i at ombytte den tomme brik med en brik fra et af nabofelterne. En omflytning af brikkerne fra én placering til en anden kan angives ved den permutation i S_{16}, der er bestemt ved at brikken på felt nummer i er flyttet hen på felt nummer $\sigma(i)$. Bemærk, at permutationen beskriver, hvordan brikkerne bliver flyttet; den er uafhængig af hvordan brikkerne er mærket. Et tilladt træk er en transposition: den tomme brik ombyttes med en af naboerne. Det er naturligvis ikke alle transpositioner, der kan udføres med et tilladt træk. I udgangsstillingen kan vi fx kun udføre transpositionerne (15 16) og (12 16). Transpositionen (12 16) fører brikken på det 12'te felt hen på det sidste felt, og felt nummer 12 bliver tomt. Herefter kan vi udføre transpositionerne (8 12), (11 12) og (16 12).

Betragt fx den tredie figur. Vi kan flytte brikken 'n' ned på det tomme felt, altså udføre transpositionene (12 16). Herefter er felt nummer 12 tomt, og vi kan flytte brikken 'e' hen på det tomme felt, dvs udføre transpositionen (11 12). Herefter kan vi flytte brikken 'l' op på felt nummer 11, dvs udføre transpositionen (11 15). Endelig kan vi flytte brikken 'n', der nu står på felt nummer 16, hen på felt nummer 15, dvs udføre transpositionen (15 16). Det er måske lettest at tænke på, at den „tomme brik“ blev flyttet først et skridt opad, så et skridt til venstre, så et skridt nedad, og til sidst et skridt til højre (hvorved den endte hvor den begyndte). I alt udførte vi permutationen,

$$(15\ 16)(11\ 15)(11\ 12)(12\ 16) = (11\ 12\ 15).$$

Betragt tilsvarende permutationen, der fører den første figur til den anden. Den er bestemt ved at brikken på felt nr 1 er flyttet til felt nr 13, altså ved $1 \mapsto 13$, brikken på felt nr 2 er flyttet til felt nr 9, altså ved $2 \mapsto 9$, osv. Cykelfremstillingen af permutationen er produktet,

$$(1\ 13\ 12\ 3\ 5\ 14\ 8\ 2\ 9\ 15\ 4)(6\ 10\ 11\ 7)(16).$$

Betragt en vilkårlig placering, der kan fremkomme af den første figur ved en række tilladte træk. Hvert tilladt træk fører den tomme brik til et af nabofelterne. På den første figur er den tomme brik placeret på felt nummer 16. Antag, at også den fremkomne placering har den tomme brik på felt nummer 16. Det følger så, at der må være anvendt et lige antal tilladte træk, endda et lige antal „vandrette“ træk og et lige antal „lodrette“ træk. Da hvert tilladt træk er en transposition sluttes, at *den permutation, der beskriver den fremkomne placering, må være en lige permutation.* Det er i øvrigt ikke så svært at vise, fx ved brug af Sætning (2.24), at man faktisk kan opnå enhver placering, der beskrives ved en lige permutation og har den tomme brik på sidste felt.

Permutationen ovenfor har typen $1^1 4^1 11^1$, og derfor fortegnet $(-1)^{16-3} = -1$. Den er derfor ulige. Placeringen på den anden figur kan derfor ikke opnås ved tilladte træk fra den første figur. Hvordan kan placeringen af brikkerne på den tredie figur ændres med tilladte træk således, at der kommer til at stå „også svær uden tal“?

(2.26) Opgaver.
1. Lad γ være en p-cykel. Vis, at γ^2 er en p-cykel, når p er ulige, og at γ^2 ikke er en cykel, når p er lige (og forskellig fra 2).

2. I den direkte notation er $\sigma = (9, 7, 5, 3, 8, 1, 6, 4, 2)$ en permutation $\sigma \in \mathrm{S}_9$. Bestem fremstillingen af σ og af σ^{-1} som produkt af disjunkte cykler.

3. Skriv permutationen $(1\,3\,7\,4)(1\,5\,7\,6\,3)(1\,2)(1\,4\,2)$ som produkt af disjunkte cykler.

4. Ved $x \mapsto 7x + 3$ bestemmes en bijektiv afbildning $\sigma\colon \mathbb{Z}/10 \to \mathbb{Z}/10$. Idet tallene $1, 2, \dots, 10$ identificeres med deres restklasser modulo 10, opfattes σ som permutation i S_{10}. Angiv σ i den direkte notation. Angiv fremstillingen af σ som produkt af disjunkte cykler.

5. Ved $x \mapsto x^3$ defineres en permutation σ af $\mathbb{Z}/15$ og dermed en permutation i S_{15}. Vis, at σ er bijektiv ved at angive fremstillingen af σ som produkt af disjunkte cykler.

6. Angiv de mulige cykeltyper for permutationerne i S_5 og S_6.

7. Bestem fortegnet for permutationen $(9, 7, 5, 3, 8, 1, 6, 4, 2)$ (i den direkte notation).

8. Ved $x \mapsto -x$ bestemmes en permutation af $\mathbb{Z}/n$. Bestem permutationens fortegn.

9. Angiv de mulige cykeltyper for permutationerne i A_4, A_5, og A_6.

10. Vis, at A_n ikke er kommutativ, når $n \geqslant 4$.

11. *Betragt n-cyklen $\gamma_n = (1\,2\,\dots\,n)$ og transpositionen $\tau = (1\,2)$ i S_n. Vis, at de to permutationer frembringer gruppen S_n i den forstand, at enhver permutation i S_n kan skrives som et produkt af faktorer, hvor hver faktor er en af de to permutationer γ_n og τ.

12. *For en tabelfremstilling $\sigma = \binom{x_1\,\dots\,x_n}{y_1\,\dots\,y_n}$ af en permutation $\sigma \in \mathrm{S}_n$ er x_i'erne og y_i'erne tal, og vi kan betragte brøken,

$$\prod_{i<j} \frac{x_j - x_i}{y_j - y_i}\,.$$

Ingen af nævnerne er 0, da tallene y_i er forskellige. Mere præcist ser vi, at differenserne $y_j - y_i$ på nær fortegn er samtlige differenser mellem to af tallene $1, \dots, n$. Vis, at brøkens værdi er ± 1. Vis, at brøkens værdi ikke ændres, når to nabosøjler i tabellen ombyttes, og slut, at brøkens værdi $s := s(\sigma)$ kun afhænger af σ og ikke af den valgte tabelfremstilling. Vis, at $s(\sigma\mu) = s(\sigma)s(\mu)$. Vis, at $s(\sigma) = \operatorname{sign}(\sigma)$.

13. Lad $\sigma = (\sigma_1, \dots, \sigma_n) \in \mathrm{S}_n$ være en permutation i S_n (i den direkte notation). Ved en *inversion* for σ forstås et par af indices (i, j) med $i < j$ og $\sigma_i > \sigma_j$. Antallet af inversioner $\ell(\sigma)$ bestemmes sådan: Gennemløb pladserne, for $i = 1, \dots, n$, og tæl for hver plads i hvor mange gange, der på en senere plads j står et tal, der er mindre end det i'te: $\sigma_j < \sigma_i$. Antag, at $\sigma_k > \sigma_{k+1}$, og lad σ' være permutationen, der (i den direkte notation) fås fra σ ved at ombytte tallene σ_k og σ_{k+1}. Vis, at $\ell(\sigma') = \ell(\sigma) - 1$. Vis, at $\sigma' = \sigma\tau_k$, hvor τ_k er nabotranspositionen $\tau_k = (k\,k{+}1)$. Slut heraf, at σ kan skrives som produkt af $\ell(\sigma)$ nabotranspositioner, og specielt, at $\operatorname{sign}(\sigma) = (-1)^{\ell(\sigma)}$.

14. Lad $p(n)$ være antallet af cykeltyper i S_n, altså antallet af partitioner af n, og lad $p_h(n)$ være antallet af typer, hvor længden af den største bane er h. Øjensynlig er $p(n) = \sum_{h=1}^{n} p_h(n)$. Vis rekursionsformlen: $p_n(n) = 1$ og for $h < n$ er $p_h(n) = \sum_{j=1}^{h} p_j(n-h)$.

15. Lad der være givet en bijektiv afbildning $\mu\colon X \to Y$. Gør rede for, at hvis σ er en permutation af X, så er ${}^{\mu}\sigma := \mu\sigma\mu^{-1}$ en permutation af Y. Vis, at hvis σ er produkt af disjunkte cykler $(x_1\,\dots\,x_p)$, så er ${}^{\mu}\sigma$ produkt af de tilsvarende disjunkte cykler $(\mu(x_1)\,\dots\,\mu(x_p))$.

16. *Med $k = k(\sigma) = n - m(\sigma) = \sum(p-1)m_p(\sigma)$ som i GRP(2.18.1) kan σ skrives som produkt af k transpositioner. Vis, at σ ikke kan skrives som produkt af færre end k transpositioner.

17. Bestem cykelfremstillingen af $(1\,2\,3\,\ldots\,n)\cdots(1\,2\,3\,4)(1\,2\,3)(1\,2)$.
*Bestem cykelfremstillingen af $(1\,2)(1\,2\,3)(1\,2\,3\,4)\cdots(1\,2\,3\,\ldots\,n)$.

18. Antag, at X er en ordnet mængde med n elementer. Vis, at enhver permutation σ af X har en entydig fremstilling som et produkt af følgende form (med $k \geqslant 0$ transpositioner):

$$\sigma = (i_1\,j_1)\cdots(i_k\,j_k),\ \text{hvor } i_s < j_s \text{ for } s = 1,\ldots,k \text{ og } j_1 < \cdots < j_k, \tag{*}$$

og at $n-k$ er antallet af baner for σ. [Vink: For $\sigma = \mathrm{id}$ anvendes den tomme fremstilling ($k = 0$). For $\sigma \neq \mathrm{id}$ kan man lade $j(\sigma)$ betegne det største element, der flyttes af σ. Begrund, at i en fremstilling (*) må der gælde $j(\sigma) = j_k$ og $\sigma(i_k) = j_k$, og benyt dette til at vise påstanden ved fuldstændig induktion efter $j(\sigma)$.]

Stirling-tallene af første art, for $n \geqslant 0$ og $0 \leqslant m \leqslant n$, er antallene,

$$\begin{bmatrix} n \\ m \end{bmatrix} := \text{antallet af permutationer i } S_n \text{ med } m \text{ baner.}$$

Vis, at

$$\begin{bmatrix} n \\ n-k \end{bmatrix} = \sum_{1 \leqslant j_1 < j_2 < \cdots < j_k \leqslant n-1} j_1 j_2 \cdots j_k.$$

[Vink: Tæl antallet af fremstillinger (*), fx når $X = \{0, 1, \ldots, n-1\}$.]

Udled, ved at multiplicere parenteserne, følgende ligning mellem polynomier:

$$x(x+1)\cdots(x+n-1) = \sum\nolimits_r \begin{bmatrix} n \\ r \end{bmatrix} x^r.$$

19. *Stirling-tallene af anden art*, for $n \geqslant 0$ og $0 \leqslant m \leqslant n$, er antallene,

$$\begin{Bmatrix} n \\ m \end{Bmatrix} := \text{antallet af klassedelinger af } \{1,\ldots,n\} \text{ med } m \text{ klasser.}$$

I en klassedeling af $X = \{1,\ldots,n\}$ med m klasser kan man (entydigt) nummerere klasserne $X_1,\ldots,X_m$ sådan, at når h_i er det mindste tal i X_i, så er $h_1 < h_2 < \cdots < h_m$. Øjensynlig er så $h_1 = 1$, og $h_m \leqslant n$. Følgen $h_1,\ldots,h_m$ kan alternativt bestemmes ud fra følgen $a_1,\ldots,a_m$, hvor a_i er antallet af tal h som opfylder $h_i < h < h_{i+1}$ (hvor $h_{m+1} := n+1$). Overvej nu:

de a_1 tal h med $h_1 < h < h_2$ ligger alle i X_1;
de a_2 tal h med $h_2 < h < h_3$ ligger i X_1 eller i X_2;
de a_3 tal h med $h_3 < h < h_4$ ligger i X_1 eller i X_2 eller i X_3; osv.

Slut heraf, at for en given følge $a_1,\ldots,a_m$ er der $1^{a_1}2^{a_2}\cdots m^{a_m}$ muligheder for klassedelingen. Vis herved, at

$$\begin{Bmatrix} n \\ m \end{Bmatrix} = \sum_{a_1+\cdots+a_m = n-m} 1^{a_1}2^{a_2}\cdots m^{a_m} = \sum_{1 \leqslant j_1 \leqslant j_2 \leqslant \cdots \leqslant j_{n-m} \leqslant m} j_1 j_2 \cdots j_{n-m}\,.$$

3. Cykliske grupper.

(3.1) Indledning. I det følgende betegner G en fast (multiplikativt skrevet) gruppe, med neutralt element e. Som nævnt i (1.6) kaldes en delmængde $H \subseteq G$ en *undergruppe* af G, hvis følgende betingelse er opfyldt:

(†) Delmængden H er stabil, det neutrale element e ligger i H, og for alle x i H ligger også x^{-1} i H.

Trivielt gælder betingelsen, når $H := G$ opfattes som delmængde af sig selv. Da $e{\cdot}e = e$ og $e^{-1} = e$, gælder betingelsen også for delmængden $H := \{e\}$. De to delmængder G og $\{e\}$ er altså undergrupper i G. De kaldes også de *trivielle undergrupper* af G. En undergruppe H kaldes en *ægte undergruppe*, hvis $H \subset G$.

I dette kapitel vil vi nærmere betragte de såkaldte *cykliske* undergrupper.

(3.2) Potenser. For hvert element $g \in G$ defineres *potensen* g^n med eksponent $n \in \mathbb{Z}$ således: For $n > 0$ sættes

$$g^n := \overbrace{g \cdot g \cdots g}^{n},$$

for $n = 0$ sættes $g^0 := e$, og for $n > 0$ sættes $g^{-n} := (g^{-1})^n$. Specielt, for $n = 1$, er $g^1 = g$, og for $n = -1$ er potensen g^{-1} det inverse element til g.

Herom gælder *potensreglerne*, for alle $n,\, p \in \mathbb{Z}$, og alle $g, h \in G$,

$$g^1 = g, \tag{0}$$

$$g^{p+n} = g^p\, g^n, \tag{1}$$

$$g^{pn} = (g^p)^n, \tag{2}$$

$$(gh)^n = g^n h^n, \quad \text{når } gh = hg. \tag{3}$$

Reglen (0) var jo en del af definitionen. Betragt de resterende potensregler. Når p og n er positive følger ligningerne umiddelbart: Vi har

$$\overbrace{g \cdots g}^{p+n} = \overbrace{g \cdots g}^{p} \cdot \overbrace{g \cdots g}^{n},$$

idet antallet af faktorer på højresiden er $p + n$; videre er

$$g^{pn} = (\overbrace{g \cdots g}^{p}) \cdots (\overbrace{g \cdots g}^{p}), \quad \text{med } n \text{ parenteser},$$

idet antallet af faktorer på højresiden er pn; endelig er

$$\overbrace{(gh) \cdots (gh)}^{n} = \overbrace{g \cdots g}^{n} \cdot \overbrace{h \cdots h}^{n},$$

thi af de $2n$ faktorer på venstresiden er n faktorer lig med g og n faktorer lig med h, og dem kan vi kommutere, da $gh = hg$.

Hvis $n = 0$ eller $p = 0$ følger de tre ligninger umiddelbart. Hvis p og/eller n er negative, kan de tre regler vises ved at opdele i en række tilfælde afhængige af fortegnene af tallene p, n, $p + n$ og pn.

Hvis gruppen G er kommutativ og additivt skrevet, anvendes altid *additiv notation* for potenserne: Den n'te potens af et element g, for $n > 0$, er bestemt som

$$\overbrace{g + g + \cdots + g}^{n},$$

Det er derfor naturligt at betegne den n'te potens med ng. For $n = 0$ er altså $0g = 0$ og for $n > 0$ er $(-n)g = n(-g)$. Med denne notation er potensreglerne følgende:

$$1g = g, \quad (p+n)g = pg + ng, \quad (pn)g = p(ng), \quad n(g+h) = ng + nh.$$

Bemærk, at den tredie potensregel er uden forbehold, idet en additivt skrevet gruppe altid antages at være kommutativ.

(3.3) Bemærkning. Alternativt kan potensreglerne bevises ved et induktionsargument. Hertil viser vi først, for et givet element $g \in G$, at potenserne $\pi(n) := g^n$, som funktion af $n \in \mathbb{Z}$, er *karakteriseret* ved ligningerne,

$$\pi(1) = g, \quad \pi(n+1) = \pi(n) \cdot g \text{ for alle } n \in \mathbb{Z}. \tag{$*$}$$

Eller anderledes udtrykt: Funktionen $\pi(n) := g^n$ opfylder ligningerne, dvs $g^1 = g$ og $g^{n+1} = g^n g$, og det er den eneste funktion, der gør det. Af (*) fås nemlig først $\pi(2) = \pi(1)g = g \cdot g$, dernæst $\pi(3) = \pi(2)g = g \cdot g \cdot g$, og induktivt, for $n > 0$, følger det, at $\pi(n) = g \cdots g$ med n faktorer. Videre fås af (*), ved multiplikation med g^{-1}, at $\pi(n) = \pi(n+1)g^{-1}$, og så fås $\pi(0) = \pi(1)g^{-1} = gg^{-1} = e$, dernæst $\pi(-1) = \pi(0)g^{-1} = eg^{-1} = g^{-1}$, dernæst $\pi(-2) = \pi(-1)g^{-1} = g^{-1} \cdot g^{-1}$, og induktivt, for $n > 0$, følger det, at $\pi(-n) = g^{-1} \cdots g^{-1}$ med n faktorer.

Af dette resultat kan vi udlede potensreglerne. For at vise den første betragtes, for et fast $p \in \mathbb{Z}$, funktionen $\pi(n) := (g^p)^{-1} g^{p+n}$. Øjensynlig er $\pi(1) = (g^p)^{-1} g^p g = g$, og

$$\pi(n+1) = (g^p)^{-1} g^{p+n+1} = (g^p)^{-1} g^{p+n} g = \pi(n) g.$$

Altså er ligningerne (*) opfyldt. Følgelig er $\pi(n) = g^n$, dvs $(g^p)^{-1} g^{p+n} = g^n$. Multiplikation med g^p fra venstre giver så den første potensregel.

For at vise den anden betragtes, for et fast $p \in \mathbb{Z}$, funktionen $\pi(n) := g^{pn}$. Øjensynlig er $\pi(1) = g^p$, og ved brug af første potensregel fås

$$\pi(n+1) = g^{pn+p} = g^{pn} g^p = \pi(n) g^p.$$

Altså er ligningerne (*) opfyldt med $g := g^p$. Følgelig er $\pi(n) = (g^p)^n$, dvs $g^{pn} = (g^p)^n$.

Antag nu, at $gh = hg$. For at vise den tredie potensregel viser vi først, at der for alle n gælder $gh^n = h^n g$. Hertil betragtes funktionen $\pi(n) := g^{-1} h^n g$. Øjensynlig er $\pi(1) = g^{-1} hg = g^{-1} gh = h$, og

$$\pi(n+1) = g^{-1} h^{n+1} g = g^{-1} h^n hg = g^{-1} h^n gh = \pi(n) h.$$

Følgelig er $\pi(n) = h^n$, dvs $g^{-1} h^n g = h^n$. Ved multiplikation med g fra venstre fås den ønskede ligning $h^n g = gh^n$. Dernæst betragtes funktionen $\pi(n) := g^n h^n$. Øjensynlig er $\pi(1) = gh$, og

$$\pi(n+1) = g^{n+1} h^{n+1} = g^n g h^n h = g^n h^n gh = \pi(n)(gh).$$

Følgelig er $\pi(n) = (gh)^n$, dvs $g^n h^n = (gh)^n$.

(3.4) Elementorden. For et element g i G er der to muligheder: Enten er $g^n \neq e$ for alle $n > 0$, eller også findes naturlige tal n således, at $g^n = e$. I det første tilfælde siges g at have *uendelig orden*, og vi skriver $|g| = \infty$. I det andet tilfælde defineres g's *orden*, betegnet $|g|$, som det mindste naturlige tal n således, at $g^n = e$.

Tallet 1 er det mindste naturlige tal, og vi har $g^1 = e$, hvis og kun hvis $g = e$. Heraf ses, at det neutrale element e i G altid har orden 1, og at alle andre elementer i G har orden større end 1.

(3.5) Sætning. *Lad g være et element i G. Da er delmængden,*

$$\langle g\rangle := \{\dots, g^{-2}, g^{-1}, e, g, g^2, g^3, \dots\},$$

bestående af alle potenser g^i, en undergruppe af G. Hvis g har uendelig orden, så gælder for alle hele tal i, j, at $g^i = g^j$, hvis og kun hvis $i = j$; i dette tilfælde er $\langle g\rangle$ uendelig. Hvis g har endelig orden n, så gælder for alle hele tal i, j, at $g^i = g^j$, hvis og kun hvis $i \equiv j \pmod{n}$; i dette tilfælde er de n potenser $e, g, \dots, g^{n-1}$ forskellige, og

$$\langle g\rangle = \{e, g, \dots, g^{n-1}\}; \tag{3.5.1}$$

specielt har $\langle g\rangle$ orden n.

I begge tilfælde gælder altså, at g's orden er lig med ordenen af undergruppen $\langle g\rangle$.

Bevis. Delmængden $\langle g\rangle$ er stabil, idet vi for to potenser g^i og g^j har $g^i g^j = g^{i+j} \in \langle g\rangle$ ifølge den første potensregel. Det neutrale element e tilhører $\langle g\rangle$, idet $e = g^0$. Endelig har vi for hver potens g^i, at $(g^i)^{-1} = g^{-i} \in \langle g\rangle$. Følgelig er $\langle g\rangle$ en undergruppe.

For hele tal i, j er $g^i = g^j$, hvis og kun hvis $g^{i-j} = e$. Den anden ligning fås nemlig af den første ved multiplikation med g^{-j}, og den første fås af den anden ved multiplikation med g^j.

Antag, at g har uendelig orden. Hvis $g^i = g^j$, kan vi antage, at $i \geqslant j$. Altså er $g^{i-j} = e$, hvor $i - j \geqslant 0$. Da g har uendelig orden, følger det, at $i - j = 0$, altså at $i = j$. Heraf ses, at $i \mapsto g^i$ er en injektiv afbildning $\mathbb{Z} \to G$. Billedmængden er øjensynlig $\langle g\rangle$, så specielt er $\langle g\rangle$ uendelig.

Antag, at g har endelig orden n. Betragt en potens g^k. Ifølge Sætningen om division med rest findes hele tal q og r således, at $k = qn + r$ og $0 \leqslant r < n$. Følgelig finder vi,

$$g^k = g^{qn+r} = (g^n)^q g^r = e^q g^r = g^r.$$

Heraf fremgår specielt, at venstresiden i (3.5.1) er indeholdt i højresiden, og dermed at lighed gælder. Da n er ordenen af g og $0 \leqslant r < n$, følger det yderligere, at $g^r = e$, hvis og kun hvis $r = 0$. Altså er $g^k = e$, hvis og kun hvis $r = 0$, dvs hvis og kun hvis $n \mid k$.

For hele tal i, j er $g^i = g^j$, hvis og kun hvis $g^{i-j} = e$. Af det lige viste, med $k := i - j$, følger derfor, at $g^i = g^j$, hvis og kun hvis $i \equiv j \pmod{n}$. Når $0 \leqslant i, j < n$, følger det specielt, at $g^i = g^j$, hvis og kun hvis $i = j$. De n potenser på højresiden af (3.5.1) er altså forskellige.

Hermed er påstandene også vist i tilfældet, hvor g har endelig orden. Sætningens sidste påstand er en umiddelbar konsekvens af det allerede viste. ▯

(3.6) Korollar. *Antag, at elementet g i G har endelig orden n. Da gælder for hvert helt tal k, at $g^k = e$, hvis og kun hvis n går op i k.*

Bevis. Påstanden er blot specialtilfældet $i := k$ og $j := 0$ i Sætningen. □

(3.7) Cyklisk gruppe. Hvis $g \in G$ har endelig orden n, følger det af Sætning (3.5), at potenserne g^i for $i = 0, \dots, n-1$ er forskellige, og at de herefter gentages *cyklisk*,

$$g^n = e, g^{n+1} = g, \dots, g^{2n-1} = g^{n-1}, g^{2n} = e, g^{2n+1} = g, \dots .$$

Undergruppen $\langle g \rangle$ bestående af alle potenser g^i kaldes, i alle tilfælde, den *cykliske undergruppe frembragt* af g. Det fremgår af Sætning (3.5), at undergruppens orden, altså elementantallet i $\langle g \rangle$, altid er lig med g's orden.

Hvis gruppen G er endelig, er $\langle g \rangle$ også endelig. Det første tilfælde i Sætning (3.5) er derfor udelukket. I en endelig gruppe har altså alle elementer endelig orden, endda højst orden lig med gruppens orden $|G|$. Vi skal senere se, at ordenen af et element altid er divisor i $|G|$.

Det er værd at bemærke, at hvis g ligger i en undergruppe H af G, så er $\langle g \rangle \subseteq H$, dvs alle potenser g^i tilhører H. Da H er stabil, får vi nemlig, for $i > 0$, at $g^i = g \cdots g \in H$. Trivielt er $g^0 = e \in H$. Og endelig får vi, for $i < 0$, at $g^i = (g^{-i})^{-1} \in H$. Altså er $\langle g \rangle \subseteq H$.

Gruppen G kaldes en *cyklisk gruppe*, hvis der findes et element $g \in G$således, at $G = \langle g \rangle$.

Bemærk, at „regning" i en cyklisk gruppe $G = \langle g \rangle$ foregår ved addition af eksponenterne: $g^i g^j = g^{i+j}$. Hvis gruppen har endelig orden n, kan eksponenterne adderes modulo n. Bemærk specielt, at en cyklisk gruppe er kommutativ, idet $g^i g^j = g^{i+j} = g^{j+i} = g^j g^i$.

(3.8) Eksempel. Betragt gruppen $\mathbb{Z}$, af hele tal med addition som komposition. For et helt tal g er den additive potens ng blot produktet $n \cdot g$. Den cykliske undergruppe $\langle g \rangle$ frembragt af et helt tal g består altså af alle produkter,

$$\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}.$$

Denne undergruppe betegnes også $g\mathbb{Z}$ eller $\mathbb{Z}g$. For $g = 0$ fås den trivielle undergruppe $\mathbb{Z}0 = \{0\}$ bestående alene af 0. For $g = 1$ har vi øjensynlig $\mathbb{Z}1 = \mathbb{Z}$. Gruppen $\mathbb{Z}$ er altså den cykliske gruppe frembragt af tallet 1. For $g > 1$ er $\mathbb{Z}g$ en ikke-triviel undergruppe af $\mathbb{Z}$; den består af de hele tal, som er multipla af g.

(3.9) Eksempel. Betragt den (additive) restklassegruppe $\mathbb{Z}/n$, defineret i (1.11). For en restklasse $[x]$ i $\mathbb{Z}/n$ og $i > 0$ får vi for den additive potens,

$$i[x] = \overbrace{[x] + \cdots + [x]}^{i} = \left[\overbrace{x + \cdots + x}^{i}\right] = [ix].$$

For $i = 0$ har vi $0[x] = [0] = [0x]$, og for $i < 0$ får vi $i[x] = -(-i)[x] = -[-ix] = [ix]$. Ligningen $i[x] = [ix]$ gælder altså for alle hele tal i. Specielt får vi for $x = 1$, at $i[1] = [i]$. Den cykliske undergruppe frembragt af restklassen [1] består altså af alle restklasser $[i]$. Restklassegruppen $\mathbb{Z}/n$ er altså cyklisk, frembragt af restklassen [1].

(3.10) Eksempel. Betragt for et naturligt tal n den (multiplikative) gruppe $(\mathbb{Z}/n)^*$ af primiske restklasser. Elementerne i $(\mathbb{Z}/n)^*$ er restklasser $[a]$ modulo n, hvor a er primisk med n. Det neutrale element er restklassen [1], og øjensynlig er $[a]^d = [a^d]$. Ordenen af en primisk restklasse $[a]$ er altså det mindste positive tal d således, at $[a^d] = [1]$, eller, med andre ord, det mindste positive tal d således, at

$$a^d \equiv 1 \pmod{n}.$$

Restklassen [1] har orden 1 og restklassen $[-1]$ har orden 2, når $n > 2$. I almindelighed er der ikke nogen „formel" til bestemmelse af ordenen.

Betragt for eksempel de primiske restklasser modulo 7. Der er 6 restklasser, [1], [2], [3], [4], [5], [6]. Vi finder

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 1;$$
$$3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1.$$

Det følger, at restklassen [2] har orden 3 og at restklassen [3] har orden 6. Specielt ses, at gruppen $(\mathbb{Z}/7)^*$ er cyklisk, frembragt af restklassen [3]. Man kan vise, at der for hvert primtal p gælder, at gruppen $(\mathbb{Z}/p)^*$ af primiske restklasser modulo p er cyklisk.

(3.11) Eksempel. Den cykliske (multiplikative) gruppe C_n, defineret i (1.13), består af de n potenser ζ_n^a, for $a = 0, \dots, n-1$, hvor $\zeta_n = e^{2\pi i/n}$. Vi har $\zeta_n^n = 1$, så ζ_n har orden n. Gruppen C_n er altså den cykliske undergruppe af $\mathbb{C}^*$ frembragt af ζ_n.

(3.12) Eksempel. Diedergruppen D_4 har orden 8. Den består af identiteten id, af to drejninger D og D^{-1} med vinkler $\pm\pi/2$, videre af D^2, som er drejningen med vinklen π (eller multiplikation med -1), samt endelig af 4 spejlinger $S_i = D^i S$ for $i = 0, \dots, 3$. Drejningerne D og D^{-1} har orden 4, og de frembringer den samme cykliske undergruppe af orden 4. Drejningen D^2 har orden 2, og frembringer altså en cyklisk undergruppe af orden 2. Spejlingerne har ligeledes orden 2, og hver spejling frembringer altså en cyklisk undergruppe af orden 2.

De cykliske undergrupper af D_4 er således gruppen $\langle \mathrm{id} \rangle = \{\mathrm{id}\}$ bestående alene af identiteten, den cykliske undergruppe $\langle D \rangle$ af orden 4 frembragt af D, heri den cykliske undergruppe $\langle D^2 \rangle$ af orden 2, samt yderligere 4 undergrupper $\langle S_i \rangle$ af orden 2 frembragt af de 4 spejlinger.

(3.13) Eksempel. Kvaterniongruppen Q_8 har orden 8. Identiteten $\mathbf{1}$ frembringer den trivielle gruppe $\langle \mathbf{1} \rangle = \{\mathbf{1}\}$. Matricen $-\mathbf{1}$ frembringer en cyklisk undergruppe af orden 2. For matricen $\mathbf{i}$ har vi $\mathbf{i}^1 = \mathbf{i}$, $\mathbf{i}^2 = -\mathbf{1}$, og dermed $\mathbf{i}^3 = -\mathbf{i}$ og $\mathbf{i}^4 = \mathbf{1}$. Matricen $\mathbf{i}$ har altså orden 4, og

$$\langle \mathbf{i} \rangle = \{\mathbf{1}, \mathbf{i}, -\mathbf{1}, -\mathbf{i}\}$$

er altså en cyklisk undergruppe af orden 4. Tilsvarende har vi yderligere to cykliske undergrupper $\langle \mathbf{j} \rangle$ og $\langle \mathbf{k} \rangle$ af orden 4.

(3.14) Eksempel. Lad X være en endelig mængde, og betragt den fulde permutationsgruppe S_X. For en p-cykel $\gamma = (x_1 \ldots x_p)$ har vi øjensynlig $\gamma^i(x_j) = x_{j+i}$, hvor indices regnes modulo p, og $\gamma^i(x) = x$, når x er forskelligt fra x_j'erne. For $i = 1, \ldots, p-1$ følger det specielt, at $\gamma^i(x_1) = x_{i+1} \neq x_1$. Altså er $\gamma^i \neq \mathrm{id}$ for $i = 1, \ldots, p-1$. Videre følger det, at $\gamma^p = \mathrm{id}$. Heraf ses, at en p-cykel har orden p.

Betragt nu en vilkårlig permutation σ. Ifølge Cykelsætningen er σ et produkt,

$$\sigma = \gamma_1 \cdots \gamma_r, \tag{1}$$

af parvis disjunkte cykler γ_s. Da $\gamma_s\gamma_t = \gamma_t\gamma_s$, følger det af tredie potensregel, at

$$\sigma^i = \gamma_1^{\,i} \cdots \gamma_r^{\,i}.$$

Betragt en cykel γ_s i fremstillingen. Lad os antage, at γ_s er p-cyklen $\gamma_s = (x_1 \ldots x_p)$. Elementerne x_j er netop de elementer, der flyttes af γ_s; alle andre elementer er fixpunkter for γ_s. Det følger specielt, at hvert element der flyttes af $\gamma_s^{\,i}$ må være et af x_j'erne. Heraf ses, at $\sigma^i = \mathrm{id}$, hvis og kun hvis $\gamma_s^{\,i} = \mathrm{id}$ for $s = 1, \ldots, r$. Hvis γ_s er en p_s-cykel, altså af orden p_s, har vi altså $\sigma^i = \mathrm{id}$, hvis og kun hvis $p_s \mid i$ for $s = 1, \ldots, r$. Ordenen af σ er altså det mindste fælles multiplum af ordenerne af de disjunkte cykler γ_s i fremstillingen (1).

(3.15) Lemma. *Lad g være et element i G af endelig orden n. Da har potensen g^t orden n/d, hvor $d = (t, n)$ er største fælles divisor for t og n. Yderligere gælder, at $\langle g^t \rangle = \langle g^d \rangle$.*

Bevis. Potensen g^t tilhører undergruppen $\langle g \rangle$, som ifølge antagelsen har den endelige orden n. Specielt følger det, at g^t har endelig orden. For hvert helt tal k gælder følgende to biimplikationer:

$$(g^t)^k = e \iff n \mid tk \iff \frac{n}{d} \mid k.$$

Den første biimplikation følger nemlig af Korollar (3.6), og den anden er en velkendt egenskab ved største fælles divisor.

Nu fremgår det umiddelbart, at ordenen af g^t, altså det mindste positive tal k således, at $(g^t)^k = e$, er lig med det mindste positive tal k, som er et multiplum af n/d. Ordenen er altså lig med n/d.

For at vise ligheden $\langle g^t \rangle = \langle g^d \rangle$ bemærker vi først, at vi har $t = qd$, da d er divisor i t. Følgelig er $g^t = (g^d)^q \in \langle g^d \rangle$. Elementet g^t tilhører altså undergruppen $\langle g^d \rangle$, og heraf følger $\langle g^t \rangle \subseteq \langle g^d \rangle$. For at vise den omvendte inklusion benytter vi, at den største fælles divisor d har en fremstilling $d = xt + yn$, hvor x, y er hele tal. Følgelig er $g^d = g^{xt+yn} = (g^t)^x (g^n)^y = (g^t)^x e^y = (g^t)^x$. Altså er $g^d \in \langle g^t \rangle$, og dermed $\langle g^d \rangle \subseteq \langle g^t \rangle$.

Hermed er lemmaet bevist. □

(3.16) Sætning. *Antag, at G er en cyklisk gruppe, $G = \langle g \rangle$. Da er enhver undergruppe H af G ligeledes cyklisk. Hvis G er uendelig, og $H \neq \{e\}$, så er H uendelig. Hvis G har endelig orden n, så er H's orden divisor i n, og for hver divisor d i n findes præcis én undergruppe af orden d, nemlig undergruppen $\langle g^{n/d} \rangle$, og der findes præcis $\varphi(d)$ elementer af orden d.*

Bevis. Da $G = \langle g \rangle$, er hvert element i G en potens g^i. Det skal vises, for en given undergruppe $H \subseteq G$, at $H = \langle g^t \rangle$ med en passende eksponent t. For den trivielle undergruppe $H = \{e\}$ har vi øjensynlig $H = \langle g^0 \rangle$. Antag derfor, at $H \neq \{e\}$, altså at der i H findes et element $g^j \neq e$. Specielt er så $j \neq 0$, og da vi også har $g^{-j} = (g^j)^{-1} \in H$, kan vi antage, at $j > 0$. Der findes altså positive tal j således, at $g^j \in H$. Lad nu t være det mindste positive tal således, at $g^t \in H$. Sæt $h_0 := g^t$. Det påstås, at

$$H = \langle h_0 \rangle. \tag{1}$$

Elementet h_0 tilhører H, og følgelig er $\langle h_0 \rangle \subseteq H$. For at vise den omvendte inklusion betragtes et vilkårligt element $h = g^i$ i H. Ifølge Sætningen om division med rest findes hele tal q, r således, at $i = qt + r$ og $0 \leqslant r < t$. Nu er

$$h = g^i = g^{qt+r} = g^{tq} g^r = (h_0)^q g^r.$$

Vi har $g^r = h_0^{-q} h$, og da H er en undergruppe, følger det at $g^r \in H$. Desuden er $0 \leqslant r < t$. Valget af t, som den mindste positive tal med $g^t \in H$, sikrer derfor, at $r = 0$. Altså er $g^r = e$, og så er $h = h_0^q \in \langle h_0 \rangle$. Hermed er den omvendte inklusion, og dermed ligningen (1), bevist.

Antag, at $G = \langle g \rangle$ er uendelig og at $H \neq \{e\}$. Da har g uendelig orden, og $H = \langle g^t \rangle$ med $t > 0$. Følgelig er $(g^t)^i = g^{ti} \neq e$ for $i > 0$, og så er $H = \langle g^t \rangle$ uendelig.

Antag endelig, at G er endelig, af orden n, altså at frembringeren g har orden n. Lad d være divisor i n. Så har $g^{n/d}$ orden d, så undergruppen $\langle g^{n/d} \rangle$ har orden d. Antag omvendt, at H er en undergruppe i G. Ifølge det allerede viste er H cyklisk, $H = \langle g^t \rangle$, og så følger det af Lemma (3.15), at $H = \langle g^{n/d} \rangle$ med en passende divisor d i n. Denne divisor må være H's orden, da $\langle g^{n/d} \rangle$ har orden d. Hermed har vi vist, at H's orden er divisor i n, og at undergruppen $\langle g^{n/d} \rangle$, for en divisor d i n, er den eneste undergruppe af orden d.

Elementet g^t frembringer G, netop når g^t har orden n. Af Lemma (3.15) følger, at det sker præcis, når t er primisk med n; den cykliske gruppe G har altså $\varphi(n)$ frembringere. Elementerne af orden d er frembringerne for den entydigt bestemte cykliske undergruppe af orden d. Af det lige viste, med $n := d$, ses så, at antallet af sådanne elementer er $\varphi(d)$. □

(3.17) Lemma. *Lad g og h være elementer i G af endelige ordener n og m. Antag, at $gh = hg$. Da har gh endelig orden, og ordenen er divisor i nm. Hvis n og m er primiske, har gh orden nm. Hvis n og m ikke er primiske, har gh orden mindre end nm.*

Bevis. Ifølge tredie potensregel er $(gh)^i = g^i h^i$. Hvis $n \mid i$ og $m \mid i$, har vi $g^i = e$ og $h^i = e$, og følgelig er $(gh)^i = e$. Specielt, for $i := mn$, slutter vi, at $(gh)^{nm} = e$, og heraf følger, at gh's orden er divisor i nm. Mere præcist slutter vi, at når k er det mindste fælles multiplum af n og m, så er $(gh)^k = e$. Ordenen af gh er altså divisor i det mindste fælles multiplum k.

Hvis n og m ikke er primiske, så er det mindste fælles multiplum mindre end produktet nm. I dette tilfælde har gh altså orden mindre end nm.

Antag nu, at m og n er primiske. For at bestemme ordenen af gh betragtes et helt tal i således, at $(gh)^i = e$. Sæt $x := g^i$. Da er

$$x = g^i = h^{-i}.$$

Af $x = g^i$ følger, at x har en orden, der er divisor i n, og af $x = h^{-i}$ følger, at x har en orden, der er divisor i m. Følgelig har x orden 1. Altså er $x = e$. Da $e = g^i$, er i et multiplum af n og da $e = h^i$, er i et multiplum af m. Følgelig er i et multiplum af mn. Det mindste positive multiplum af mn er mn. Heraf følger, at gh har orden mn. ∎

(3.18) Eksempel. I (3.17) er det essentielt, at g og h kommuterer. Betragt fx i gruppen $SL_2(\mathbb{Z})$ følgende 3 matricer,

$$s := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \qquad t := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad v := \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}.$$

En let udregning giver $s^2 = -1$ og $s^4 = 1$ (hvor 1 er enhedsmatricen), og følgelig har s orden 4. Videre er $v^3 = 1$, så v har orden 3. Produktet sv er matricen t, og vi finder

$$t^i = \begin{bmatrix} 1 & i \\ 0 & 1 \end{bmatrix}.$$

Potensen t^i er altså kun lig med 1, når $i = 0$. Produktet $t = sv$ har altså uendelig orden.

(3.19) Produkt af grupper. For to givne grupper G_1 og G_2 betragtes produktmængden $G := G_1 \times G_2$ bestående af par (g_1, g_2). I produktmængden G defineres *koordinatvis komposition* ved

$$(g_1, g_2)(h_1, h_2) := (g_1h_1\ ,\ g_2h_2).$$

Det er umiddelbart at se, at produktmængden G med denne komposition er en gruppe. Den kaldes *produktgruppen*, eller det *direkte produkt* af G_1 og G_2. Det neutrale element i G er parret $e = (e_1, e_2)$, hvor e_1 og e_2 er de neutrale elementer i G_1 og G_2, og det inverse til (g_1, g_2) er parret (g_1^{-1}, g_2^{-1}).

Betragt et par $g = (g_1, g_2) \in G$. Øjensynlig er $g^i = (g_1^i, g_2^i)$. Altså har vi biimplikationerne,

$$g^i = e \iff (g_1^i, g_2^i) = (e_1, e_2) \iff g_1^i = e_1 \text{ og } g_2^i = e_2.$$

Antag, at g_1 og g_2 har endelige ordener k_1 og k_2. Det følger af biimplikationerne, at $g^i = e$, hvis og kun hvis $k_1 \mid i$ og $k_2 \mid i$. Ordenen af parret $g = (g_1, g_2)$ er derfor det mindste fælles multiplum af k_1 og k_2.

(3.20) Sætning. *Lad G_1 og G_2 være cykliske grupper af endelige ordener n_1 og n_2. Da er produktgruppen $G_1 \times G_2$ cyklisk, hvis og kun hvis n_1 og n_2 er primiske.*

Bevis. Lad m være det mindste fælles multiplum for n_1 og n_2. Som bekendt er $m = n_1n_2/d$, hvor d er den største fælles divisor for n_1, n_2. Specielt er $m = n_1n_2$, hvis n_1 og n_2 er primiske, og $m < n_1n_2$, hvis n_1 og n_2 ikke er primiske.

For et par $g = (g_1, g_2)$ i produktgruppen $G = G_1 \times G_2$ er der n_1 muligheder for g_1 og n_2 muligheder for g_2. Produktgruppen G har altså orden n_1n_2. Lad k_1 og k_2 være ordenerne af g_1 og g_2. Da G_1 er cyklisk af orden n_1, er k_1 divisor i n_1. Følgelig er k_1 divisor i m, som var et multiplum af n_1. Tilsvarende er k_2 divisor i m. Som nævnt i (3.19), følger det, at g's orden er divisor i m.

Antag først, at n_1 og n_2 ikke er primiske. Da er $m < n_1 n_2$. Da hvert element $g \in G$ ifølge det viste har en orden, som er divisor i m, har intet element i G orden $n_1 n_2$. Gruppen G, som har orden $n_1 n_2$, er derfor ikke cyklisk.

Antag dernæst, at n_1 og n_2 er primiske. Vælg som g_1 en frembringer for G_1, altså et element af orden n_1 i G_1, og vælg tilsvarende g_2 af orden n_2 i G_2. Da n_1 og n_2 er primiske, har elementet $g = (g_1, g_2)$ orden $n_1 n_2$, og det frembringer derfor gruppen G. Gruppen G er således cyklisk. □

(3.21) Eksempel. Gruppen $\mathrm{C}_4 \times \mathrm{C}_3$ har orden $4 \cdot 3 = 12$. Den er cyklisk.

Gruppen $\mathrm{C}_2 \times \mathrm{C}_2$ har orden 4. Den kaldes også *Klein's Vierer-gruppe*. Den er ikke cyklisk.

(3.22) Opgaver.

1. Bestem i hver af grupperne $\mathbb{R}^*_+$, $\mathbb{R}^*$, $\mathbb{C}^*$, og $\mathbb{U}$ de elementer, der har endelig orden.

2. Hvilke tal kan være orden af et element i den additive gruppe $\mathbb{R}$?

3. Angiv en primisk restklasse modulo 17, hvis orden i gruppen $(\mathbb{Z}/17)^*$ er lig med 16.

4. Hvilke permutationer i S_4 har orden 2?

5. Angiv symmetrierne af orden 2 i diedergruppen D_n.

6. Hvilke ordener har symmetrierne i diedergruppen D_6?

7. Vis, for elementer g, h i en gruppe G, at g og hgh^{-1} altid har samme orden. Vis, at gh og hg altid har samme orden.

8. Vis, for et element g i en gruppe G, at g og g^{-1} har samme orden. Vis, at hvis G har lige orden, så findes der et element af orden 2 i G.

9. Betragt n-cyklen $\gamma = (1\,2\,\ldots\,n)$ i S_n. Lad d være ordenen af potensen γ^i. Vis, at cykelfremstillingen af γ^i er et produkt af n/d cykler af længde d.

10. En cyklisk gruppe G har orden 2006. Bestem antallet af frembringere for G.

11. Lad G være en cyklisk gruppe af orden n. Vis for hvert naturligt tal k, at antallet af løsninger $g \in G$ til ligningen $g^k = e$ er lig med den største fælles divisor (n, k).

12. Lad G være en uendelig cyklisk gruppe og lad $H \neq \{e\}$ være en vilkårlig gruppe. Vis, at $G \times H$ ikke er cyklisk.

13. Vis, at en permutation af ulige orden i S_n må være en lige permutation.

14. Angiv de mulige cykeltyper for permutationer i S_n af orden 2.

15. Giv et eksempel på en endelig gruppe, der indeholder to elementer g, h således, at g og h har orden 2 og gh har orden 3.

16. Vis, at enhver p-gruppe, dvs en ikke-triviel gruppe hvis orden er en potens af *primtallet* p, indeholder et element af orden p.

4. Sideklasser.

(4.1) Indledning. Lad G være en fast (multiplikativt skrevet) gruppe. Produkt af elementer i G udvides umiddelbart til en komposition (produkt) af delmængder, idet vi for $A, B \subseteq G$ sætter

$$AB := \{ab \mid a \in A \text{ og } b \in B\}.$$

Lad H være en undergruppe af G. For hvert element $g \in G$ kan vi da betragte produktet gH, altså delmængden,

$$gH := \{gh \mid h \in H\}.$$

Delmængder af G af denne form kaldes *sideklasser modulo H*. En delmængde A af G er altså en sideklasse, hvis der findes et element $g \in G$ således, at $A = gH$.

Hvert element $g \in G$ bestemmer en sideklasse, nemlig sideklassen gH, men, som vi skal se, kan to forskellige elementer g og g' bestemme den samme sideklasse: vi kan have $gH = g'H$ for $g \neq g'$. Antallet af sideklasser kaldes undergruppens *index* i G, og det betegnes $|G{:}H|$. Mængden af sideklasser betegnes G/H. Index er altså elementantallet i mængden G/H. Hvis der er uendelig mange sideklasser, skrives $|G{:}H| = \infty$.

I dette kapitel viser vi, hvordan sideklasserne modulo en given undergruppe H deler gruppen G i lige store delmængder. Dette (helt elementære) resultat spiller en hovedrolle i mange kombinatoriske anvendelser af gruppeteori. Desuden viser vi, at hvis H er en *normal* undergruppe, så er der en naturlig komposition i mængden af sideklasser. Med denne komposition bliver mængden G/H af sideklasser selv en gruppe, *kvotientgruppen*.

(4.2) Lagrange's Indexsætning. *Sideklasserne modulo en given undergruppe H udgør en klassedeling af G, og to elementer x, x' i G ligger i den samme sideklasse, hvis og kun hvis $x^{-1}x' \in H$. Hver sideklasse har samme elementantal som H, og antallet af sideklasser er bestemt ved formlen,*

$$|G| = |G{:}H| \cdot |H|.$$

Bevis. Det skal først vises, at sideklasserne udgør en klassedeling af G, altså at sideklasserne ikke er tomme og at G er den disjunkte forening af sideklasserne. Den sidste betingelse betyder, at hvert element i G ligger i præcis én sideklasse.

En sideklasse er en delmængde af formen gH. Da $g = ge$, slutter vi, at $g \in gH$. Altså er sideklasserne ikke tomme, og elementet g ligger i sideklassen gH. Vi mangler at vise, for $g \in G$, at gH er den eneste sideklasse, der indeholder g. Antag derfor, at g ligger i sideklassen $g'H$. Da er $g = g'h_0$ med $h_0 \in H$. Da H er en undergruppe, gælder for hvert element $h \in H$, at $h_0h \in H$ og $h_0^{-1}h \in H$, og dermed, at

$$gh = g'h_0h \in g'H, \qquad g'h = gh_0^{-1}h \in gH.$$

Altså er $gH \subseteq g'H$ og $g'H \subseteq gH$. Følgelig er $g'H = gH$. Hermed er vist, at sideklassen gH er den eneste sideklasse, der indeholder g.

Elementet $x \in G$ tilhører sideklassen xH. Hvis elementer x og x' tilhører samme sideklasse, må denne sideklasse altså være xH. Følgelig er $x' \in xH$. Vi har altså $x' = xh$ med

$h \in H$, og så er $x^{-1}x' = h \in H$. Antag omvendt, at $x^{-1}x' \in H$. Da er $x' = xx^{-1}x' \in xH$, og da også $x \in xH$, ligger x og x' i samme sideklasse, nemlig i xH.

En vilkårlig sideklasse har formen gH. Ved $h \mapsto gh$ defineres øjensynlig en surjektiv afbildning $H \to gH$. Afbildningen er også injektiv, thi hvis $gh_1 = gh_2$, fås ved multiplikation med g^{-1} fra venstre, at $h_1 = h_2$. Afbildningen $H \to gH$ er altså bijektiv. Følgelig har H og gH samme elementantal.

Da sideklasserne udgør en klassedeling af G, kan elementantallet i G, når G er endelig, bestemmes ved at addere elementantallene i sideklasserne. Alle sideklasser har samme elementantal, så additionen giver antallet af sideklasser, $|G{:}H|$, ganget med det fælles elementantal, $|H|$, hvilket er den søgte formel.

Hvis G er uendelig, må enten H være uendelig eller antallet af sideklasser være uendeligt (eller begge dele), og det er, med oplagt regning med ∞, indholdet af formlen i dette tilfælde.

Hermed er Indexsætningen bevist. □

(4.3) Korollar. *For en undergruppe H af en endelig gruppe G gælder, at undergruppens orden, $|H|$, og index, $|G{:}H|$, er divisorer i $|G|$.*

Bevis. Af Indexsætningen fremgår, at $|H|$ og $|G{:}H|$ endda er komplementære divisorer i den forstand, at deres produkt er lig med $|G|$. □

(4.4) Observation. Klassedelinger svarer som bekendt til ækvivalensrelationer, og ækvivalensrelationen svarende til sideklasserne modulo H er bestemt i sætningen: to elementer x, x' i G er ækvivalente, hvis og kun hvis $x^{-1}x' \in H$. Ækvivalente elementer siges også at være *kongruente modulo H*, og vi skriver:

$$x' \equiv x \pmod{H} \overset{\text{DEF}}{\iff} x^{-1}x' \in H.$$

Sideklassen gH er ækvivalensklassen, der indeholder g, og den kan også betegnes $[g]$. Mængden af sideklasser G/H er altså kvotienten af G mht ækvivalensrelationen. Den *kanoniske afbildning* $G \to G/H$ er afbildningen, der til et element $g \in G$ knytter den ækvivalensklasse, som indeholder g; det er altså afbildningen $g \mapsto gH$.

Hvis index $|G{:}H| = r$ er endeligt, er der r sideklasser, $g_1H, \dots, g_rH$, og G er den disjunkte forening,

$$G = g_1H \cup \cdots \cup g_rH.$$

Hvis gruppen G er (kommutativ og) additivt skrevet, bruges den additive notation naturligvis også for kompositionen af delmængder, indført i (4.1). Summen af to delmængder $A, B \subseteq G$ er altså delmængden,

$$A + B = \{a + b \mid a \in A \text{ og } b \in B\}.$$

For en undergruppe H af en sådan gruppe er sideklassen, der indeholder g, altså delmængden $g + H$. Kongruens modulo H får her formen,

$$x' \equiv x \pmod{H} \iff x' - x \in H.$$

(4.5) Eksempel. For den trivielle undergruppe $H := \{e\}$ har vi $g\{e\} = \{g\}$. Sideklasserne er altså delmængderne med ét element, og vi kan identificere $G/\{e\}$ med G. Specielt er antallet af sideklasser lig med elementantallet i G, altså $|G{:}\{e\}| = |G|$.

Den anden trivielle undergruppe er $H := G$. Her er $eG = G$, så der er kun én sideklasse modulo G. Specielt er $|G{:}G| = 1$.

Betragt i den additive gruppe $\mathbb{Z}$ undergruppen $n\mathbb{Z}$ bestående af alle multipla af et givet naturligt tal n. En sideklasse er her en delmængde af $\mathbb{Z}$ af formen $a + n\mathbb{Z}$, bestående af tal $a + qn$ for $q \in \mathbb{Z}$. Sideklasserne er altså restklasserne modulo n, og kongruens modulo undergruppen $n\mathbb{Z}$ er kongruens modulo n. Der er som bekendt n restklasser, så $|\mathbb{Z} : n\mathbb{Z}| = n$.

(4.6) Eksempel. Betragt den symmetriske gruppe $G = \mathrm{S}_3$, af orden $3! = 6$. Transpositionen $\tau = (1\,2)$ har orden 2, så $H := \langle\tau\rangle$ er en undergruppe af orden 2. Der er altså 3 sideklasser. Idet σ betegner 3-cyklen $(1\,2\,3)$ finder vi,

$$H = \{(1)\,,\ (1\,2)\}, \qquad \sigma H = \{(1\,2\,3)\,,\ (1\,3)\}, \qquad \sigma^2 H = \{(1\,3\,2)\,,\ (2\,3)\}.$$

Sideklasserne H, σH og $\sigma^2 H$ er altså de tre sideklasser, og $|\,\mathrm{S}_3 : H| = 3$.

(4.7) Korollar. *Et vilkårligt element g i en endelig gruppe G har en orden, som er divisor i $|G|$. Specielt gælder altid ligningen,*

$$g^{|G|} = e.$$

Bevis. Lad d være ordenen af g. Ifølge (3.5) har undergruppen $\langle g\rangle$ orden d. Af Korollar (4.3) følger så, at d er divisor i $|G|$.

Da d er divisor i $|G|$, har vi $|G| = qd$ med et helt tal q, og følgelig er

$$g^{|G|} = g^{qd} = (g^d)^q = e^q = e.$$

Hermed er de to påstande bevist. ∎

(4.8) Korollar. *En gruppe G, hvis orden er et primtal p, er cyklisk. Mere præcist gælder for hvert element $g \neq e$ i G, at $G = \langle g\rangle$.*

Bevis. For et element $g \neq e$ har den cykliske undergruppe $\langle g\rangle$ orden større end 1, da den indeholder e og g. Da ordenen er divisor i primtallet p, må ordenen altså være p. Altså har delmængden $\langle g\rangle$ samme elementantal som G, og følgelig er $\langle g\rangle = G$. ∎

(4.9) Fermat's lille Sætning. *Hvis primtallet p ikke er divisor i det hele tal a, så er*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Bevis. For et primtal p har vi $\varphi(p) = p - 1$. Hvis p ikke går op i a, er a og p primiske. Derfor er Fermat's lille Sætning indeholdt i det følgende resultat. ∎

(4.10) Euler's generalisering. *Lad n være et naturligt tal, og lad a være et helt tal primisk med n. Da gælder kongruensen,*

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \tag{4.10.1}$$

hvor $\varphi(n)$ er Euler's φ-funktion.

Bevis. Da a er primisk med n er restklassen $[a]$ en primisk restklasse. Altså er $[a]$ element i gruppen $(\mathbb{Z}/n)^*$. Denne gruppe har orden $\varphi(n)$, og restklassen $[1]$ er det neutrale element. Af Korollar (4.7) får vi derfor ligningen $[a]^{\varphi(n)} = [1]$. Denne ligning mellem restklasser modulo n er ækvivalent med kongruensen (4.10.1). ∎

(4.11) Lemma. *For undergrupper H, K af G gælder, at fællesmængden $H \cap K$ er en undergruppe og produktet HK er en foreningsmængde af sideklasser modulo K. For elementantallet i HK gælder ligningen,*

$$|HK| = |H : H \cap K| \cdot |K|. \tag{4.11.1}$$

Hvis $K \subseteq H$ gælder ligningen,

$$|G{:}K| = |G{:}H| \cdot |H{:}K|. \tag{4.11.2}$$

Bevis. Det er let at se, at fællesmængden $H \cap K$ af to undergrupper selv er en undergruppe. Produktet HK er øjensynlig foreningsmængden af sideklasserne hK for $h \in H$. To forskellige af disse sideklasser er disjunkte, og elementantallet i hver af dem er $|K|$. Det er altså indholdet i (4.11.1), at antallet af disse sideklasser er lig med index $|H : H \cap K|$.

Index $|H : H \cap K|$ er antallet af sideklasser af formen $h(H \cap K)$, for $h \in H$. Det er altså påstanden, at antallet af sideklasser af formen $h(H \cap K)$, for $h \in H$, er lig med antallet af sideklasser af formen hK, for $h \in H$. Hertil undersøges, for $h, h_1 \in H$, inklusionen,

$$h_1(H \cap K) \subseteq hK. \tag{1}$$

Den er øjensynlig opfyldt for $h_1 = h$. Enhver sideklasse af den første form er altså indeholdt i en sideklasse af den anden form og enhver sideklasse af den anden form indeholder en sideklasse af den første form. For at vise, at der er lige mange sideklasser af de to former, er det derfor nok at vise, at en sideklasse af den anden form kun indeholder én sideklasse af den første form. Det skal med andre ord vises, at hvis inklusionen (1) er opfyldt, så er sideklassen $h_1(H \cap K)$ lig med sideklassen $h(H \cap K)$.

Antag altså, at inklusionen (1) er opfyldt, med $h, h_1 \in H$. Elementet h_1 ligger på venstresiden, og dermed i hK. Vi har altså $h_1 = hk$ med $k \in K$. Da H er en undergruppe og $k = h^{-1}h_1$, er $k \in H$. Altså er $k \in H \cap K$. Følgelig er $h_1 = hk \in h(H \cap K)$, og heraf følger $h_1(H \cap K) = h(H \cap K)$, som ønsket. Hermed er (4.11.1) bevist.

Antag nu, at $K \subseteq H$. Betragt først tilfældet, hvor K har endeligt index r i H. Da har vi en deling af H i en foreningsmængde af r disjunkte sideklasser,

$$H = h_1K \cup \cdots \cup h_rK.$$

Afbildningen $x \mapsto gx$ er en bijektiv afbildning af G på sig selv (med $y \mapsto g^{-1}y$ som den inverse). Den afbilder øjensynlig H på gH og sideklassen hK på sideklassen ghK. Følgelig er sideklassen gH den disjunkte forening af de r sideklasser gh_iK. Antallet af sideklasser i G/K er derfor r gange antallet af sideklasser af formen gH, altså $r \cdot |G{:}H|$, hvilket er ligningen (4.11.2).

Hvis $|H{:}K| = \infty$, er der uendelig mange sideklasser af formen hK for $h \in H$. Specielt er der uendelig mange sideklasser i G/K. Begge sider af (4.11.2) er altså ∞ i dette tilfælde. ∎

(4.12) Eksempel. Bortset fra valg af betegnelser er der præcis to grupper af orden 6. Antag nemlig, at G er en gruppe af orden 6. De mulige ordener af elementerne i G er da 1, 2, 3 og 6.

Det er udelukket, at alle elementer $g \neq e$ har orden 2. Antag nemlig, indirekte, at $g^2 = e$ for alle $g \in G$. Hvert element i G har da sig selv som det inverse. Vælg to forskellige elementer τ_1 og τ_2 af orden 2. Produktet $\tau_1\tau_2$ er da forskelligt fra e, τ_1, τ_2, og lig med sin egen inverse,

$$\tau_1\tau_2 = (\tau_1\tau_2)^{-1} = \tau_2^{-1}\tau_1^{-1} = \tau_2\tau_1.$$

Vi har altså $\tau_1^2 = \tau_2^2 = e$ og $\tau_1\tau_2 = \tau_2\tau_1$. Heraf følger let, at de fire elementer $e, \tau_1, \tau_2, \tau_1\tau_2$ udgør en undergruppe af G. Dette er imidlertid i modstrid med Indexsætningen, da G har orden 6.

Der findes altså i G et element af orden 3 eller 6. Hvis g har orden 6, har g^2 orden 3. Altså findes i G et element σ af orden 3. Lad $K = \{e, \sigma, \sigma^2\}$ være den cykliske undergruppe frembragt af σ. Det påstås, at K er den eneste undergruppe i G af orden 3. Antag nemlig, indirekte, at $H \neq K$ er endnu en undergruppe af orden 3. Fællesmængden $H \cap K$ er da en undergruppe af K. Ordenen af $H \cap K$ er derfor divisor i 3. Ordenen kan ikke være 3, da $K \not\subseteq H$. Altså er $|H \cap K| = 1$. Af (4.11.1) følger derfor, at $|HK| = 3 \cdot 3 = 9$, hvilket er en modstrid, da G kun indeholder 6 elementer.

Da K er den eneste undergruppe af orden 3, følger det specielt, at σ og $\sigma^2 = \sigma^{-1}$ er de eneste elementer af orden 3. Hvis g har orden 6, har g^3 orden 2. Følgelig findes i G et element τ af orden 2. Da $\tau \notin K$, er K og τK de to sideklasser. Vi har altså $G = K \cup \tau K$, så G består af de 6 elementer i listen,

$$e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2.$$

Produkt af vilkårlige to af disse 6 elementer er igen et element i listen. Vi har $\sigma^3 = e$ og $\tau^2 = e$. For at bestemme produktet af vilkårlige to elementer er det derfor nok at afgøre, hvor i listen produktet $\sigma\tau$ befinder sig. Det er let at se, at $\tau^{-1}\sigma\tau$ har samme orden som σ, altså orden 3. Følgelig må $\tau^{-1}\sigma\tau$ enten være σ eller σ^2. I det første tilfælde har vi $\sigma\tau = \tau\sigma$, idet andet tilfælde er $\sigma\tau = \tau\sigma^2$. Vi har altså de to muligheder,

$$\sigma\tau = \tau\sigma \quad \text{eller} \quad \sigma\tau = \tau\sigma^2.$$

Vi har således vist, at i en gruppe G af orden 6 findes elementer τ af orden 2 og σ af orden 3 således, at gruppens elementer er de seks elementer i listen. Yderligere er multiplikation i G bestemt ved en af de to muligheder ovenfor. Der er derfor højst to muligheder for gruppen G, bortset fra valg af betegnelser for elementerne i G. Det er klart, at ved den første mulighed er G kommutativ, ved den anden mulighed er G ikke-kommutativ. Da vi kender en kommutativ gruppe, nemlig den cykliske gruppe C_6, og en ikke-kommutativ gruppe, nemlig den symmetriske gruppe S_3, forekommer begge muligheder.

(4.13) Normale undergrupper. For en given undergruppe H af G kan man, svarende til definitionen i (4.1), betragte delmængder af formen,

$$Hg = \{hg \mid h \in H\},$$

for elementer $g \in G$. Delmængder af denne form kaldes *højre-sideklasser modulo* H, og mængden af højre-sideklasser kan betegnes $H\backslash G$. Sideklasserne betragtet i (4.1) kaldes også *venstre-sideklasser*. (Huskeregel: $H\emptyset$ er en Højre-sideklasse.)

Hvis A er en venstre-sideklasse modulo H, så er delmængden $A^{-1} := \{a^{-1} \mid a \in A\}$ en højre-sideklasse. Mere præcist gælder $(gH)^{-1} = Hg^{-1}$. Heraf følger let, at der ved $A \mapsto A^{-1}$ defineres en bijektiv afbildning fra mængden af venstre-sideklasser på mængden af højre-sideklasser. Specielt er antallet af højre-sideklasser modulo H lig med antallet af venstre-sideklasser, altså lig med index $|G{:}H|$.

Hvis G er kommutativ, er øjensynlig $gH = Hg$, men hvis G ikke er kommutativ, vil klassedelingerne med venstre-sideklasser og med højre-sideklasser i almindelighed være forskellige.

En undergruppe N af G siges at være en *normal undergruppe*, hvis den opfylder en af følgende tre ækvivalente betingelser:

(i) For alle $g \in G$ gælder $gN = Ng$.
(ii) For alle $g \in G$ gælder $gNg^{-1} = N$.
(iii) For alle $g \in G$ gælder $gNg^{-1} \subseteq N$.

Betingelserne er ækvivalente. Er nemlig ligningen i (i) opfyldt, får vi ligningen i (ii) ved multiplikation med g^{-1} fra højre, og tilsvarende fås (i) af (ii) ved multiplikation med g fra højre. Ligningen i (ii) medfører naturligvis inklusionen i (iii). Antag endelig, at inklusionen i (iii) gælder for alle g. For $g := g^{-1}$ følger det så, at $g^{-1}Ng \subseteq N$. Ved multiplikation med g fra venstre og g^{-1} fra højre fås inklusionen $N \subseteq gNg^{-1}$. Sammenligning med inklusionen i (iii) giver så ligheden i (ii).

Hvis gruppen G er kommutativ, er $gh = hg$ for alle g, h. Ligningen i (i) gælder derfor altid. I en kommutativ gruppe er altså enhver undergruppe normal.

(4.14) Lemma. *Lad N være en normal undergruppe i G. Der findes da netop en komposition '$*$' i mængden G/N af sideklasser modulo N således, at der for alle elementer $g_1, g_2 \in G$ gælder, at*

$$(g_1N) * (g_2N) = g_1g_2N. \tag{4.14.1}$$

Med denne komposition er G/N en gruppe, hvis neutrale element er sideklassen $N = eN$.

Bevis. Betragt modulo N to sideklasser A_1 og A_2. Vælg elementer $g_1 \in A_1$ og $g_2 \in A_2$. Da er $A_1 = g_1N$ og $A_2 = g_2N$. Ligningen (4.14.1) fastlægger derfor kompositet $A_1 * A_2$ som sideklassen g_1g_2N. Men ligningen definerer ikke uden videre kompositionen '$*$'. Hertil kræves, at definitionen er „lovlig". En sideklasse A kan jo skrives på formen gN med et vilkårligt element $g \in A$. I definitionen indgår et valg af g_1 og g_2, og det skal sikres, at højresiden er uafhængig af dette valg. Et alternativt valg er givet ved elementer $g_1' \in g_1N$ og $g_2' \in g_2N$. Det skal vises, at $g_1g_2N = g_1'g_2'N$. Da $g_1' \in g_1N$ og $g_2' \in g_2N$, er $g_1' = g_1k_1$ og $g_2' = g_2k_2$ med $k_1, k_2 \in N$. Altså har vi ligningen,

$$g_1'g_2' = g_1k_1g_2k_2 = g_1g_2(g_2^{-1}k_1g_2)k_2.$$

På højresiden er $g_2^{-1}k_1g_2 \in N$, fordi $k_1 \in N$ og N er normal. Altså er $(g_2^{-1}k_1g_2)k_2 \in N$. Af ligningen følger derfor, at $g_1'g_2' \in g_1g_2N$. Altså er $g_1'g_2'N = g_1g_2N$, som ønsket. Hermed er vist, at definitionen af '$*$'er lovlig.

Nu følger det umiddelbart, at G/N er en gruppe: For tre sideklasser g_1N, g_2N og g_3N får vi, at

$$(g_1N * g_2N) * g_3N = (g_1g_2N) * g_3N = (g_1g_2)g_3N = g_1g_2g_3N,$$

og tilsvarende er $g_1N * (g_2N * g_3N) = g_1g_2g_3N$. Altså er '$*$' associativ. Af (4.14.1) følger umiddelbart, at sideklassen $N = eN$ er neutralt element for '$*$'. Endelig får vi, for $g \in G$, at

$$gN * g^{-1}N = gg^{-1}N = eN = N, \text{ og } g^{-1}N * gN = g^{-1}gN = eN = N,$$

og heraf fremgår, at sideklassen $g^{-1}N$ er den inverse til sideklassen gN.

Hermed er lemmaet bevist. □

(4.15) Definition. Når N er en normal undergruppe i G, er kvotienten G/N, altså mængden af sideklasser modulo N, en gruppe med kompositionen beskrevet i (4.14). Den kaldes *kvotientgruppen* af G modulo N. Når G er multiplikativt skrevet, vil vi også skrive kompositionen i G/N multiplikativt. Produktet af sideklasser er altså fastlagt ved ligningen,

$$(g_1N)(g_2N) = g_1g_2N.$$

Hvis G er en kommutativ, additivt skrevet gruppe, skrives kompositionen i kvotientgruppen også additivt. Sum af sideklasser er her fastlagt ved ligningen,

$$(g_1{+}N) + (g_2{+}N) = (g_1 + g_2) + N.$$

(4.16) Eksempel. Den trivielle undergruppe $N := \{e\}$ er altid normal, idet vi har $geg^{-1} = e$ for alle elementer $g \in G$. Sideklasserne modulo $\{e\}$ er delmængderne med ét element, så de svarer til elementerne i G. Kvotientgruppen $G/\{e\}$ kan altså naturligt identificeres med gruppen G.

Den anden trivielle undergruppe er $N := G$. Der er kun den ene sideklasse $G = eG = Ge$. Specielt er G en normal undergruppe i G, og kvotientgruppen G/G er en gruppe med ét element. Kvotientgruppen er altså den trivielle gruppe C_1.

I en kommutativ gruppe er enhver undergruppe normal, og kvotientgruppen G/N er altså defineret for enhver undergruppe N. Det er klart, at kvotientgruppen igen er kommutativ.

Betragt, for et givet $n \geqslant 1$, undergruppen $n\mathbb{Z}$ i den additive gruppe $\mathbb{Z}$. Sideklasserne er restklasser modulo n, og komposition af sideklasser defineret i (4.14) er netop den velkendte addition af restklasser. Kvotientgruppen $\mathbb{Z}/n\mathbb{Z}$ er altså den additive gruppe $\mathbb{Z}/n$ af restklasser modulo n.

Undergruppen $H = \langle\tau\rangle$ af S_3, behandlet i Eksempel (4.6), består af $\tau = (1\,2)$ og identiteten. For 3-cyklen $\sigma = (1\,2\,3)$ finder vi

$$\sigma\tau\sigma^{-1} = (1\,2\,3)(1\,2)(3\,2\,1) = (2\,3).$$

Altså er $\sigma\tau\sigma^{-1} \notin H$. Undergruppen H er derfor ikke normal i S_3.

(4.17) Observation. En undergruppe N af index 2 i G er altid normal. Det skal hertil vises, at venstre-sideklasser og højre-sideklasser er de samme: $gN = Ng$ for alle g. Dette følger af, at der er netop to sideklasser (både venstre- og højre-). Den ene er N, og den anden må derfor være komplementærmængden af N i G.

(4.18) Eksempel. Af Lagrange's Indexsætning fremgår, at ordenen af en undergruppe af G altid er divisor i $|G|$. Der gælder ikke omvendt, at der for enhver divisor d i $|G|$ eksisterer en undergruppe af orden d.

For eksempel har den alternerende gruppe A_4 af orden 12 ingen undergrupper af orden 6. Antag nemlig, indirekte, at $N \subseteq A_4$ er en undergruppe af orden 6. Da har N index 2, og N er følgelig normal i A_4. Kvotientgruppen A_4/N er derfor en gruppe af orden 2. Det følger specielt for hvert element $g \in A_4$, at sideklassen gN opfylder $(gN)^2 = N$. Altså gælder $g^2 \in N$ for hvert element $g \in A_4$. En 3-cykel $(a\,b\,c)$ er en lige permutation, og vi har $(a\,b\,c) = (a\,c\,b)^2$. Altså vil enhver 3-cykel tilhøre N. Men dette er en modstrid, da der er 8 cykler af længde 3 i A_4 og kun 6 elementer i N.

(4.19) Opgaver.

1. Betragt den multiplikative gruppe $\mathbb{C}^*$. Angiv for undergruppen $\mathbb{R}^*$ sideklasserne $z\mathbb{R}^*$. Besvar det tilsvarende spørgsmål for undergrupperne $\mathbb{U}$ og $\mathbb{R}^*_+$ af $\mathbb{C}^*$. Lad K være cirkelskiven bestemt ved uligheden $|w - 1| \leqslant \frac{1}{2}$. Beskriv delmængderne zK for $z \in \mathbb{C}^*$. Udgør de en klassedeling af $\mathbb{C}^*$?

2. Betragt den additive gruppe $\mathbb{C}$, med undergruppen $\mathbb{R}$. Angiv sideklasserne $z + \mathbb{R}$. Lad K være cirkelskiven bestemt ved uligheden $|w| \leqslant 1$. Beskriv delmængderne $z + K$. Udgør de en klassedeling af $\mathbb{C}$?

3. Vis for den additive gruppe $\mathbb{R}$, at undergruppen $\mathbb{Z}$ har uendeligt index. Hvilket index har undergruppen $\mathbb{Q}$?

4. Den cykliske gruppe C_9 består af potenserne af $\zeta := e^{2\pi i/9}$. Vis, at potenserne $1, \zeta^3, \zeta^6$ udgør en undergruppe H af C_9. Marker på en figur de 3 sideklasser uH for $u \in C_9$.

5. Lad H og K være undergrupper af orden n og m i en gruppe G. Vis, at hvis $(n, m) = 1$, så er $H \cap K = \{e\}$.

6. Lad a, b være hele tal, der ikke begge er lig med 0. Vis ligningerne,

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}, \qquad a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z},$$

hvor d er den største fælles divisor for a, b, og m er det mindste fælles multiplum.

7. Vis, at for hver restklasse a i $(\mathbb{Z}/21)^*$ er $a^{12} = [1]$. Hvilke elementer i $(\mathbb{Z}/21)^*$ har den største orden?

8. Vis, for to forskellige ulige primtal p og q, at gruppen $(\mathbb{Z}/pq)^*$ har orden $(p-1)(q-1)$. Vis, at gruppen ikke kan være cyklisk. [Vink: brug Den kinesiske Restklassesætning.]

9. Vis, for Euler's φ-funktion, at $\sum_{d|n} \varphi(d) = n$.

10. Lad T og U være mængden af reelle 2×2-matricer af, henholdsvis, formerne,

$$\begin{bmatrix} \mu & a \\ 0 & \nu \end{bmatrix}, \quad \text{og} \quad \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix},$$

hvor $\mu\nu \neq 0$ for matricerne i T. (1) Vis, at U og T er undergrupper af $\mathrm{GL}_2(\mathbb{R})$. (2) Vis, at U er en kommutativ gruppe, og at T ikke er kommutativ. (3) Vis, at U er en normal undergruppe af T, og beskriv, for en given matrix $t \in T$, sideklassen tU. (4) Vis, at T/U er kommutativ. (5) Vis, at T ikke er normal i $\mathrm{GL}_2(\mathbb{R})$.

11. Lad H og G^+ være undergrupper af en gruppe G. Antag, at G^+ har index 2 i G, og sæt $H^+ := H \cap G^+$. Hvornår er $H^+ = H$? Vis, at hvis $H \not\subseteq G^+$, så har H^+ index 2 i H.

12. Hvilke undergrupper af kvaterniongruppen Q_8 er normale? Samme spørgsmål for diedergruppen D_4.

13. Bestem samtlige undergrupper i A_4, og angiv de normale.

14. Vis, at hvis K og N er normale undergrupper af G, så er KN og $K \cap N$ også normale undergrupper.

15. Vis for en normal undergruppe N af gruppen G, at sideklassen gN i kvotientgruppen G/N har en orden, der er divisor i ordenen af g. Vis, at hvis G er endelig og G/N har et element af orden d, så har gruppen G et element af orden d.

16. Lad N være en normal undergruppe af gruppen G. Antag, at N og G/N er cykliske og at deres ordener er primiske. Vis, at hvis gruppen G er kommutativ, så er den cyklisk.

17. *Sæt $U := (\mathbb{Z}/p^\nu)^*$, hvor p er et ulige primtal. Lad U_0 være delmængden bestående af restklasser $[u]$ modulo p^ν for $u \equiv 1 \pmod{p}$. Vis, at U_0 er en undergruppe af U. Vis, fx ved induktion efter ν, at

$$(1+p)^{p^{\nu-1}} \equiv 1 + p^\nu \pmod{p^{\nu+1}}.$$

Slut heraf, at restklassen $[1+p]$ i U_0 har orden $p^{\nu-1}$, og dernæst, at U_0 er cyklisk af orden $p^{\nu-1}$. Fik du brug for, at p var ulige? Man kan vise, at gruppen $(\mathbb{Z}/p)^*$ er cyklisk. Slut heraf, at gruppen $U = (\mathbb{Z}/p^\nu)^*$ er cyklisk.

18. Vis, at gruppen $(\mathbb{Z}/2^\nu)^*$ ikke er cyklisk, når $\nu \geqslant 3$.

19. For hvilke n er gruppen $(\mathbb{Z}/n)^*$ cyklisk?

20. For elementer g, h i en gruppe G er *kommutatoren* elementet $[g,h] := ghg^{-1}h^{-1}$. Vis, for en undergruppe N af G, at følgende betingelser er ækvivalente:

(i) N indeholder alle kommutatorer.
(ii) N er normal og kvotientgruppen G/N er kommutativ.

21. Lad G være en gruppe og lad G' være *kommutatorundergruppen*, dvs undergruppen frembragt af alle kommutatorer. Vis, at G' er en normal undergruppe og at kvotientgruppen G/G' er kommutativ. Vis, at kommutatorundergruppen G' er den mindste blandt de normale undergrupper N således, at G/N er kommutativ. Bestem G' for $G = \mathrm{D}_3, \mathrm{D}_4, \mathrm{S}_3, \mathrm{Q}_8$.

22. *Vis, at hvis $g^k = e$ for alle elementer g i en endelig kommutativ gruppe G, så er $|G|$ divisor i en potens af k. [Vink: Vis påstanden ved fuldstændig induktion efter $|G|$. I induktionsskridtet betragtes en kvotientgruppe G/H, hvor H er en (næsten vilkårlig) undergruppe af G.]

23. Vis, at der er præcis to ikke-kommutative grupper af orden 8, nemlig . . . .

24. *Vis, at der findes uendelig mange primtal p med $p \equiv 1 \pmod 4$. [Vink: sæt $x := 2p_1 \cdots p_k$ og kig på en primdivisor p i $x^2 + 1$. Vis og udnyt, at $x \pmod p$ har orden 4 i gruppen $(\mathbb{Z}/p)^*$.] (Dirichlet's sætning udsiger mere generelt, at når $(a, n) = 1$, så findes der uendelig mange primtal p med $p \equiv a \pmod n$.)

25. *Bestem kommutatorundergrupperne S_n' og A_n'. [Vink: For $n \geqslant 5$ er enhver 3-cykel en kommutator af to 3-cykler. Undersøg også, hvad der sker for $n \leqslant 4$.]

26. Lad N være en normal undergruppe af gruppen G. To sideklasser, $A_1 = g_1N$ og $A_2 = g_2N$, er specielt delmængder af G. Produktet A_1A_2 har derfor to definitioner, i GRP(4.1) og i GRP(4.15). Giver de to definitioner samme resultat?

5. Homomorfi og isomorfi.

(5.1) Definition. Lad G og G' være grupper. En afbildning $\varphi\colon G \to G'$ kaldes en *gruppe-homomorfi* eller blot en *homomorfi*, hvis der for alle $x, y \in G$ gælder, at

$$\varphi(xy) = \varphi(x)\varphi(y). \tag{5.1.1}$$

En bijektiv gruppehomomorfi kaldes også en *(gruppe-)isomorfi*.

I (5.1.1) har vi antaget, at begge grupper G og G' er multiplikativt skrevne. Det skal understreges, at produktet xy på venstresiden er kompositet i G og at produktet $\varphi(x)\varphi(y)$ på højresiden er kompositet i G'. Hvis G og G' er (kommutative) additivt skrevne grupper, får betingelsen formen

$$\varphi(x + y) = \varphi(x) + \varphi(y); \tag{5.1.2}$$

den får formen $\varphi(x + y) = \varphi(x)\varphi(y)$, hvis fx G er additivt skrevet og G' er multiplikativt skrevet.

Det fremgår af (5.1.2) at homomorfier mellem grupper er analoge til lineære afbildninger mellem vektorrum, og de spiller en tilsvarende fundamental rolle. I dette kapitel kigger vi nærmere på homomorfier og isomorfier, og vi viser tre fundamentale isomorfisætninger.

(5.2) Observation. For en gruppehomomorfi $\varphi\colon G \to G'$ gælder ligningerne,

$$\varphi(e) = e', \qquad \varphi(x^{-1}) = \varphi(x)^{-1},$$

hvor e og e' i den første ligning er det neutrale element i henholdsvis G og G'. Med $w := \varphi(e)$ har vi nemlig $ww = \varphi(e)\varphi(e) = \varphi(ee) = \varphi(e) = w$, altså $ww = w$. Ved multiplikation med w^{-1} fås $w = e'$. Altså er $\varphi(e) = e'$. Videre har vi ligningerne,

$$\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(e) = e',$$

og heraf følger, at $\varphi(x^{-1}) = \varphi(x)^{-1}$.

(5.3) Kerne og billede. Lad $\varphi\colon G \to G'$ være en gruppehomomorfi. For hver undergruppe $H \subseteq G$ er billedmængden $\varphi(H)$ en undergruppe af G'. For $y_1, y_2 \in \varphi(H)$ har vi nemlig $y_1 = \varphi(h_1)$ og $y_2 = \varphi(h_2)$ med $h_1, h_2 \in H$, og så er $y_1y_2 = \varphi(h_1)\varphi(h_2) = \varphi(h_1h_2)$. Da H er en stabil delmængde af G, er $h_1h_2 \in H$, og følgelig er $y_1y_2 \in \varphi(H)$. Altså er $\varphi(H)$ en stabil delmængde af G'. Videre er $e' = \varphi(e) \in \varphi(H)$, så det neutrale element tilhører $\varphi(H)$. Er endelig $y \in \varphi(H)$, så er $y = \varphi(h)$ og dermed $y^{-1} = \varphi(h^{-1}) \in \varphi(H)$. Altså er $\varphi(H)$ en undergruppe af G'.

Specielt ses, at billedmængden $\varphi(G)$ er en undergruppe af G'. Den kaldes også *billed-gruppen* eller *billedet* for homomorfien φ.

For hver undergruppe H' af G' er originalmængden $\varphi^{-1}(H')$ en undergruppe af G. For $x_1, x_2 \in \varphi^{-1}(H')$ har vi nemlig $\varphi(x_1), \varphi(x_2) \in H'$. Da H' er en stabil delmængde af G', følger det, at $\varphi(x_1x_2) = \varphi(x_1)\varphi(x_2) \in H'$, og følgelig er $x_1x_2 \in \varphi^{-1}(H')$. Altså er $\varphi^{-1}(H')$ en stabil delmængde af G. Videre er $\varphi(e) = e' \in H'$, så det neutrale element e tilhører $\varphi^{-1}(H')$. Er endelig $x \in \varphi^{-1}(H')$, så er $\varphi(x) \in H'$, og det følger, at $\varphi(x^{-1}) = \varphi(x)^{-1} \in H'$; altså er $x^{-1} \in \varphi^{-1}(H')$.

Specielt ses, at originalmængden $\varphi^{-1}(e')$ er en undergruppe af G. Den kaldes også *kernen* for homomorfien φ.

(5.4) Lemma. *For enhver gruppehomomorfi $\varphi\colon G \to G'$ er kernen $\varphi^{-1}(e')$ en normal undergruppe af G. Endvidere er φ injektiv, hvis og kun hvis $\varphi^{-1}(e') = \{e\}$.*

Bevis. Som nævnt i (5.3) er kernen $N := \varphi^{-1}(e')$ en undergruppe af G. Hvis $h \in N$ og $g \in G$, får vi

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)e'\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e',$$

og heraf fremgår, at $ghg^{-1} \in N$. Altså er N en normal undergruppe.

Antag, at φ er injektiv. Hvis $x \in N$, så er $\varphi(x) = e' = \varphi(e)$, og følgelig er $x = e$. Altså er $N = \{e\}$. Antag omvendt, at $N = \{e\}$. Lad x_1, x_2 være elementer i Gsåledes, at $\varphi(x_1) = \varphi(x_2)$. Da er

$$\varphi(x_1x_2^{-1}) = \varphi(x_1)\varphi(x_2)^{-1} = e',$$

og altså $x_1x_2^{-1} \in N = \{e\}$. Følgelig er $x_1x_2^{-1} = e$, og altså $x_1 = x_2$. Afbildningen φ er derfor injektiv. □

(5.5) Eksempler. (0) Den *trivielle homomorfi* $\varphi\colon G \to G'$ er afbildningen defineret ved $\varphi(g) = e'$ for alle $g \in G$. Den er øjensynlig en homomorfi. Dens kerne er G, og dens billedgruppe er den trivielle undergruppe $\{e'\}$ af G'.

(1) Hvis $H \subseteq G$ er en undergruppe, så er inklusionsafbildningen, $x \mapsto x$ for $x \in H$, en injektiv homomorfi $H \to G$. Dens kerne er den trivielle undergruppe $\{e\}$ af H.

(2) Lad $N \subseteq G$ være en normal undergruppe. Ligningen (4.14.1) bestemmer produktet i kvotientgruppen G/N. Det følger af ligningen, at den kanoniske afbildning, $x \mapsto xN$, er en homomorfi $G \to G/N$. Den kaldes også den *kanoniske homomorfi*. Øjensynlig er den surjektiv. Dens kerne er den givne normale undergruppe N, thi sideklassen N er det neutrale element i G/N, og vi har $xN = N$, hvis og kun hvis $x \in N$.

(3) Lad g være et element i gruppen G. Ifølge Første Potensregel er $g^{i+j} = g^ig^j$. Med andre ord er afbildningen $i \mapsto g^i$ en gruppehomomorfi $\mathbb{Z} \to G$. Billedgruppen er den cykliske undergruppe $\langle g\rangle$. Kernen består af de hele tal i, for hvilke $g^i = e$. Ifølge (5.4) er kernen en undergruppe af $\mathbb{Z}$, og afbildningen $i \mapsto g^i$ er injektiv, hvis og kun hvis $g^i \neq e$ for alle $i \neq 0$. Hvis afbildningen $i \mapsto g^i$ ikke er injektiv, er kernen en undergruppe forskellig fra $\{0\}$ i $\mathbb{Z}$. Den er derfor cyklisk af formen $\mathbb{Z}n$ med et tal $n > 0$. Det er klart, at tallet n netop er ordenen af g.

(4) Ifølge Sætning (2.20) er fortegnet for permutationer en homomorfi $\mathrm{sign}\colon \mathrm{S}_n \to \{\pm 1\}$. Homomorfien er surjektiv, når $n > 1$. Kernen for homomorfien er undergruppen A_n bestående af alle lige permutationer. Undergruppen A_n er altså en normal undergruppe af S_n.

(5) For eksponentialfunktionen $x \mapsto e^x$ gælder som bekendt ligningen $e^{x+y} = e^xe^y$, og e^x er altid forskellig fra 0. Eksponentialfunktionen er altså en homomorfi,

$$\exp\colon \mathbb{R} \to \mathbb{R}^*,$$

fra den additive gruppe af reelle tal til den multiplikative gruppe af reelle tal forskellige fra 0. Som bekendt er eksponentialfunktionen injektiv og billedet er mængden af positive reelle tal. De positive tal udgør en undergruppe $\mathbb{R}^*_+$ af den multiplikative gruppe $\mathbb{R}^*$, og vi kan opfatte eksponentialfunktionen som en isomorfi $\mathbb{R} \to \mathbb{R}^*_+$. Den inverse afbildning er logaritmefunktionen, der er en isomorfi $\log\colon \mathbb{R}^*_+ \to \mathbb{R}$.

Som bekendt gælder, at den komplekse eksponentialfunktion er en surjektiv homomorfi,

$$\exp\colon \mathbb{C} \to \mathbb{C}^*.$$

Dens kerne er undergruppen $2\pi i\mathbb{Z}$ bestående af komplekse tal af formen $2\pi i q$ med $q \in \mathbb{Z}$.

Tilsvarende definerer $\theta \mapsto e^{i\theta}$ en surjektiv homomorfi,

$$\mathbb{R} \to \mathbb{U},$$

af den additive gruppe $\mathbb{R}$ på den multiplikative gruppe $\mathbb{U}$ af komplekse fortegn. Dens kerne er undergruppen $2\pi\mathbb{Z}$.

(6) For determinant af matricer gælder som bekendt ligningen $\det(AB) = \det(A)\det(B)$. Heraf ses, at determinanten definerer en homomorfi,

$$\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*.$$

Kernen, der består af matricerne med determinant 1, er den specielle lineære gruppe $\mathrm{SL}_n(\mathbb{R})$. Denne undergruppe er altså normal i den generelle lineære gruppe $\mathrm{GL}_n(\mathbb{R})$.

(5.6). Lad $\kappa\colon G \to \overline{G}$ være en given homomorfi mellem grupper G og $\overline{G}$. For en gruppehomomorfi $\overline{\varphi}\colon \overline{G} \to H$ er den sammensatte afbildning $\overline{\varphi}\kappa$ en homomorfi $G \to H$. En homomorfi $\varphi\colon G \to H$, der har formen $\varphi = \overline{\varphi}\kappa$ med en (passende) homomorfi $\overline{\varphi}\colon \overline{G} \to H$, siges at være *induceret via* κ af homomorfien $\overline{\varphi}$ (eller bare: *induceret fra* $\overline{G}$).

Homomorfisætningen. *Lad der være givet en surjektiv gruppehomomorfi $\kappa\colon G \to \overline{G}$, og lad $N := \kappa^{-1}(\bar{e})$ betegne kernen. Da gælder for en vilkårlig gruppehomomorfi $\varphi\colon G \to H$, at φ er induceret fra $\overline{G}$, hvis og kun hvis $\varphi(N) = \{e\}$.*

Bevis. Hvis φ er induceret via κ af $\overline{\varphi}$, altså $\varphi = \overline{\varphi}\kappa$, så er $\varphi(N) = \overline{\varphi}(\kappa(N)) = \overline{\varphi}(\{\bar{e}\}) = \{e\}$.

Antag omvendt, at $\varphi(N) = \{e\}$. Det skal vises, at der findes en homomorfi $\overline{\varphi}\colon \overline{G} \to H$ således, at $\varphi = \overline{\varphi}\kappa$, altså en homomorfi $\overline{\varphi}\colon \overline{G} \to H$, som opfylder ligningerne,

$$\overline{\varphi}(\kappa(x)) = \varphi(x), \quad \text{for alle } x \in G. \tag{5.6.1}$$

Disse ligninger fastlægger afbildningen $\overline{\varphi}$: Da κ er surjektiv, har hvert element $y \in \overline{G}$ nemlig formen $y = \kappa(x)$ med $x \in G$, og så er $\overline{\varphi}(y) = \overline{\varphi}(\kappa(x)) = \varphi(x)$. For den søgte homomorfi $\overline{\varphi}$ må der altså gælde, at

$$\overline{\varphi}(y) = \varphi(x), \quad \text{når } y = \kappa(x), \tag{*}$$

og hermed er værdien $\overline{\varphi}(y)$ bestemt. Specielt kan der højst være én afbildning $\overline{\varphi}$ således, at ligningerne (5.6.1) er opfyldt.

Vi viser nu, at (*) er en *lovlig definition* af en afbildning $\overline{\varphi}\colon \overline{G} \to H$. Man kan også kalde definitionen i (*) en „dynamisk definition“: For at bestemme værdien $\overline{\varphi}(y)$ skal vi foretage et valg, nemlig vælge et element $x \in G$ med $\kappa(x) = y$, og „lovligheden“ betyder, at den opnåede værdi er uafhængig af det foretagne valg. Det er let at indse uafhængigheden: For et andet valg, lad os sige $x' \in G$ med $\kappa(x') = y$, er $\kappa(x') = \kappa(x)$. Heraf følger, at $x'x^{-1}$ ligger i kernen for κ, altså i N. Antagelsen om at $\varphi(N) = \{e\}$ sikrer så, at $\varphi(x'x^{-1}) = e$, og det medfører, da φ er en homomorfi, at $\varphi(x') = \varphi(x)$. Højresiden i (*) er altså uafhængig af det foretagne valg.

Videre er afbildningen $\overline{\varphi}\colon \overline{G} \to H$ en homomorfi. Betragt nemlig to elementer y_1, y_2 i $\overline{G}$. Vælg i G elementer x_1, x_2 således, at $y_1 = \kappa(x_1)$ og $y_2 = \kappa(x_2)$. Da er $y_1 y_2 = \kappa(x_1)\kappa(x_2) = \kappa(x_1 x_2)$. Af (*) følger derfor, at

$$\overline{\varphi}(y_1 y_2) = \varphi(x_1 x_2) = \varphi(x_1)\varphi(x_2) = \overline{\varphi}(y_1)\overline{\varphi}(y_2).$$

Altså er $\overline{\varphi}$ en homomorfi. Endelig fremgår det umiddelbart af (*), at for $x \in G$ er $\overline{\varphi}(\kappa(x)) = \varphi(x)$. Derfor er φ induceret via κ af $\overline{\varphi}$. □

(5.7) Observation. I Homomorfisætningen indgår betingelsen, at $\varphi(N) = \{e\}$, altså at der for alle $x \in N$ gælder $\varphi(x) = e$, hvor e er det neutrale element i H. Hvis H er en additivt skrevet kommutativ gruppe, så er kravet, at $\varphi(x) = 0$ for alle $x \in N$. I analogi med dette tilfælde udtrykker man ofte betingelsen $\varphi(N) = \{e\}$ ved at sige, at φ *forsvinder* på N.

Standardanvendelsen af sætningen er på den kanoniske homomorfi $\kappa\colon G \to G/N$, bestemt ved $g \mapsto gN$, hvor N er en given normal undergruppe af G. Hvis en homomorfi $\varphi\colon G \to H$ forsvinder på N, så findes ifølge Homomorfisætningen en homomorfi $\overline{\varphi}\colon G/N \to H$ således, at

$$\overline{\varphi}([g]) = \varphi(g), \tag{5.7.1}$$

hvor $[g] = gN$. Det fremgår af beviset for Homomorfisætningen, at $\overline{\varphi}$ er entydigt bestemt. Man siger også, at homomorfien $\overline{\varphi}\colon G/N \to H$ er *induceret* af φ.

(5.8) Isomorfisætningen. *Lad $\varphi\colon G \to G'$ være en gruppehomomorfi, og lad $N := \varphi^{-1}(e')$ betegne kernen. Da fastlægger forskriften,*

$$xN \mapsto \varphi(x),$$

en veldefineret isomorfi $G/N \xrightarrow{\sim} \varphi(G)$ af G modulo kernen på billedgruppen $\varphi(G)$.

Bevis. At forskriften bestemmer en veldefineret afbildning svarer til at definitionen er lovlig: For at anvende forskriften til at bestemme billedet af en sideklasse S, skal man skrive sideklassen på formen $S = xN$; man skal altså vælge et element x i sideklassen S for at bestemme billedet af S. Det skal altså vises, at det opnåede billedelement i G' ikke afhænger af det foretagne valg. Antag hertil, at x og x' begge ligger i sideklassen S. Så er $x' \in xN$, altså $x' = xh$ med $h \in N$. Da $N = \varphi^{-1}(e')$, følger det, at $\varphi(x') = \varphi(xh) = \varphi(x)$. Hermed er vist, at definitionen er lovlig. Øjensynlig udgør de opnåede billedelementer netop delmængden $\varphi(G)$ af G'. Forskriften bestemmer altså en surjektiv afbildning $\overline{\varphi}\colon G/N \to \varphi(G)$.

Afbildningen $\overline{\varphi}$ er en homomorfi. Betragt hertil to sideklasser $S, T \in G/N$. Vælg repræsentanter: $S = xN$ og $T = yN$. Produktet af sideklasserne er da sideklassen $ST = xyN$. Altså er

$$\overline{\varphi}(ST) = \overline{\varphi}(xyN) = \varphi(xy) = \varphi(x)\varphi(y) = \overline{\varphi}(S)\overline{\varphi}(T).$$

For et fuldføre beviset, skal det vises, at $\overline{\varphi}$ også er injektiv. Det er nok at vise, at kernen for $\overline{\varphi}$ kun består af det neutrale element i G/N. Antag hertil, for en sideklasse S, at $\overline{\varphi}(S) = e'$. Er $S = xN$, er altså $\varphi(x) = e'$. Men så er $x \in \varphi^{-1}(e')$, altså $x \in N$, og derfor er $S = xN = N$ det neutrale element i G/N.

Hermed er Isomorfisætningen bevist. □

(5.9) Eksempler. (1) Lad g være et element i gruppen G. Som nævnt i Eksempel (5.5)(3) er $i \mapsto g^i$ en homomorfi $\mathbb{Z} \to G$. Billedet er den cykliske undergruppe $\langle g \rangle$. Hvis g har uendelig orden, er homomorfien injektiv, altså en isomorfi $\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$. Antag, at g har endelig orden n. Homomorfiens kerne er da undergruppen $n\mathbb{Z}$ af $\mathbb{Z}$. Af Isomorfisætningen følger derfor, at $i \mapsto g^i$ inducerer en isomorfi,

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \langle g \rangle.$$

(2) Fortegnet for permutationer er en homomorfi sign: $\mathrm{S}_n \to \{\pm 1\} = \mathrm{C}_2$. Dens kerne er undergruppen A_n. For $n \geqslant 2$ er homomorfien surjektiv, og den inducerer en isomorfi,

$$\mathrm{S}_n \,/\, \mathrm{A}_n \xrightarrow{\sim} \mathrm{C}_2\,.$$

(3) Den komplekse eksponentialfunktion er en surjektiv homomorfi exp: $\mathbb{C} \to \mathbb{C}^*$, med kernen $2\pi i\mathbb{Z}$. Homomorfien inducerer derfor en isomorfi,

$$\mathbb{C}/2\pi i\mathbb{Z} \xrightarrow{\sim} \mathbb{C}^*.$$

Tilsvarende inducerer $t \mapsto e^{it}$ en isomorfi,

$$\mathbb{R}/2\pi\mathbb{Z} \xrightarrow{\sim} \mathbb{U}.$$

(4) Determinant af kvadratiske matricer er en homomorfi $\mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$, og dens kerne er undergruppen $\mathrm{SL}_n(\mathbb{R})$ bestående af matricer med determinant 1. Det er let at indse, at homomorfien er surjektiv. Den inducerer derfor en isomorfi,

$$\mathrm{GL}_n(\mathbb{R})/\,\mathrm{SL}_n(\mathbb{R}) \xrightarrow{\sim} \mathbb{R}^*.$$

(5.10) Definition. Gruppen G siges at være *isomorf* med gruppen G', hvis der findes en isomorfi $\varphi\colon G \xrightarrow{\sim} G'$. Isomorfien φ er specielt en bijektiv afbildning $G \to G'$, og det er let at se, at den inverse afbildning $\varphi^{-1}\colon G' \to G$ igen er en isomorfi. Vi kan derfor blot tale om, at to grupper er isomorfe.

Isomorfe grupper kan i mange henseender betragtes som ens. En isomorfi $\varphi\colon G \xrightarrow{\sim} G'$ etablerer specielt en bijektiv forbindelse mellem elementerne i G og G': til hvert element $g \in G$ svarer et og kun ét element $g' \in G'$. Da φ også er en homomorfi, svarer produkt g_1g_2 af to elementer g_1, g_2 i G under denne bijektive forbindelse til produktet $g'_1g'_2$ af de to tilsvarende elementer g'_1, g'_2 i G'. Det følger, at grupperne G og G' samtidig har alle egenskaber, der kan udtrykkes for abstrakte grupper, altså at G har egenskaben, hvis og kun hvis G' har egenskaben. Fx har G og G' samme orden, G er kommutativ hvis og kun hvis G' er kommutativ, G er cyklisk hvis og kun hvis G' er cyklisk, osv, osv.

(5.11) Eksempel. Af Eksempel (5.9)(1) fremgår, at en cyklisk gruppe G er isomorf med restklassegruppen $\mathbb{Z}/n\mathbb{Z}$, hvis G er af endelig orden n, og isomorf med $\mathbb{Z}$, hvis $|G| = \infty$. Alle cykliske grupper af samme orden er altså isomorfe.

Specielt er alle cykliske grupper af orden n altså isomorfe med den additive gruppe $\mathbb{Z}/n\mathbb{Z}$. Gruppen $\mathbb{Z}/n\mathbb{Z}$ er derfor den eneste (på nær isomorfi) cykliske gruppe af orden n. Med samme sprogbrug kan vi hævde, at den multiplikative gruppe C_n er den eneste cykliske gruppe af orden n.

Af Korollar (4.8) følger, at for et primtal p er der kun én gruppe af orden p, nemlig den cykliske gruppe C_p.

Som nævnt i (3.20) kan et produkt af to cykliske grupper selv være en cyklisk gruppe. Fx følger det, at $C_2 \times C_3$ er en cyklisk gruppe af orden 6. På nær isomorfi har vi altså ligheden,

$$C_2 \times C_3 = C_6 .$$

Det følger ligeledes, at produktet $C_2 \times C_2$ ikke er en cyklisk gruppe. Grupperne C_4 og $C_2 \times C_2$, der begge har orden 4, er altså ikke isomorfe. Det er ikke svært at vise, at (på nær isomorfi) er C_4 og $C_2 \times C_2$ de eneste grupper af orden 4.

(5.12) Eksempel. Det fremgår af Eksempel (4.12), at der (på nær isomorfi) er præcis to grupper af orden 6, nemlig den cykliske gruppe C_6 og den symmetriske gruppe S_3. Da $C_2 \times C_3$ er kommutativ, følger det også heraf, at $C_2 \times C_3$ må være isomorf med C_6. Da diedergruppen D_3 er ikke-kommutativ, følger det, at D_3 må være isomorf med S_3.

(5.13) Noether's første Isomorfisætning. *Lad H og N være undergrupper af G, hvor N antages at være normal. Da er delmængden $HN := \{hn \mid h \in H \text{ og } n \in N\}$ en undergruppe af G. Yderligere er N en normal undergruppe af HN og $H \cap N$ er en normal undergruppe af H, og der findes en naturlig isomorfi,*

$$H/(H \cap N) \xrightarrow{\sim} HN/N. \tag{5.13.1}$$

Bevis. Vi viser først, at delmængden HN er stabil. Betragt altså to elementer h_1n_1 og h_2n_2 i HN, hvor altså $h_1, h_2 \in H$ og $n_1, n_2 \in N$. For produktet har vi så, at

$$(h_1n_1)(h_2n_2) = h_1n_1h_2n_2 = h_1h_2(h_2{}^{-1}n_1h_2)n_2.$$

Højresiden er et produkt af fire faktorer. Produktet h_1h_2 af de to første faktorer tilhører øjensynlig H. Da N er normal, ligger den tredie faktor, $h_2{}^{-1}n_1h_2$, i N, og produktet af de to sidste faktorer ligger derfor i N. Heraf følger, at højresiden ligger i HN. Altså er HN en stabil delmængde af G. Da $e = ee$, ligger det neutrale element i HN. Endelig har vi, for $h \in H$ og $n \in N$, at

$$(hn)^{-1} = n^{-1}h^{-1} = h^{-1}(hn^{-1}h^{-1}).$$

På højresiden er $hn^{-1}h^{-1} \in N$, da N er normal. Det følger derfor, at $(hn)^{-1} \in HN$. Altså er HN en undergruppe.

For $h \in H$ er $h = he \in HN$, så $H \subseteq HN$. Tilsvarende er $N \subseteq HN$. Derfor er H og N undergrupper af HN. Da ligningen $gNg^{-1} = N$ gælder for alle elementer $g \in G$, gælder den specielt for elementer $g \in HN$. Følgelig er N endda en normal undergruppe af HN. Den kanoniske homomorfi $\kappa \colon HN \to HN/N$ definerer ved restriktion en homomorfi $\kappa_0 \colon H \to HN/N$, hvorved $h \in H$ afbildes på sideklassen hN i HN/N. Homomorfien κ_0 er surjektiv, thi enhver sideklasse i HN/N har formen $hnN = hN$, og hN er billedet af $h \in H$. Det neutrale element i HN/N er sideklassen N, så kernen for κ_0 består af de elementer $h \in H$, for hvilke $hN = N$, altså af de elementer $h \in H$, for hvilke $h \in N$. Kernen for κ_0 er altså fællesmængden $H \cap N$. Specielt er $H \cap N$ derfor en normal undergruppe af H, og isomorfien (5.13.1) fås ved at anvende Isomorfisætningen på κ_0. □

(5.14) Observation. Af isomorfien i (5.13.1) følger specielt, at de to grupper har samme antal elementer. Noether's første Isomorfisætning medfører altså ligningen,

$$|H : H \cap N| = |HN : N|. \tag{5.14.1}$$

Ifølge Indexsætningen er $|HN| = |HN : N|\cdot|N|$. Ligningen (5.14.1) er derfor ækvivalent med ligningen $|HN| = |H : H\cap N| \cdot |N|$, som vi beviste i (4.11) uden at forudsætte, at N er normal.

(5.15) Noether's anden Isomorfisætning. *Lad der være givet en homomorfi $\varphi\colon G \to G'$, og lad K være kernen for φ. Da gælder:*

Ved $H \mapsto \varphi(H)$ defineres en bijektiv afbildning fra mængden af de undergrupper H af G, der omfatter K, på mængden af alle undergrupper af $\varphi(G)$. Den inverse afbildning er bestemt ved $L \mapsto \varphi^{-1}(L)$, for undergrupper L af $\varphi(G)$.

Under denne bijektive afbildning gælder for en undergruppe N af G, med $N \supseteq K$, at N er normal i G, hvis og kun hvis $\varphi(N)$ er normal i $\varphi(G)$. Yderligere gælder, når N er normal i G og $N \supseteq K$, at der findes en naturlig isomorfi,

$$G/N \xrightarrow{\sim} \varphi(G)/\varphi(N). \tag{5.15.1}$$

Bevis. Lad $\mathcal{U}$ betegne mængden af de undergrupper H af G, for hvilke $H \supseteq K$, og lad $\mathcal{U}'$ betegne mængden af alle undergrupper af $\varphi(G)$.

Det følger af (5.3), at for hver undergruppe H af G er billedmængden $\varphi(H)$ en undergruppe i G'. Specielt er $\varphi(G)$ en undergruppe af G', g $\varphi(H)$ er en undergruppe af $\varphi(G)$. Tilsvarende følger det, at for hver undergruppe L af G' er originalmængden $\varphi^{-1}(L)$ en undergruppe af G, og originalmængden vil specielt omfatte $K = \varphi^{-1}(e')$.

Ved $H \mapsto \varphi(H)$ defineres følgelig en afbildning $\Phi\colon \mathcal{U} \to \mathcal{U}'$, og ved $L \mapsto \varphi^{-1}(L)$ defineres følgelig en afbildning $\Psi\colon \mathcal{U}' \to \mathcal{U}$. Det er påstanden, at afbildningen Φ er bijektiv og at afbildningen Ψ er den inverse. Hertil skal det vises, at $\Psi \circ \Phi$ er den identiske afbildning af $\mathcal{U}$ og at $\Phi \circ \Psi$ er den identiske afbildning af $\mathcal{U}'$.

Betragt først ligningen $\Phi \circ \Psi(L) = L$, hvor $L \in \mathcal{U}'$, dvs L er en undergruppe af $\varphi(G)$. Ligningen udsiger, at

$$\varphi(\varphi^{-1}L) = L. \tag{5.15.2}$$

Det er let at vise denne ligning; den gælder for afbildninger i almindelighed, og udnytter blot, at L er en delmængde af billedmængden $\varphi(G)$.

Betragt dernæst ligningen $\Psi \circ \Phi(H) = H$, hvor $H \in \mathcal{U}$, dvs H er en undergruppe af G og $H \supseteq K$. Ligningen udsiger, at

$$\varphi^{-1}(\varphi H) = H. \tag{5.15.3}$$

Det er en simpel egenskab ved afbildninger, der sikrer, at højresiden er indeholdt i venstresiden. For at vise ligheden skal vi vise den omvendte inklusion, og hertil er antagelserne nødvendige. Lad altså g være et element i venstresiden, altså $g \in \varphi^{-1}(\varphi H)$. Da er $\varphi(g) \in \varphi(H)$. Følgelig findes et element $h \in H$ således, at $\varphi(g) = \varphi(h)$. Da φ er en homomorfi, slutter vi, at $\varphi(gh^{-1}) = \varphi(g)\varphi(h)^{-1} = e'$. Altså er gh^{-1} element i kernen for φ, dvs $gh^{-1} \in K$. Da $K \subseteq H$, følger det, at $gh^{-1} \in H$. Altså er $g = (gh^{-1})h$ produkt af to elementer i H, og da H er en undergruppe, følger det at $g \in H$.

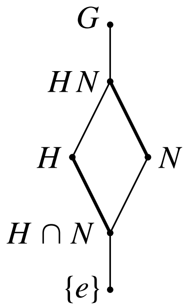
Hermed er vist, at afbildningen $\Phi\colon \mathcal{U} \to \mathcal{U}'$ er bijektiv og at afbildningen Ψ er den inverse.

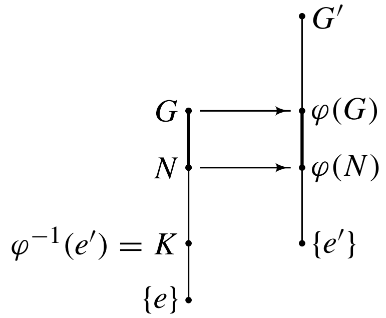
Antag, at N er en normal undergruppe af G, altså at $ghg^{-1} \in N$ for alle $g \in G$ og $h \in N$. Da er $\varphi(g)\varphi(h)\varphi(g)^{-1} \in \varphi(N)$ for alle $g \in G$ og $h \in N$. Heraf ses, at $\varphi(N)$ er en normal undergruppe af $\varphi(G)$.

Lad nu $N \in \mathcal{U}$ være en vilkårlig undergruppe med $N \supseteq K$. Vi har lige vist, at hvis N er normal i G, så er $\varphi(N)$ normal i $\varphi(G)$. Vi mangler at vise, at hvis $\varphi(N)$ er normal i $\varphi(G)$, så er N normal i G; desuden skal vi bestemme isomorfien (5.15.1).

Antag altså, at $\varphi(N)$ er normal i $\varphi(G)$. Lad $\kappa : \varphi(G) \to \varphi(G)/\varphi(N)$ være den kanoniske surjektive homomorfi. Opfattes φ som en surjektiv homomorfi $\varphi\colon G \to \varphi(G)$, får vi ved sammensætning en surjektiv homomorfi $\kappa\varphi\colon G \to \varphi(G)/\varphi(N)$, hvorved $g \in G$ afbildes på sideklassen $\varphi(g)\varphi(N)$. Betragt kernen for $\kappa\varphi$. Det neutrale element i $\varphi(G)/\varphi(N)$ er sideklassen $\varphi(N)$. Elementet g tilhører altså kernen, netop når $\varphi(g)\varphi(N) = \varphi(N)$, dvs netop når $\varphi(g) \in \varphi(N)$. Kernen består altså af de elementer g, for hvilke $\varphi(g) \in \varphi(N)$, dvs kernen er $\varphi^{-1}(\varphi N)$. Da vi har antaget, at $N \in \mathcal{U}$, følger det af (5.15.3), at $\varphi^{-1}(\varphi N) = N$. Den surjektive homomorfi $\kappa\varphi\colon G \to \varphi(G)/\varphi(N)$ har altså kernen N. Heraf følger først, at N er normal i G, og dernæst følger isomorfien (5.15.1) af Isomorfisætningen. $\square$

(5.16) Note. En situation, hvor man på én gang har givet flere grupper og homomorfier mellem dem, kan ofte anskueliggøres med et *diagram.* Man „afsætter“ grupperne som punkter i planen, og man tegner pile mellem punkterne svarende til homomorfierne. Hvis homomorfierne blot er inklusioner, svarende til at nogle af grupperne er undergrupper af andre, tegner man blot streger, og man sørger for at de største grupper anbringes øverst på tegningerne. Noether's isomorfisætninger kan anskueliggøres af følgende diagrammer:





(5.17) Observation. Noether's anden Isomorfisætning anvendes oftest på den kanoniske (surjektive) homomorfi $G \to G/K$, hvor K er en given normal undergruppe af G. For en undergruppe H af G, med $H \supseteq K$, består billedet af sideklasserne hK, for $h \in H$. Billedet kan altså identificeres med kvotientgruppen H/K. Det er altså påstanden i Sætningen, at samtlige undergrupper i G/K har formen H/K, med en entydigt bestemt undergruppe $H \supseteq K$. Yderligere gælder, at de normale undergrupper af G/K er undergrupperne N/K, hvor $N \supseteq K$ er normal i G. Isomorfien (5.15.1) er her en isomorfi,

$$G/N \xrightarrow{\sim} \frac{G/K}{N/K}\,.$$

(5.18) Opgaver.

1. Lad g være et element i gruppen G. Vis, at afbildningen $i \mapsto g^i$ er en homomorfi $\mathbb{Z} \to G$, og at det er den eneste homomorfi $\mathbb{Z} \to G$ således, at $1 \mapsto g$. Bestem antallet af homomorfier $\mathbb{Z} \to G$.

2. Vis, for en gruppe G, at antallet af homomorfier $\mathrm{C}_n \to G$ er det samme som antallet af løsninger $g \in G$ til ligningen $g^n = e$. Bestem antallet af homomorfier $\mathrm{C}_6 \to \mathrm{S}_6$.

3. Vis, at $a \mapsto [a]_n$ er en homomorfi af additive grupper $\mathbb{Z} \to \mathbb{Z}/n$, og angiv kernen.

4. Antag $d\,|\,n$. Vis, at $[a]_n \mapsto [a]_d$ er en veldefineret afbildning $\mathbb{Z}/n \to \mathbb{Z}/d$. Vis, at afbildningen er en homomorfi af additive grupper, og bestem dens kerne.

5. Antag, at $d\,|\,n$. Vis, at afbildningen $[a]_n \mapsto [a]_d$ definerer en homomorfi af multiplikative grupper $(\mathbb{Z}/n)^* \to (\mathbb{Z}/d)^*$. Vis, når $d = p$ er et primtal og $n = p^\nu$, at homomorfien er surjektiv, og bestem ordenen af kernen.

6. *Vis, for enhver divisor d i n, at homomorfien $(\mathbb{Z}/n)^* \to (\mathbb{Z}/d)^*$ er surjektiv.

7. Vis, at hvis $\varphi\colon G \to G'$ og $\varphi'\colon G' \to G''$ er gruppehomomorfier, så er også den sammensatte afbildning $\varphi' \circ \varphi\colon G \to G''$ en homomorfi.

8. Vis, at hvis $\varphi\colon G \to G'$ er en gruppeisomorfi, så er den inverse afbildning $\varphi^{-1}\colon G' \to G$ en isomorfi.

9. Lad $\varphi\colon G \to G'$ være en gruppehomomorfi. Vis, for $g \in G$, at ordenen af $\varphi(g)$ er divisor i ordenen af g. Vis, at $\varphi(\langle g \rangle) = \langle \varphi(g) \rangle$.

10. Betragt afbildningen,

$$\begin{bmatrix} \mu & a \\ 0 & \nu \end{bmatrix} \mapsto (\mu, \nu),$$

for $\mu\nu \neq 0$. Matricerne på venstresiden udgør en undergruppe T af $\mathrm{GL}_2(\mathbb{R})$, og parrene på højresiden udgør gruppen $\mathbb{R}^* \times \mathbb{R}^*$. Vis, at afbildningen er en homomorfi, og bestem kernen.

11. Vis, at homomorfierne $\mathbb{Z} \to \mathbb{Z}$ netop er afbildningerne $x \mapsto qx$ for $q \in \mathbb{Z}$. Vis, at homomorfierne $\mathbb{Q} \to \mathbb{Q}$ netop er afbildningerne $x \mapsto qx$ for $q \in \mathbb{Q}$.

12. Vis, at de kontinuerte homomorfier $\mathbb{R} \to \mathbb{R}$ netop er afbildningerne $x \mapsto qx$ for $q \in \mathbb{R}$.

13. Vis, at gruppen $\mathbb{R}\setminus\{1\}$ med „produktet“ $a * b := a + b - ab$ er isomorf med $\mathbb{R}^*$.

14. Vis, at de additive grupper $\mathbb{Z}$ og $\mathbb{Q}$ ikke er isomorfe.

15. Vis, for en gruppe G, at afbildningen $g \mapsto g^{-1}$ er en homomorfi, hvis og kun hvis G er kommutativ.

16. Find de steder i noterne, hvor Klein's Vierer-gruppe er defineret. Er det samme gruppe, der defineres?

17. Vis, at i S_4 udgør identiteten og de 3 dobbelttranspositioner en undergruppe V, der er isomorf med Klein's Vierer-gruppe. Vis, at V er en normal undergruppe af S_4.

18. Lad N være en normal undergruppe af G, og lad K være en normal undergruppe af N. Vis, ved et eksempel, at K ikke nødvendigvis er normal i G. [Vink: Klein's Vierer-gruppe kan bruges som N i et eksempel.]

19. *Lad N være en normal undergruppe af G. Vis, at hvis N er cyklisk, så er enhver undergruppe af N normal i G.

20. Vis, at en lineær afbildning $f\colon V \to W$ mellem vektorrum er en gruppehomomorfi, når vektorrummene opfattes som additive grupper.

21. Lad $\varphi\colon G \to G'$ være en gruppehomomorfi. Vis, at $|G| = |\varphi(G)| \cdot |\varphi^{-1}(e')|$.

22. Vis, at når n er ulige, så findes en isomorfi $\mathrm{C}_2 \times \mathrm{D}_n \xrightarrow{\sim} \mathrm{D}_{2n}$.

23. Vis, at følgende grupper er ikke-isomorfe [strengt taget: „er parvis ikke-isomorfe“]: $C_2 \times C_6$, C_{12}, A_4, D_6. [Vink: sammenlign fx antallene af elementer af orden 2.]

24. Vis, at grupperne S_5 og $D_6 \times D_5$ ikke er isomorfe.

25. Bestem, som funktion af n, en øvre grænse for antallet af grupper af orden n.

26. Mængden af ortogonale matricer med determinant 1 betegnes $O^+(n)$. Vis, at $O^+(n)$ er en normal undergruppe af index 2 i den ortogonale gruppe $O(n)$, og at $O(n)/\,O^+(n)$ er isomorf med C_2. Gruppen $O^+(n)$ kaldes den *specielle ortogonale gruppe*, og betegnes også $SO(n)$ eller $SO_n(\mathbb{R})$.

27. Vis, at mængden af alle matricer af formen $\begin{bmatrix} \pm 1 & a \\ 0 & 1 \end{bmatrix}$ for $a \in \mathbb{Z}$, udgør en undergruppe G af $GL_2(\mathbb{Z})$. Vis, at delmængden N bestående af alle matricer af formen $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ for $a \in n\mathbb{Z}$ er en normal undergruppe af G. Vis, at G/N er isomorf med diedergruppen D_n.

28. Vis for et givet element g i en gruppe G, at afbildningen $x \mapsto gxg^{-1}$ er en *gruppeautomorfi* af G, dvs en isomorfi af G på sig selv.

29. Lad G være en gruppe, og lad $\mathrm{Aut}(G)$ være mængden af automorfier af G. Automorfierne er specielt permutationer af G, så $\mathrm{Aut}(G)$ er en delmængde af $\mathrm{Perm}(G)$. Vis, at $\mathrm{Aut}(G)$ er en undergruppe af $\mathrm{Perm}(G)$. For hvert element $g \in G$ er afbildningen $\rho_g(x) = gxg^{-1}$ en automorfi af G. Vis, at $g \mapsto \rho_g$ er en homomorfi $G \to \mathrm{Aut}(G)$. Beskriv kernen. Vis, at billedgruppen er en normal undergruppe af $\mathrm{Aut}(G)$.

30. *Antag for grupper H, N, at der er givet en gruppehomomorfi $h \mapsto \rho_h$ fra gruppen H til gruppen $\mathrm{Aut}(N)$. Vis, at produktmængden $G := N \times H$ med kompositionen,

$$(n_1, h_1)(n_2, h_2) := (n_1\rho_{h_1}(n_2)\,,\; h_1h_2), \tag{*}$$

er en gruppe. Vis (med en oplagt notation), at delmængden $N \times 1$ af G er en undergruppe isomorf med N og at $1 \times H$ er en undergruppe isomorf med H. Vis, idet vi opfatter N og H som undergrupper af G, at N er en normal undergruppe af G og at den sammensatte homomorfi $H \to G \to G/N$ er en isomorfi. Vis, for $n \in N$ og $h \in H$, at $\rho_h(n) = hnh^{-1}$. Med kompositionen (*) kaldes gruppen $N \times H$ det *semidirekte produkt* af N og H og betegnes $N \times_\rho H$.

Eksempler: For en kommutativ gruppe A er $x \mapsto x^{-1}$ en automorfi af orden 2. Herved defineres en homomorfi $\rho_1\colon C_2 \to \mathrm{Aut}(A)$. Vis, at $C_k \times_{\rho_1} C_2 = D_k$.

Klein's Vierer-gruppe V har orden 4. Bestem en homomorfi $\rho_2\colon C_3 \to \mathrm{Aut}(V)$, som ikke er triviel, og vis, at det semi-direkte produkt $V \times_{\rho_2} C_3$ er den alternerende gruppe A_4.

Automorfigruppen for C_3 er den cykliske gruppe C_2. Slut heraf, at der findes en ikke-triviel homomorfi $\rho_3\colon V \to \mathrm{Aut}(C_3)$, og en ikke-triviel homomorfi $\rho_4\colon C_4 \to \mathrm{Aut}(C_3)$. Vis, at $C_3 \times_{\rho_3} V = D_6$. Vis, at de tre grupper D_6, A_4 og $C_3 \times_{\rho_4} C_4$ er ikke-isomorfe.

31. Vis for undergrupper H, N af G, hvor N er normal, at $HN = NH$.

32. Vis, når H er en undergruppe af G og $g \in G$, at gHg^{-1} igen er en undergruppe. Vis, at H og gHg^{-1} er isomorfe. Vis, at hvis H er den eneste undergruppe af en given orden, så er H normal.

6. Struktursætning for endelige kommutative grupper.

(6.1) Indledning. Definitionen i (3.19) af produkt af to grupper udstrækkes uden videre til produkt af r grupper $G_1, \dots, G_r$. Produktmængden $G_1 \times \cdots \times G_r$, bestående af alle r-sæt $(g_1, \dots, g_r)$ hvor $g_i \in G_i$, organiseres som en gruppe med *koordinatvis komposition*,

$$(g_1, \dots, g_r)(h_1, \dots, h_r) := (g_1h_1, \dots, g_rh_r).$$

Det neutrale element er r-sættet $e := (e_1, \dots, e_r)$, hvor e_i betegner det neutrale element i G_i, og det inverse til et r-sæt $(g_1, \dots, g_r)$ er r-sættet $(g_1^{-1}, \dots, g_r^{-1})$.

Gruppen $G_1 \times \cdots \times G_r$ kaldes *produktet*, eller det *direkte produkt* af grupperne $G_1, \dots, G_r$. Hvis grupperne G_i er kommutative, additivt skrevne grupper, kaldes produktet også den *direkte sum*, og det kan betegnes $G_1 \oplus \cdots \oplus G_r$.

For ordenen af produktet har vi øjensynlig ligningen,

$$|G_1 \times \cdots \times G_r| = |G_1| \cdots |G_r|.$$

Hver af de givne grupper G_i er relateret til produktet via to homomorfier: *projektionen*,

$$(g_1, \dots, g_r) \mapsto g_i, \tag{6.1.1}$$

er en surjektiv homomorfi $G_1 \times \cdots \times G_r \to G_i$, og *injektionen*,

$$g_i \mapsto (e_1, \dots, g_i, \dots, e_r), \quad g_i \in G_i, \tag{6.1.2}$$

hvor højresiden har g_i på den i'te plads, er en injektiv homomorfi $G_i \to G_1 \times \cdots \times G_r$. Via den i'te injektion kan vi opfatte G_i som undergruppe af produktet.

Lad G være en given gruppe. Er der givet undergrupper $H_1, \dots, H_r$ af G, defineres ved $(h_1, \dots, h_r) \mapsto h_1 \cdots h_r$ en afbildning,

$$H_1 \times \cdots \times H_r \to G. \tag{6.1.3}$$

Denne afbildning er i almindelighed ikke surjektiv, ikke injektiv, og ikke en homomorfi. Hvis afbildningen er en gruppeisomorfi, siger vi, at G *er* det direkte produkt af undergrupperne H_i. Vi udtrykker det ofte ved at skrive $H_1 \times \cdots \times H_r = G$. Det skal understreges, at lighedstegnet ikke bruges i betydningen, at de to sider er ens; det betyder her, at det er den angivne afbildning (6.1.3), der er en isomorfi.

Hvis en gruppe G er isomorf med et produkt af grupper $G_1 \times \cdots \times G_r$, så svarer gruppen G_i via den i'te injektion til en undergruppe af produktet, og dermed, via isomorfien, til en undergruppe H_i af G. Det er let at se, at G så *er* det direkte produkt af disse undergrupper H_i.

Det er hovedresultatet i dette kapitel, at enhver endelig kommutativ gruppe G er isomorf med et produkt af cykliske grupper. Det betyder, ækvivalent, at der i G findes elementer $g_1, \dots, g_r$ således, at G er det direkte produkt af de cykliske undergrupper $\langle g_i \rangle$.

(6.2) Observation. Betragt for givne undergrupper $H_1, \dots, H_r$ af G afbildningen (6.1.3). Afbildningen er en homomorfi, hvis og kun hvis der for alle $i < j$ og $h_i \in H_i$ og $h_j \in H_j$ gælder, at

$$h_i h_j = h_j h_i. \tag{6.2.1}$$

Antag nemlig først, at afbildningen er en homomorfi. Lad $\hat{h}_i = (e_1, \dots, h_i, \dots, e_r)$ være billedet af $h_i \in H_i$ ved den i'te injektion. I produktgruppen $H_1 \times \cdots \times H_r$ gælder ligningen, for $i < j$,

$$\hat{h}_i \hat{h}_j = \hat{h}_j \hat{h}_i, \tag{*}$$

idet begge sider er lig med r-sættet $(e_1, \dots, h_i, \dots, h_j, \dots, e_r)$. Ved afbildningen afbildes $\hat{h}_i$ på h_i og $\hat{h}_j$ på h_j. Da afbildningen er en homomorfi, følger ligningen (6.2.1) af (*).

Antag omvendt, at (6.2.1) er opfyldt. Produktet af to r-sæt $(h'_1, \dots, h'_r)$ og $(h''_1, \dots, h''_r)$ er r-sættet $(h'_1 h''_1, \dots, h'_r h''_r)$, som afbildes i elementet,

$$h'_1 h''_1 \cdots h'_r h''_r = h'_1 \cdots h'_r h''_1 \cdots h''_r,$$

hvor lighedstegnet følger af (6.2.1). Billedet af produktet er derfor produktet af billederne. Altså er afbildningen en homomorfi.

Bemærk specielt, at betingelsen (6.2.1) er en nødvendig betingelse for, at G kan være det direkte produkt af undergrupperne H_i.

Hvis G er kommutativ, er betingelsen naturligvis opfyldt. For en kommutativ gruppe er afbildningen (6.1.3) altså altid en homomorfi.

(6.3) Eksempel. Antag, at $n = n_1 \cdots n_r$ er et produkt af parvis primiske naturlige tal n_i. Som bekendt udsiger Den kinesiske Restklassesætning, at afbildningen $[x]_n \mapsto ([x]_{n_1}, \dots, [x]_{n_r})$, der til restklassen af x modulo n knytter r-sættet af restklasser af x modulo n_i for $i = 1, \dots, r$, er en bijektiv afbildning,

$$\mathbb{Z}/n \xrightarrow{\sim} \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r. \tag{6.3.1}$$

Afbildningen er en homomorfi, idet højresiden opfattes som det direkte produkt af grupperne $\mathbb{Z}/n_i$. Summen af restklasser $[x]_n$ og $[y]_n$ er nemlig restklassen $[x+y]_n$, og denne restklasse afbildes på

$$\begin{aligned}([x+y]_{n_1}, \dots, [x+y]_{n_r}) &= ([x]_{n_1}+[y]_{n_1}, \dots, [x]_{n_r}+[y]_{n_r}) \\ &= ([x]_{n_1}, \dots, [x]_{n_r}) + ([y]_{n_1}, \dots, [y]_{n_r}),\end{aligned}$$

altså på summen af billederne. Afbildningen (6.3.1) er altså en gruppeisomorfi. Den additive gruppe $\mathbb{Z}/n$ på venstresiden er isomorf med det direkte produkt på højresiden.

Som bekendt er x primisk med n, hvis og kun hvis x er primisk med hver faktor n_i. Heraf ses, at afbildningen (6.3.1) definerer en bijektiv afbildning mellem delmængder,

$$(\mathbb{Z}/n)^* \xrightarrow{\sim} (\mathbb{Z}/n_1)^* \times \cdots \times (\mathbb{Z}/n_r)^*. \tag{6.3.2}$$

Delmængden $(\mathbb{Z}/n)^*$ er gruppen af primiske restklasser med multiplikation. Ved en tilsvarende udregning, hvor sum erstattes med produkt, ses, at afbildningen (6.3.2) er en homomorfi mellem (multiplikative) grupper, og dermed en isomorfi. Gruppen $(\mathbb{Z}/n)^*$ er altså isomorf med det direkte produkt af grupperne $(\mathbb{Z}/n_i)^*$.

(6.4) Lemma. *Lad G være en gruppe, og lad H og K være undergrupper af G. Da er følgende to betingelser ækvivalente:*

(i) *Gruppen G er det direkte produkt af undergrupperne H og K, dvs afbildningen $H \times K \to G$ bestemt ved $(h, k) \mapsto hk$ er en isomorfi.*

(ii) *Undergrupperne H og K er normale, og der gælder ligningerne $H \cap K = \{e\}$ og $HK = G$.*

Bevis. Billedmængden ved afbildningen $H \times K \to G$ er øjensynlig delmængden HK af G. Afbildningen er altså surjektiv, hvis og kun hvis $HK = G$.

Antag først (i), altså at afbildningen er en isomorfi. Specielt er afbildningen da surjektiv, så $HK = G$. Ved injektionen $h \mapsto (h, e)$ afbildes H på undergruppen $H \times \{e\}$ af $H \times K$. Øjensynlig er $H \times \{e\}$ netop kernen for projektionen $H \times K \to K$. Specielt er $H \times \{e\}$ en normal undergruppe af $H \times K$. Tilsvarende er $\{e\} \times K$ en normal undergruppe af $H \times K$. Øjensynlig er fællesmængden af $H \times \{e\}$ og $\{e\} \times K$ den trivielle undergruppe i $H \times K$. Ved isomorfien afbildes $H \times \{e\}$ på H og $\{e\} \times K$ på K. Altså er H og K normale undergrupper af G, og $H \cap K$ er den trivielle undergruppe $\{e\}$. Hermed er betingelsen (ii) eftervist.

Antag omvendt betingelsen (ii). Da $HK = G$, er afbildningen surjektiv. For at vise, at afbildningen er en homomorfi, skal vi vise, at $hk = kh$ for alle $h \in H$ og $k \in K$. Øjensynlig har vi ligningerne,

$$h(kh^{-1}k^{-1}) = (hk)(kh)^{-1} = (hkh^{-1})k^{-1}.$$

På venstresiden er $kh^{-1}k^{-1} \in H$, fordi H er normal. Heraf følger, at venstresiden ligger i H. Tilsvarende ligger højresiden i K. Altså ligger $(hk)(kh)^{-1}$ i $H \cap K = \{e\}$. Derfor er $hk = kh$. Hermed er vist, at afbildningen er en homomorfi. For at vise, at afbildningen er injektiv, undersøger vi kernen. Lad (h, k) være et par i kernen. Da er $hk = e$. Vi har $h \in H$ og $h = k^{-1} \in K$, og slutter, at $h \in H \cap K = \{e\}$. Altså er $h = e$. Af $hk = e$ følger, at også $k = e$. Kernen består altså alene af parret (e, e). Da afbildningen var en homomorfi, følger det, at den er injektiv. Hermed er betingelsen (i) eftervist. □

(6.5) Sætning. *Antag, at $n = n_1 \cdots n_r$ er et produkt af parvis primiske tal n_i. Lad G være en kommutativ gruppe af orden n. Da er hver delmængde,*

$$H_i := \{g \in G \mid g^{n_i} = e\},$$

en undergruppe af G, og G er det direkte produkt af undergrupperne H_i,

$$H_1 \times \cdots \times H_r \xrightarrow{\sim} G. \tag{6.5.1}$$

Bevis. Det følger af Den kinesiske Restklassesætning, at der for hvert $i = 1, \ldots, r$ findes et helt tal d_i, som opfylder kongruenserne,

$$(1)\ d_i \equiv 1 \pmod{n_i}, \qquad (2)\ d_i \equiv 0 \pmod{n_j} \text{ for } j \neq i.$$

Kongruenserne medfører følgende kongruenser:

$$(3)\ d_1 + \cdots + d_r \equiv 1 \pmod{n}, \qquad (4)\ d_i n_i \equiv 0 \pmod{n}.$$

Kongruenserne i (1) og (2) medfører nemlig, at summen $d_1 + \cdots + d_r$ er kongruent med 1 modulo n_i for alle i, og så følger kongruensen (3) af Den kinesiske Restklassesætning. Videre er $d_i n_i \equiv 0 \pmod{n_j}$ for alle j, thi for $j = i$ er det trivielt og for $j \neq i$ følger det af (2). Altså gælder kongruensen (4).

Antag nu, at gruppen G er kommutativ af orden n. Lad k være et helt tal. Hvis $g^k = e$ og $h^k = e$, er $(gh)^k = g^k h^k = e$; trivielt er $e^k = e$; og hvis $g^k = e$, så er også $(g^{-1})^k = g^{-k} = e$. Heraf følger specielt, for $k := n_i$, at hver delmængde H_i er en undergruppe af G.

Det skal nu vises, at afbildningen (6.5.1), bestemt ved $(g_1, \dots, g_r) \mapsto g_1 \cdots g_r$ er en bijektiv homomorfi. Afbildningen er en homomorfi, fordi G er kommutativ. At afbildningen er bijektiv betyder, at hvert element $g \in G$ kan fremstilles som et produkt,

$$g = g_1 \cdots g_r, \quad \text{med } g_i \in H_i, \tag{*}$$

med entydigt bestemte faktorer g_i.

For at vise entydigheden antages, at der er givet en fremstilling (*) af elementet g. Vi har $g_j^{n_j} = e$ for alle j. Det følger derfor af (1), at $g_i^{d_i} = g_i$, og af (2), at $g_j^{d_i} = e$ for $j \neq i$. Altså er

$$g^{d_i} = (g_1 \cdots g_r)^{d_i} = g_1^{d_i} \cdots g_r^{d_i} = e \cdots g_i \cdots e = g_i.$$

Heraf følger entydigheden. Mere præcist har vi vist, at den i'te faktor i (*) er bestemt som $g_i = g^{d_i}$. For at vise eksistensen af fremstillingen må vi derfor vise, for et vilkårligt element $g \in G$, at

$$g = g^{d_1} \cdots g^{d_r} \quad \text{og} \quad g^{d_i} \in H_i \text{ for alle } i.$$

Da n er ordenen af G, er $g^n = e$. Ligningen $g = g^{d_1} \cdots g^{d_r}$ følger derfor af (3). Videre følger af (4), at $(g^{d_i})^{n_i} = e$. Altså er $g^{d_i} \in H_i$, som ønsket. □

(6.6) Observation. Standardanvendelsen af Sætning (6.5) er på primopløsningen $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$. For en kommutativ gruppe G af orden n er primtallene p_i netop primdivisorerne i $|G|$. For et sådant primtal p_i består undergruppen H_i af de elementer g, for hvilke $g^{p_i^{\nu_i}} = e$. For et sådant element er ordenen en divisor i $p_i^{\nu_i}$, og derfor er ordenen en potens p_i^{μ} med $\mu \leqslant \nu_i$. Antag omvendt, at $g \in G$ har en orden, der er en potens p_i^{μ}. Ordenen er divisor i gruppens orden n, og derfor er $\mu \leqslant \nu_i$. Følgelig er $g \in H_i$.

Det fremgår, at undergruppen H_i består af de elementer $g \in G$, hvis orden er en potens af p_i. Undergruppen betegnes også $G(p_i)$. Det følger af sætningen, at G er det direkte produkt af sine undergrupper $G(p_i)$.

Man kan vise, i almindelighed, at undergruppen H_i i (6.5) har orden n_i. Specielt har undergruppen $G(p_i)$ orden $p_i^{\nu_i}$.

(6.7) Lemma. *Lad G være en kommutativ gruppe, lad $\varphi\colon G \to \overline{G}$ være en surjektiv gruppehomomorfi, og lad G_0 være en undergruppe af G. Antag, at restriktionen $G_0 \to \overline{G}$ er bijektiv. Da er G det direkte produkt af G_0 og kernen for φ,*

$$G_0 \times \varphi^{-1}(\bar{e}) \xrightarrow{\sim} G.$$

Bevis. Lad $K := \varphi^{-1}(\bar{e})$ være kernen for φ. Ved restriktion definerer φ en homomorfi $G_0 \to \overline{G}$. Kernen for restriktionen er øjensynlig $G_0 \cap \varphi^{-1}(\bar{e})$, altså $G_0 \cap K$, og billedet er $\varphi(G_0)$. Det er altså forudsætningen, at $G_0 \cap K = \{e\}$ og $\varphi(G_0) = \overline{G}$. Vi efterviser betingelsen (6.4)(ii). Da G er kommutativ, er G_0 og K normale, og vi har vist, at $G_0 \cap K = \{e\}$. Vi mangler at vise, at $G = G_0K$. Betragt hertil et element $g \in G$. Ifølge antagelsen er $\varphi(g) \in \varphi(G_0)$. Der findes altså et element $g_0 \in G_0$ således, at $\varphi(g) = \varphi(g_0)$. Det følger, at $k := g_0^{-1}g$ tilhører kernen for φ, altså at $k \in K$. Derfor er $g = g_0k \in G_0K$. Hermed er vist, at $G = G_0K$. ∎

(6.8) Sætning. *Lad G være en endelig abelsk gruppe, og lad m være den maksimale orden for elementerne i G. Da har hvert element i G en orden, som er divisor i m.*

Bevis. Lad g være et element af den maksimale elementorden m. Vi skal vise, hvis d er ordenen af et element h i G, så er d divisor i m. Antag, indirekte, at d ikke er divisor i m. For hvert primtal p kan vi skrive $m = p^{\mu}m_0$ og $d = p^{\delta}d_0$, hvor p ikke går op i m_0 og ikke går op i d_0. Da d ikke er divisor i m, kan vi bestemme primtallet p således, at $\delta > \mu$. Nu har G et element af orden m_0, nemlig g^{m/m_0}, og et element af orden p^{δ}, nemlig $g^{d/p^{\delta}}$. Da de to ordener, m_0 og p^{δ}, er primiske, følger det af Lemma (3.17), at G har et element af orden $p^{\delta}m_0$. Men da $p^{\delta}m_0 > m$, er dette i modstrid med, at m var den maksimale orden. ∎

(6.9) Sætning. *Lad G være en endelig kommutativ gruppe, og lad g_0 være et element af maksimal elementorden m. Da findes en undergruppe K af G således, at G er det direkte produkt af undergrupperne $\langle g_0\rangle$ og K,*

$$\langle g_0\rangle \times K \xrightarrow{\sim} G.$$

Bevis. Det er nok at vise, at hvis $\langle g_0\rangle \subset G$, så findes en gruppe $\overline{G}$ af orden mindre end ordenen af G og en surjektiv homomorfi $\varphi\colon G \to \overline{G}$ således, at restriktionen $\langle g_0\rangle \to \overline{G}$ er injektiv. Antag nemlig, at dette er bevist. Hvis $\langle g_0\rangle = G$, er påstanden i sætningen triviel, idet vi som K kan bruge den trivielle undergruppe $\{e\}$. Hvis $\langle g_0\rangle \subset G$, anvendes den surjektive homomorfi φ. For hvert element g i G har billedet $\bar{g} = \varphi(g)$ en orden, som er divisor i ordenen af g. Da $\langle g_0\rangle$ afbildes injektivt ved φ, har $\bar{g}_0$ samme orden, m, som g_0. Følgelig er $\bar{g}_0$ et element af maksimal elementorden i $\overline{G}$. Hvis $\langle \bar{g}_0\rangle \subset \overline{G}$, gentages processen på $\bar{g}_0$ og $\overline{G}$. Efter endeligt mange skridt opnås, ved sammensætning af homomorfierne, en surjektiv homomorfi $\varphi\colon G \to \overline{G}$ således, at restriktionen $\langle g_0\rangle \to \overline{G}$ er injektiv og $\langle \bar{g}_0\rangle = \overline{G}$. Den sidste ligning betyder, at restriktionen $\langle g_0\rangle \to \overline{G}$ også er surjektiv, og så følger det af Lemma (6.7), at G er produktet af $\langle g_0\rangle$ og kernen for φ.

Vi antager altså, at $\langle g_0\rangle \subset G$, og vi viser, at den søgte homomorfi $\varphi\colon G \to \overline{G}$ kan fås som den kanoniske homomorfi $\kappa\colon G \to G/\langle h_0\rangle$ for et passende valgt element $h_0 \in G$. For at $\overline{G}$ har orden mindre end ordenen af G kræves, at $h_0 \neq e$. For at restriktionen $\langle g_0\rangle \to G/\langle h_0\rangle$ er injektiv kræves, at

$$\langle g_0\rangle \cap \langle h_0\rangle = \{e\}. \tag{1}$$

Betragt hertil først et vilkårligt element h, af orden n, i G og en undergruppe K af G. Fællesmængden $K \cap \langle h \rangle$ er en undergruppe af $\langle h \rangle$, så af Sætning (3.16) følger, at

$$K \cap \langle h \rangle = \langle h^l \rangle, \quad \text{hvor } l \mid n. \tag{2}$$

Yderligere følger af (2), at l er ordenen af sideklassen hK i kvotientgruppen G/K. Sideklassens orden bestemmes nemlig ved at betragte eksponenter i med $(hK)^i = eK$, dvs med $h^i \in K$, og ligningen (2) sikrer, for $i = 1, \dots n$, at $h^i \in K$, hvis og kun hvis $l \mid i$.

For at bestemme det søgte element h_0 vælger vi først et element $h \notin \langle g_0 \rangle$. Lad n være ordenen af h. Ifølge (2), med $K := \langle g_0 \rangle$, har vi

$$\langle g_0 \rangle \cap \langle h \rangle = \langle h^l \rangle, \tag{3}$$

hvor l er divisor i n, og l er ordenen af h modulo $\langle g_0 \rangle$. Da $h^l \in \langle g_0 \rangle$, er $h^l = g_0^i$. Da h^l har orden n/l, er $(g_0^i)^{n/l} = e$. Følgelig er m divisor i $i(n/l)$, altså $mt = i(n/l)$ med et helt tal t. Altså er $i = (m/n)tl$, og her er m/n et helt tal ifølge Sætning (6.8). Sæt

$$g_1 := g_0^{(m/n)t}, \qquad h_0 := hg_1^{-1}.$$

Det følger, at $g_1^l = g_0^i = h^l$, og derfor er $h_0^l = e$. Øjensynlig er $g_1 \in \langle g_0 \rangle$. Da $h \notin \langle g_0 \rangle$, følger det først, at $h_0 \neq e$. Videre følger det, at sideklassen af h modulo $\langle g_0 \rangle$ ikke ændres, hvis h erstattes med h_0. Følgelig ændres ordenen modulo $\langle g_0 \rangle$ ikke. Ligningen (3) gælder derfor, hvis h erstattes med h_0. Da $h_0^l = e$, har vi således opnået den søgte ligning (1).

Hermed er sætningen bevist. $\square$

(6.10) Struktursætning for endelige abelske grupper. *Lad G være en endelig abelsk gruppe af orden n. Da gælder:* (1) *Gruppen G er isomorf med et produkt af cykliske grupper,*

$$G \simeq \mathrm{C}_{m_1} \times \cdots \times \mathrm{C}_{m_r}, \tag{6.10.1}$$

hvor $m_i > 1$ for alle i. (Her vedtager vi, at et produkt af *ingen* grupper er den trivielle gruppe, således at vi for den trivielle gruppe har en isomorfi med $r = 0$.)

(2) *Ordenerne $m_1, \dots, m_r$ kan vælges således, at m_{i+1} er divisor i m_i for $i = 1, \dots, r-1$. Med et sådant valg er følgen $m_1, \dots, m_r$ entydigt bestemt.*

(3) *Ordenerne $m_1, \dots, m_r$ kan vælges således, at hvert m_j er en primtalspotens. Med et sådant valg er tallene m_j (med multiplicitet) entydigt bestemt.*

Bevis. Eksistensen af isomorfien (6.10.1) vises ved fuldstændig induktion efter ordenen $|G|$. Med vedtagelsen nævnt i (1) er eksistensen triviel, hvis $|G| = 1$. Antag, at $|G| > 1$. Lad $g \in G$ være et element af maksimal elementorden m. Da er $m > 1$, og $\langle g \rangle$ er isomorf med C_m. Af Sætning (6.9) fås derfor en isomorfi $G \simeq \mathrm{C}_m \times G'$ med en undergruppe G' af G. Af isomorfien følger $|G| = m|G'|$. Specielt er $|G'| < |G|$. Induktivt er G' derfor isomorf med et produkt af cykliske grupper. Følgelig er også $G = \mathrm{C}_m \times G'$ isomorf med et produkt af cykliske grupper. Hermed er (1) bevist.

Det samme (induktive) argument giver, at tallene m_i kan vælges således, at $m_{i+1}\,|\,m_i$. Tallet $m := m_1$ var jo valgt som den maksimale elementorden i G, og med notationen i argumentet er m_2 den maksimale elementorden i G' osv. Da G' er en undergruppe af G, er m_2 ordenen af et element i G. Af Sætning (6.8) følger derfor, at $m_2\,|\,m_1$.

For at indse, at tallene m_i kan vælges som primtalspotenser, bruges Sætning (6.5) på primopløsningen af n. Det følger, at G er isomorf med et produkt af undergrupper $G(p)$, svarende til primdivisorerne p i n. Hvert element h i $G(p)$ opfylder en ligning $h^{p^\nu} = e$. Heraf følger, at ordenen af hvert element i $G(p)$ er en potens af p. Ifølge det allerede viste er $G(p)$ isomorf med et produkt af cykliske grupper; hver af de cykliske faktorer må altså være frembragt af et element, hvis orden er en potens af p. Hver faktor har altså en orden, der er en potens af p. Det følger, at G er isomorf med et produkt af cykliske grupper, hvor hver faktors orden er en primtalspotens.

Vi mangler at vise entydigheden i (2) og i (3). For hvert primtal p kan vi betragte delmængden,

$$ {}_pG := \{x \in G \mid x^p = e\}. $$

Det er let at se, at ${}_pG$ er en undergruppe i G. Undergruppens orden er antallet af løsninger $x \in G$ til ligningen $x^p = e$. For en sådan løsning x er ordenen en divisor i p. Da p er et primtal, følger det, at en løsning $x \neq e$ til ligningen nødvendigvis har orden p. Specielt har vi $|{}_pG| = 1$, hvis p ikke er divisor i $|G|$. Hvis G er cyklisk, og p er divisor i $|G|$, findes netop én undergruppe af orden p i G. I dette tilfælde gælder altså $|{}_pG| = p$. Hvis G er et produkt af grupper G_i,

$$ G = G_1 \times \cdots \times G_r, \tag{6.10.2} $$

så er hvert element $x \in G$ et r-sæt $(x_1, \dots, x_r)$. Vi har $x^p = e$, hvis og kun hvis $(x_1^p, \dots, x_r^p) = (e, \dots, e)$, altså hvis og kun hvis $x_i \in {}_pG_i$ for $i = 1, \dots, r$. Følgelig er ${}_pG = {}_pG_1 \times \cdots \times {}_pG_r$ og $G/{}_pG = (G_1/{}_pG_1) \times \cdots \times (G_r/{}_pG_r)$. Specielt er

$$ |{}_pG| = |{}_pG_1| \cdots |{}_pG_r|. \tag{6.10.3} $$

Af en isomorfi (6.10.1) får vi fremstillingen (6.10.2) med $G_i = \mathrm{C}_{m_i}$. Hver gruppe G_i er altså cyklisk. Det følger, at hver faktor $|{}_pG_i|$ i (6.10.3) er lig med 1 eller lig med p. Specielt er $|{}_pG|$ en potens p^s, hvor $s \leqslant r$. Hvis m_{i+1} er divisor i m_i for $i = 1, \dots, r-1$, ser vi, at $|{}_pG| = p^r$, hvis $p\,|\,m_r$ og at $|{}_pG| = p^s$ med $s < r$, hvis $p \nmid m_r$. Hvis hvert m_j er en primtalspotens, $m_j = p_j^{\mu_j}$, ser vi, at $|{}_pG| = p^s$, hvor s er antallet af indices j, for hvilke $p_j = p$.

Nu vises entydigheden ved fuldstændig induktion efter ordenen af G. Lad der være givet endnu en fremstilling, med r' cykliske faktorer af ordener $m'_1, \dots, m'_{r'}$. Antag, at begge fremstillinger opfylder kravene i (2). Vælg en primdivisor p i m_r. Da $|{}_pG| = p^r$, følger det, at $r \leqslant r'$. Af symmetrigrunde er altså $r = r'$, og nu følger det, at $p\,|\,m'_r$. For kvotienten $G/{}_pG$ har vi nu to fremstillinger, med cykliske faktorer af ordener $m_1/p, \dots, m_r/p$ og $m'_1/p, \dots, m'_r/p$ (hvor nogle af ordenerne m_i/p eller m'_i/p eventuelt kan være 1). Induktivt sluttes, at $m_1/p = m'_1/p, \dots, m_r/p = m'_r/p$, hvoraf entydigheden i (2) fremgår.

Antag i stedet, at alle tallene m_j og m'_j er primtalspotenser. Det skal vises, for hver primtalspotens p^μ, at antallet af gange p^μ forekommer blandt tallene m_j er det samme som antallet af gange p^μ forekommer blandt tallene m'_j. Ved at omnummerere faktorerne kan vi antage, at det netop er ordenerne $m_1, \dots, m_s$ og $m'_1, \dots, m'_{s'}$, der er potenser af p, og vi kan antage, at $m_1 \geqslant \cdots \geqslant m_s$ og $m'_1 \geqslant \cdots \geqslant m'_{s'}$. Det skal så vises, at $s = s'$ og at $m_i = m'_i$ for $i = 1, \dots, s$. Den første påstand følger af, at vi har $|{}_pG| = p^s = p^{s'}$. Den anden følger ved at betragte de to fremstillinger af kvotienten $G/{}_pG$, ganske som i tilfældet (2). Hermed er også entydigheden i (3) bevist. ▯

(6.11) Observation. Af Struktursætningen fremgår, hvor mange kommutative grupper der findes af en given endelig orden n. Lad nemlig $n = p_1^{\nu_1} \cdots p_s^{\nu_s}$ være en primopløsning. Enhver kommutativ gruppe G af orden n er så isomorf med et produkt,

$$G = \mathrm{C}_{m_1} \times \cdots \times \mathrm{C}_{m_r},$$

hvor hvert m_j er en primtalspotens. Af isomorfien følger ligningen $n = m_1 \cdots m_r$ mellem ordenerne. Specielt følger heraf, at hvert m_j må være en potens af et af primtallene p_i, endda af formen p_i^μ, hvor $\mu \leqslant \nu_i$. Yderligere følger det, at produktet af de tal m_j, for hvilke m_j er en potens af p_i, er lig med $p_i^{\nu_i}$.

De mulige fremstillinger svarer altså til de mulige måder, hvorpå hvert $p_i^{\nu_i}$ kan skrives som et produkt af potenser af p_i eller, ækvivalent, de mulige måder, hvorpå eksponenten ν_i kan skrives som sum af positive eksponenter. Disse mulige valg svarer ifølge entydigheden i (3) præcis til de forskellige (på nær isomorfi) kommutative grupper af orden n.

Det følger i øvrigt af Struktursætningen, for en kommutativ gruppe G af orden n, at undergrupperne $G(p_i)$ bestemt i (6.6) har orden $p_i^{\nu_i}$. Hvert element i $G(p_i)$ har nemlig en orden, der er en potens af p_i. Følgelig er $G(p_i)$ isomorf med et produkt af cykliske grupper, hvis ordener er potenser af p_i. Specielt har $G(p_i)$ en orden, som er en potens af p_i. Da vi desuden har ligningerne,

$$|G(p_1)| \cdots |G(p_s)| = |G| = n = p_1^{\nu_1} \cdots p_s^{\nu_s},$$

følger det, at $|G(p_i)| = p_i^{\nu_i}$ for alle i.

(6.12) Eksempel. Der er præcis 3 kommutative grupper af orden $24 = 2^3 3$, nemlig

$$\mathrm{C}_{24} = \mathrm{C}_8 \times \mathrm{C}_3, \quad \mathrm{C}_{12} \times \mathrm{C}_2 = \mathrm{C}_4 \times \mathrm{C}_2 \times \mathrm{C}_3, \quad \mathrm{C}_6 \times \mathrm{C}_2 \times \mathrm{C}_2 = \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_3 .$$

(6.13) Opgaver.

1. Vis, at gruppen $\mathbb{C}^*$ er det direkte produkt af sine undergrupper $\mathbb{U}$ og $\mathbb{R}_+^*$ (enhedscirklen og den positive reelle halvakse).

2. Antag, at der er givet grupper G_i og undergrupper $H_i \subseteq G_i$ for $i = 1, \dots, r$. Vis, at produktet $H := H_1 \times \cdots \times H_r$ er en undergruppe i produktet $G = G_1 \times \cdots \times G_r$. Vis, at hvis H_i er normal i G_i for alle i, så er H normal i G, og der findes en kanonisk isomorfi,

$$(G_1 \times \cdots \times G_r)/(H_1 \times \cdots \times H_r) \xrightarrow{\sim} (G_1/H_1) \times \cdots \times (G_r/H_r).$$

3. *Vis, at undergruppen H_i i (6.5) har orden n_i.

4. Angiv de kommutative grupper af orden 32.

5. Angiv 7 ikke-kommutative grupper af orden 24. [Vink: prøv med grupper af formen $G_1 \times G_2$, hvor G_1 og/eller G_2 er nogen af de ikke-kommutative grupper, du kender.]

6. Angiv fremstillingen af $(\mathbb{Z}/72)^*$ som produkt af cykliske grupper af primtalspotensorden.

7. En *karakter* på gruppen G er en homomorfi $\chi : G \to \mathbb{U}$. Specielt er karaktererne komplekse funktioner $G \to \mathbb{C}$. Vis, at med sædvanlig multiplikation af funktioner udgør karaktererne på G en kommutativ gruppe. Den kaldes *karaktergruppen* for G, og vi betegner den $\widehat{G}$. Vis, at hvis G er cyklisk af orden n, så er $\widehat{G}$ cyklisk af orden n. Hvordan bestemmes karaktererne på et direkte produkt $G_1 \times G_2$? Lad G være en endelig kommutativ gruppe. Vis, fx ved hjælp af Struktursætningen, at der findes en isomorfi $G \simeq \widehat{G}$ af G på karaktergruppen $\widehat{G}$.

8. Vis, at for en gruppehomomorfi $\varphi \colon H \to G$ defineres ved $\chi \mapsto \chi \circ \varphi$ en gruppehomomorfi $\hat{\varphi} \colon \widehat{G} \to \widehat{H}$. Vis, at hvis $H \to G$ er surjektiv, så er $\widehat{G} \to \widehat{H}$ injektiv. *Vis, at hvis H er undergruppe af en endelig kommutativ gruppe G, så er $\widehat{G} \to \widehat{H}$ surjektiv og kernen for $\widehat{G} \to \widehat{H}$ er undergruppen $\widehat{G/H}$ af $\widehat{G}$.

9. Lad G være en endelig kommutativ gruppe. Vis, at for hvert $g \in G$ er afbildningen $\chi \mapsto \chi(g)$ en homomorfi $\widehat{G} \to \mathbb{U}$, altså en karakter på $\widehat{G}$. Vis, at den herved bestemte afbildning $G \to \widehat{\widehat{G}}$ er en homomorfi. Vis, at homomorfien er injektiv, og slut, at den er en isomorfi.

10. *Lad G være en endelig abelsk gruppe af orden n. Funktionerne $f \colon G \to \mathbb{C}$ udgør da et komplekst vektorrum $\mathcal{F}(G)$ af dimension n. Det udstyres med det indre produkt,

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g) \overline{f_2(g)}.$$

Vis, at de n karakterer på G udgør en ortonormal basis for $\mathcal{F}(G)$. [Vink: udregn, for to karakterer χ_1, χ_2 og $h \in G$, summen $\sum_{g_1 g_2 = h} \chi_1(g_1)\chi_2(g_2)$.]

11. Ud fra en fremstilling af formen i (2) i Struktursætningen (6.10) får man en fremstilling af formen i (3) ved at bruge Den kinesiske Restklassesætning på hver faktor C_{m_i}. Hvordan får man omvendt, fra en fremstilling af formen i (3), en fremstilling af formen i (2)?

12. *Det var nærliggende at bevise entydigheden i Struktursætningen (6.10)(2) på følgende måde: Antag, at vi har givet to fremstillinger $G = \mathrm{C}_{m_1} \times \cdots = \mathrm{C}_{m'_1} \times \cdots$ af den nævnte form. Af formen af fremstillingen følger, at m_1 (og m'_1) er den maksimale elementorden i G, så $m'_1 = m_1$. Vi har altså en isomorfi $\mathrm{C}_{m_1} \times H \simeq \mathrm{C}_{m_1} \times H'$, hvor H og H' er produkterne af de øvrige faktorer i fremstillingen. Heraf ville vi gerne slutte, at $H \simeq H'$, for så følger det induktivt, at de to fremstillinger er ens. Problemet er, at vi *ikke* har bevist *forkortningsreglen:* Hvis $C \times H \simeq C \times H'$, så er $H \simeq H'$. Vis, som konsekvens af Struktursætningen, at forkortningsreglen gælder for endelige kommutative grupper. Vis, at den ikke gælder for uendelige grupper. I øvrigt kan man vise, at forkortningsreglen gælder for alle endelige grupper.

13. Lad G være en endelig kommutativ gruppe. Vis for et primtal p, at antallet af elementer i G, der har orden 1 eller p, er en potens af p.

14. *Lad G være en endelig kommutativ gruppe, og lad a være produktet af samtlige elementer i G. Vis, at $a = e$, på nær hvis G har præcis ét element af orden 2; og at a i undtagelsestilfældet er det entydigt bestemte element af orden 2. Hvilken konklusion fås for $G = (\mathbb{Z}/n)^*$? [Vink: Kan vises ved hjælp af struktursætningen, men også uden.]

7. Gruppevirkninger.

(7.1) Indledning. For en given gruppe G vil der altid være visse mængder X, som gruppen *virker* på i den forstand, at gruppens elementer „gør noget“ ved X: gruppeelementerne flytter rundt på elementerne i X. Mange grupper er „født“ med en naturlig virkning på en bestemt mængde.

I dette kapitel kigger vi på en lang række begreber knyttet til gruppers virkning. Hovedresultatet er en tælleformel af kombinatorisk art, der har anvendelser både på abstrakt gruppeteori og på konkrete optællinger af mønstre.

(7.2) Definition. Lad G være en fast (multiplikativt skrevet) gruppe. Vi vil betegne det neutrale element i G med symbolet 1. Gruppen G siges at *virke* på mængden X, hvis der er givet en afbildning $G \times X \to X$, betegnet $(g, x) \mapsto g.x$, således, at følgende ligninger er opfyldt, for $x \in X$ og $g, h \in G$:

$$1.x = x, \qquad (gh).x = g.(h.x)\,. \tag{7.2.1}$$

Hvis der er givet en virkning af G på X, siges X også at være en *G-mængde*.

Når G virker på X, kan vi til et givet gruppeelement $g \in G$ knytte afbildningen $X \to X$ bestemt ved $x \mapsto g.x$. Denne afbildning betegnes ρ_g eller g_X, altså

$$\rho_g(x) = g_X(x) := g.x\,.$$

Det følger af den første ligning i (7.2.1), at $\rho_1(x) = x$ for alle x. Afbildningen $\rho_1 = 1_X$ er altså den identiske afbildning id_X. For hvert element $g \in G$ er afbildningen ρ_g bijektiv. Af ligningerne i (7.2.1) følger nemlig, for $x \in X$, at

$$\rho_{g^{-1}} \circ \rho_g(x) = \rho_{g^{-1}}(g.x) = g^{-1}.(g.x) = (g^{-1}g).x = 1.x = x\,.$$

Altså er $\rho_{g^{-1}} \circ \rho_g = \mathrm{id}_X$. Tilsvarende, eller ved at erstatte g med g^{-1}, følger det, at $\rho_g \circ \rho_{g^{-1}} = \mathrm{id}_X$. Altså er afbildningen ρ_g bijektiv, og den inverse er bestemt ved $(\rho_g)^{-1} = \rho_{g^{-1}}$.

Da afbildningen ρ_g er bijektiv, er ρ_g element i gruppen $\mathrm{Perm}(X)$ af alle bijektive afbildninger af X på sig selv. Følgelig kan vi opfatte $g \mapsto \rho_g$ som en afbildning $G \to \mathrm{Perm}(X)$, fra gruppen G til gruppen $\mathrm{Perm}(X)$. Afbildningen er en gruppehomomorfi,

$$\rho\colon G \to \mathrm{Perm}(X). \tag{7.2.2}$$

Af den anden ligning i (7.2.1) følger nemlig, at vi har $\rho_{gh}(x) = (gh).x = g.(h.x) = \rho_g(\rho_h(x))$. Altså er $\rho_{gh} = \rho_g \circ \rho_h$, og det er netop betingelsen for at ρ er en homomorfi.

Homomorfien ρ kaldes den til virkningen hørende *repræsentation* af G. Når virkningen af G på X er givet, *repræsenteres* hvert gruppeelement $g \in G$ som en permutation ρ_g af mængden X. Er der omvendt givet en gruppehomomorfi (7.2.2), er det let at se, at der ved $g.x := \rho_g(x)$ defineres en virkning af G på X.

(7.3) Note. En afbildning $G \times X \to X$ kaldes også en *(ydre) komposition*. Den knytter til et gruppeelement $g \in G$ og et element x i mængden X et element i X, kaldet *kompositet* af x med g. Når kompositet er betegnet som $g.x$, kan betingelserne for at kompositionen definerer en virkning udtrykkes ved ligningerne (7.2.1). Men det skal understreges, at betingelserne er uafhængige af den notation, der er valgt for kompositet. Af og til skrives blot gx for kompositet. En anden almindeligt brugt notation er at skrive ${}^g x$ for kompositet. Med denne notation er betingelserne, at ${}^1 x = x$ og ${}^{gh} x = {}^g({}^h x)$.

Bemærk, at notationen $g.x$ for billedet af (g, x) ved en virkning $G \times X \to X$ er ganske forstyrrende, når G er en (kommutativ) additivt skrevet gruppe, idet kravene jo er, at $0.x = x$ og at $(g + h).x = g.(h.x)$. I dette tilfælde vil det være naturligt at vælge en alternativ notation for kompositet. Eventuelt kan virkningen bestemmes ved blot at angive den tilhørende repræsentation ρ.

Bemærk også, at en ydre komposition $G \times X \to X$, betegnet $(g, x) \mapsto x.g$, som opfylder betingelserne,

$$x.1 = x, \quad x.(gh) = (x.g).h, \tag{7.3.1}$$

i almindelighed *ikke* vil være en virkning af G på X. Et krav til en virkning er jo, at kompositet af x med gruppeelementet gh kan fås ved først at komponere x med h og dernæst resultatet heraf med g, og dette krav vil i almindelighed ikke være opfyldt, idet g og h forekommer i den „forkerte rækkefølge" i (7.3.1).

En ydre komposition, der opfylder betingelserne i (7.3.1) siges også at være en *højre-virkning* af G på X. I modsætning hertil kaldes en virkning af G på X, som defineret i (7.2), også en *venstre-virkning*.

(7.4) Triviel virkning. Den *trivielle virkning* af G på mængden X er bestemt ved

$$g.x := x \text{ for alle } g \in G,\ x \in X.$$

Den tilhørende repræsentation er den trivielle homomorfi $G \to \mathrm{Perm}(X)$, som afbilder alle elementer i G på identiteten id_X i $\mathrm{Perm}(X)$.

(7.5) Eksempel. (1) Hvis G er en undergruppe i den fulde transformationsgruppe $\mathrm{Perm}(X)$ for mængden X, defineres en virkning af G på X ved

$$g.x := g(x).$$

Den tilhørende repræsentation er inklusionshomomorfien $G \to \mathrm{Perm}(X)$.

Specielt fås for $X = \{1, 2, \dots, n\}$ en virkning af den symmetriske gruppe S_n på X.

(2) Den generelle lineære gruppe $\mathrm{GL}_n(\mathbb{R})$ virker på talrummet $X := \mathbb{R}^n$ idet

$$g.x := gx,$$

hvor højresiden er produktet af matricen g og n-sættet x opfattet som søjlevektor. Den tilhørende repræsentation afbilder matricen g på den bijektive lineære afbildning $x \mapsto gx$.

(3) For et reelt vektorrum V er multiplikation af vektorer med skalarer en ydre komposition $\mathbb{R} \times V \to V$, betegnet $(a, v) \mapsto av$. Som bekendt gælder ligningerne $1v = v$ og $(ab)v = a(bv)$, for vektorer $v \in V$ og skalarer $a, b \in \mathbb{R}$. Multiplikation med skalarer forskellige fra 0 er derfor en virkning af den multiplikative gruppe $\mathbb{R}^*$ på mængden V.

(7.6) Translation. Gruppen G virker på sig selv, altså på mængden $X = G$, ved *translation*, idet vi for $g \in G$ og $x \in G$ sætter
$$g.x := gx \, .$$
Den anden ligning i (7.2.1) er blot den associative lov i gruppen G, og den første ligning følger af, at 1 er det neutrale element i G.

Det er klart, at vi med $x.g := xg$ definerer en højre-virkning af G på sig selv.

(7.7) Cayley's Sætning. *Lad G være en gruppe og lad* $\mathrm{Perm}(G)$ *være gruppen af alle permutationer af G. Lad G virke på sig selv ved translation. Da er den tilhørende repræsentation en injektiv gruppehomomorfi,*
$$\rho \colon G \to \mathrm{Perm}(G).$$

Bevis. Til gruppeelementet g hører ved repræsentationen den bijektive afbildning ρ_g bestemt ved $\rho_g(x) = gx$. Da repræsentationen er en homomorfi $\rho \colon G \to \mathrm{Perm}(G)$, er det nok at vise, at kernen kun består af det neutrale element 1 i G. Antag derfor, at ρ_g er identiteten i $\mathrm{Perm}(G)$. Da er $gx = x$ for alle $x \in G$. Specielt er så $g1 = 1$, og følgelig er $g = 1$. Hermed er det bevist, at repræsentationen er injektiv. □

(7.8) Definition. Til en given virkning af G på en mængde X hører virkninger af G på en række mængder knyttet til X. For eksempel virker G på potensmængden $\mathcal{P}(X)$, idet vi for en delmængde $A \subseteq X$ definerer
$$g.A := \{g.a \mid a \in A\}. \tag{7.8.1}$$
Tilsvarende virker G på produktmængden $X \times X$ ved definitionen,
$$g.(x_1, x_2) := (g.x_1, g.x_2). \tag{7.8.2}$$
Hvis Y er en vilkårlig mængde, virker G på mængden X^Y af alle afbildninger $\xi : Y \to X$ ved definitionen,
$$(g.\xi)(y) := g.(\xi(y)). \tag{7.8.3}$$
Betragter vi i stedet mængden Y^X af afbildninger $\eta \colon X \to Y$ fås en virkning af G på Y^X ved definitionen,
$$(g.\eta)(x) := \eta(g^{-1}.x). \tag{7.8.4}$$
Det er let at se, at ovenstående definitioner bestemmer virkninger af G på de betragtede mængder.

Lad H være en undergruppe af G. En delmængde Z af X siges da at være *H-invariant* eller *H-stabil*, hvis der for alle $h \in H$ og $z \in Z$ gælder, at $h.z \in Z$. Når Z er H-invariant, definerer $(h, z) \mapsto h.z$ en afbildning $H \times Z \to Z$, som klart er en virkning af gruppen H på mængden Z. Den siges at fremkomme ved *restriktion* af den givne virkning af G på X.

For eksempel bestemmes altid ved restriktion en virkning af H på X, og for hver G-invariant delmængde Z af X bestemmes en virkning af G på Z.

(7.9) Eksempel. Den additive gruppe $\mathbb{R}$ virker på sig selv ved translation. For $t \in \mathbb{R}$ er translationen ρ_t bestemt ved $\rho_t(x) = x + t$ for $x \in \mathbb{R}$. Ligningen (7.8.4) fastlægger, hvordan gruppen $\mathbb{R}$ virker på mængden af alle afbildninger $\eta\colon \mathbb{R} \to Y$, hvor Y er en vilkårlig mængde. Afbildningen $\rho_t(\eta)$ er bestemt ved $\rho_t(\eta)\,(x) = \eta(x - t)$.

(7.10) Eksempel. Diedergruppen D_n er defineret som en undergruppe i den generelle lineære gruppe $\mathrm{GL}_2(\mathbb{R})$. Gruppen $\mathrm{GL}_2(\mathbb{R})$ virker på planen $\mathbb{R}^2$, så ved restriktion fås en virkning af diedergruppen D_n på $\mathbb{R}^2$. De n hjørner $p_1, \dots, p_n = p_0$ i n-kanten, jfr (1.21), udgør en D_n-invariant delmængde X af $\mathbb{R}^2$. Specielt virker D_n på mængden af de n hjørner, og den tilhørende repræsentation er en homomorfi $\rho\colon \mathrm{D}_n \to \mathrm{S}_X$. Repræsentationen er injektiv, hvis $n \geqslant 3$. Er nemlig ρ_g identiteten i S_X, så er specielt $\rho_g(p_0) = p_0$ og $\rho_g(p_1) = p_1$, altså $gp_0 = p_0$ og $gp_1 = p_1$; da vektorerne p_0 og p_1 er lineært uafhængige og $x \mapsto gx$ er en lineær afbildning, følger det, at $g = 1$. Identificeres de n hjørner $p_1, \dots, p_n$ i rækkefølge med tallene $1, 2, \dots, n$, svarer repræsentationen til en homomorfi,

$$\rho\colon \mathrm{D}_n \to \mathrm{S}_n .$$

Denne homomorfi er altså injektiv, når $n \geqslant 3$. Bemærk, at under denne homomorfi afbildes drejningen D med vinklen $2\pi/n$ på n-cyklen $(1\,2\,\dots\,n)$. Spejlingen i aksen gennem midtpunktet af kanten p_0p_1 afbildes i permutationen ω bestemt ved $\omega(i) = n + 1 - i$.

(7.11) Eksempel. Hexaedergruppen H, som vi senere ser nærmere på, består af de 24 drejninger i rummet $\mathbb{R}^3$, under hvilke en given terning (med midtpunkt i origo) er invariant; drejningerne er omkring symmetriakser, der kan være en *sideakse* (linie gennem midtpunktet af to modstående sider), en *kantakse* eller en *hjørneakse*. Specielt virker H på hele $\mathbb{R}^3$. Delmængden bestående af hexaederets hjørner er invariant, så H virker på denne delmængde med 8 elementer. Drejningerne i H permuterer altså de 8 hjørner, og herved bestemmes en repræsentation $\mathrm{H} \to \mathrm{S}_8$. De 6 sidemidtpunkter udgør ligeledes en invariant delmængde, og herved bestemmes en repræsentation $\mathrm{H} \to \mathrm{S}_6$.

Hexaedergruppen virker også på mængden af delmængder af $\mathbb{R}^3$. Systemet bestående af de 12 kanter er øjensynlig en invariant delmængde. Drejningerne i H permuterer altså de 12 kanter, og herved bestemmes en repræsentation $\mathrm{H} \to \mathrm{S}_{12}$. Tilsvarende virker H på systemet af de 6 sider; den tilsvarende repræsentation $\mathrm{H} \to \mathrm{S}_6$ er naturligvis identisk med repræsentationen bestemt ved virkningen på sidernes midtpunkter. Videre virker H på systemet af de 4 hjørneakser. Det er ikke svært at vise, at den tilhørende repræsentation $\mathrm{H} \to \mathrm{S}_4$ er bijektiv; specielt er H isomorf med S_4. Endelig virker H på systemet bestående af de 3 sideakser. Herved bestemmes en repræsentation $\mathrm{H} \to \mathrm{S}_3$. Det er ikke svært at vise, at homomorfien $\mathrm{H} \to \mathrm{S}_3$ er surjektiv. Dens kerne er Klein's Vierer-gruppe.

(7.12) Definition. Antag, at gruppen G virker på mængden X. To elementer $x, x' \in X$ kaldes da *G-ækvivalente*, og vi skriver

$$x' \sim x \qquad \text{(eller udførligt: } x' \underset{G}{\sim} x\text{)},$$

hvis der findes et gruppeelement $g \in G$ således, at $x' = g.x$. Relationen er en ækvivalensrelation. Den er nemlig refleksiv, fordi $x = 1.x$; den er symmetrisk, thi af $x' = g.x$ følger $x = g^{-1}.x'$; endelig er den transitiv, thi af $x' = g.x$ og $x'' = h.x'$ følger $x'' = (hg).x$.

Ækvivalensklasserne kaldes *baner*. For et givet element $x \in X$ kan vi betragte banen *gennem* x (eller *bestemt ved* x), dvs banen, der indeholder x. Det er delmængden $G.x$ bestemt ved

$$G.x := \{g.x \mid g \in G\}. \tag{7.12.1}$$

Elementantallet i en bane kaldes også banens *længde*. Det er klart, at længden er endelig, når G er en endelig gruppe eller når X er en endelig mængde.

Mængden af ækvivalensklasser, altså mængden af baner, kaldes *banerummet*, og betegnes

$$X/G \qquad \text{(læses: „}X\text{ modulo }G\text{“).}$$

Banerummet er altså kvotienten af X mht G-ækvivalens.

Ligningen $g.x = x$, for $g \in G$ og $x \in X$, har fundamental betydning. Hvis ligningen er opfyldt, siges elementet x at være *fixpunkt* for (eller *invariant* under) gruppeelementet g, og g siges at *stabilisere* x.

For et givet element $x \in X$ betegnes med G_x mængden af de elementer $g \in G$, der stabiliserer x, altså

$$G_x := \{g \in G \mid g.x = x\}. \tag{7.12.2}$$

Det er let at se, at G_x er en undergruppe af G. Den kaldes også *isotropigruppen* eller *stabilisatorgruppen* for x.

For et givet gruppeelement g betegnes med X^g mængden af de elementer x, der er fixpunkter for g, altså

$$X^g := \{x \in X \mid g.x = x\}. \tag{7.12.3}$$

Endelig siges elementet $x \in X$ at være *fixpunkt for virkningen* af G, eller at være *G-invariant*, hvis det er fixpunkt for hvert gruppeelement g. Alternativt er x et fixpunkt for virkningen, hvis og kun hvis isotropigruppen G_x er hele G eller, ækvivalent, hvis og kun hvis banen $G.x$ består alene af x (banen er en *et-punkts-bane*). Mængden af fixpunkter for virkningen betegnes X^G, altså

$$X^G = \bigcap_{g \in G} X^g = \{x \in X \mid G_x = G\} = \{x \in X \mid G.x = \{x\}\}.$$

(7.13) Eksempler. (1) Betragt den trivielle virkning af G på X. Her er G-ækvivalens blot lighed. Alle baner er et-punkts-baner, og banerummet kan identificeres med X. Ethvert punkt $x \in X$ er fixpunkt for virkningen.

(2) Betragt for en endelig mængde X virkningen af permutationsgruppen $G := \mathrm{Perm}(X)$ på X. For to forskellige elementer $x, x' \in X$ er transpositionen $\gamma = (x\,x')$ en bijektiv afbildning således, at $x' = \gamma(x)$. Alle elementer er derfor ækvivalente, og der er kun én bane. Betragt, for en given permutation $\sigma \in \mathrm{Perm}(X)$, den cykliske undergruppe $\langle\sigma\rangle$, bestående af potenserne σ^i for $i \in \mathbb{Z}$. Ved restriktion bestemmes en virkning af $\langle\sigma\rangle$ på X. Banen gennem x er her delmængden bestående af billederne $\sigma^i(x)$ for $i \in \mathbb{Z}$. Banerne for virkningen af gruppen $\langle\sigma\rangle$ er med andre ord netop banerne for permutationen σ. Det er klart,

at vi har $\sigma(x) = x$, hvis og kun hvis $\sigma^i(x) = x$ for alle $i \in \mathbb{Z}$. Elementet $x \in X$ er altså fixpunkt for permutationen σ, hvis og kun hvis det er fixpunkt for virkningen af $\langle\sigma\rangle$ på X.

(3) Betragt virkningen af $\mathrm{GL}_n(\mathbb{R})$ på talrummet $\mathbb{R}^n$. En vektor $x \in \mathbb{R}^n$ er fixpunkt for matricen g, hvis og kun hvis $gx = x$, dvs hvis og kun hvis x er egenvektor for den lineære afbildning $x \mapsto gx$ med egenværdi 1. Nul-vektoren 0 er fixpunkt for enhver lineær afbildning, og altså fixpunkt for virkningen. For to vilkårlige vektorer x, x', forskellige fra 0, findes som bekendt en lineær afbildning, der afbilder x i x'. Det følger, at vektorerne forskellige fra 0 udgør en bane.

(4) Betragt virkningen af $\mathbb{R}^*$ på et vektorrum V, givet ved multiplikation af vektorer med skalarer. Nul-vektoren 0 er fixpunkt, idet $a0 = 0$ for alle $a \in \mathbb{R}^*$; nul-vektoren udgør altså én bane. For en vektor $v \neq 0$ består banen af alle multipla av med $a \neq 0$. Banen fås altså af det 1-dimensionale underrum bestemt ved v ved at fjerne nul-vektoren.

(5) Den additive gruppe $\mathbb{R}$ virker på $\mathbb{C}$ ved drejninger: repræsentationen er bestemt ved $\rho_t(z) = e^{it}z$. Tallet 0 er fixpunkt for virkningen, så $\{0\}$ er en bane. De øvrige baner er cirklerne med centrum i 0.

(6) Betragt virkningen af G på $X := G$ bestemt ved translation. For to givne elementer $x, x' \in G$ findes et gruppeelement $g \in G$ således, at $x' = g.x$, nemlig $g := x'x^{-1}$. Alle elementer er derfor ækvivalente, og der er kun én bane. Ligningen $gx = x$ er kun opfyldt for $g = 1$. For hvert $x \in G$ er isotropigruppen G_x altså den trivielle undergruppe $\{1\}$ af G.

Betragt nu restriktion til en given undergruppe H af virkningen bestemt ved translation. Gruppen, der virker, er altså H, og den virker på $X := G$. Banen gennem $x \in G$, altså delmængden $H.x$, er øjensynlig højresideklassen Hx, og banerummet er derfor mængden $H\backslash G$ af højresideklasser modulo H.

(7) Betragt virkningen af den additive gruppe $\mathbb{R}$ på funktioner $\eta\colon \mathbb{R} \to Y$, jfr Eksempel (7.9). For et givet reelt tal t er $\rho_t\eta(x) = \eta(x - t)$. Funktionen η er altså fixpunkt for gruppeelementet t, hvis $\eta(x - t) = \eta(x)$ for alle x, dvs hvis η er periodisk med periode t.

(7.14) Note. Elementerne i banerummet er delmængder af X af formen $G.x$, med $x \in X$. I overensstemmelse med andre tilsvarende notationer ville det faktisk være mest naturligt at betegne banerummet $G\backslash X$ (det læses „X modulo G“ og må naturligvis ikke forveksles med komplementærmængde). Vi vil imidlertid normalt anvende notationen X/G for banerummet (jfr dog (7.13)(6) for virkningen af H på G). Det skal understreges, at ved notationen X/G såvel som ved de øvrige notationer i (7.12) er det underforstået, hvilken virkning af G på X der er givet.

(7.15) Baneformlen. *Lad der være givet en virkning af gruppen G på mængden X. Betragt et vilkårligt element $x \in X$. Den ved $g \mapsto g.x$ bestemte afbildning $G \to X$ er da konstant på hver sideklasse modulo isotropigruppen G_x, og den inducerer en bijektiv afbildning,*

$$G/G_x \xrightarrow{\sim} G.x, \tag{7.15.1}$$

af mængden af venstre-sideklasser modulo isotropigruppen G_x på banen $G.x$. For længden af banen gælder formlen,

$$|G.x| = |G : G_x|, \tag{7.15.2}$$

altså at længden af banen gennem x er lig med index af isotropigruppen G_x. Specielt gælder, når G er en endelig gruppe, at hver banes længde er divisor i $|G|$.

Bevis. Lad $I := G_x$ være isotropigruppen. For alle elementer $g, g_0 \in G$ gælder biimplikationen,

$$gI = g_0 I \iff g.x = g_0.x\,.$$

Antag nemlig først, at $gI = g_0 I$. Da er $g \in g_0 I$, og altså $g = g_0 h$ med $h \in I$. Følgelig er $g.x = (g_0 h).x = g_0.(h.x) = g_0.x$. Antag omvendt, at $g.x = g_0.x$. Da er $(g_0^{-1}g).x = g_0^{-1}.(g.x) = g_0^{-1}.(g_0.x) = (g_0^{-1}g_0).x = 1.x = x$. Følgelig er $g_0^{-1}g \in I$, og dermed er $gI = g_0 I$.

Elementerne g, som opfylder $gI = g_0 I$ er netop elementerne $g \in g_0 I$. Implikationen fra venstre mod højre sikrer altså, at afbildningen $g \mapsto g.x$ er konstant på sideklassen $g_0 I$. Vi kan derfor definere en afbildning $\psi \colon G/I \to X$ ved at fastsætte, at værdien $\psi(g_0 I)$ er $g_0.x$. Implikationen fra højre mod venstre sikrer, at ψ er injektiv. Billedmængden for ψ er øjensynlig banen $G.x$. Afbildningen ψ definerer derfor den bijektive afbildning (7.15.1).

Formlen (7.15.2) følger af, at afbildningen i (7.15.1) er bijektiv, idet elementantallet i G/G_x jo er index af G_x. Af Lagrange's Indexsætning følger nu specielt, når G er endelig, at $|G.x|$ er divisor i $|G|$. □

(7.16) Eksempel. Gruppen G virker på sig selv ved translation, og dermed, jfr (7.8), også på mængden af delmængder af G. For en delmængde $K \subseteq G$ og $g \in G$ er den translaterede delmængde blot produktet gK. Antag, at K er en undergruppe af G. For K, opfattet som delmængde af G, består banen gennem K altså af sideklasserne gK; banen er altså mængden G/K af sideklasser modulo K.

Lad nu H være endnu en undergruppe af G. Ved restriktion fås en virkning af H på delmængder af G. Under denne virkning består banen gennem K af sideklasserne hK for $h \in H$. Antallet af sådanne sideklasser er altså længden af denne bane. Ifølge baneformlen er længden lig med index i H af isotropigruppen for K. Øjensynlig er $hK = K$, netop hvis $h \in K$. Isotropigruppen er altså $H \cap K$. Vi genfinder altså resultatet fra (4.11)(1), at antallet af sideklasser hK for $h \in H$ er lig med index $|H : H \cap K|$.

(7.17) Konjugering. Gruppen G virker på sig selv, altså på mængden $X = G$, ved *konjugering*, idet vi for $g \in G$ og $x \in G$ sætter

$${}^{g}x := gxg^{-1}.$$

Det er nemlig klart, at ${}^{1}x = x$ og da

$${}^{gh}x = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = g({}^{h}x)g^{-1} = {}^{g}({}^{h}x),$$

er begge ligninger svarende til (7.2.1) opfyldt. Ved denne virkning svarer til hvert element $g \in G$ den bijektive afbildning $x \mapsto gxg^{-1}$. Den kaldes *konjugering med g*. Det er værd at bemærke, at konjugering med g er en *gruppeautomorfi*, dvs en bijektiv homomorfi af gruppen på sig selv. Dette følger af ligningerne,

$${}^{g}(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = {}^{g}x\,{}^{g}y.$$

For den til denne virkning hørende ækvivalensrelation har vi for elementer $x, x' \in G$, at $x' \sim x$, hvis og kun hvis der findes et element $g \in G$ således, at $x' = gxg^{-1}$. Ækvivalente elementer siges også at være *konjugerede*, og banerne for virkningen, altså ækvivalensklasserne, kaldes *konjugeretklasser* i gruppen G.

For et givet element x i G består isotropigruppen af de elementer $g \in G$ for hvilke $gxg^{-1} = x$. Øjensynlig er $gxg^{-1} = x$, hvis og kun hvis $gx = xg$. Isotropigruppen er altså undergruppen,

$$C(x) := \{g \in G \mid gx = xg\},$$

bestående af de elementer $g \in G$, der kommuterer med x. Denne undergruppe kaldes *centralisatoren* for elementet $x \in G$, og den kan udførligt betegnes $C_G(x)$. Da g specielt kommuterer med alle potenser g^i, er $\langle g \rangle \subseteq C(g)$.

For et givet element g i G består fixpunkterne for g af de elementer $x \in G$, for hvilke $gxg^{-1} = x$. Fixpunkterne for g er altså de elementer $x \in G$, der kommuterer med g; mængden af fixpunkter for $g \in G$ er altså centralisatoren $C(g)$.

Det følger, at fixpunkterne for virkningen er de elementer $x \in G$, der kommuterer med alle elementer $g \in G$. Denne delmængde af gruppen G kaldes gruppens *centrum*, og den betegnes $\mathrm{Cent}(G)$, altså,

$$\mathrm{Cent}(G) := \{x \in G \mid gx = xg \text{ for alle } g \in G\}.$$

Det er let at indse, at $\mathrm{Cent}(G)$ er en undergruppe af G. Bemærk, at konjugeretklassen indeholdende gruppeelementet x består alene af x, hvis og kun hvis x tilhører centret. Elementerne i centret svarer altså til konjugeretklasser med netop ét element.

Det følger af Baneformlen, at *antallet af elementer i G, der er konjugerede til et givet element $x \in G$ er lig med index $|G : C(x)|$*. Specielt gælder, når G er en endelig gruppe, at elementantallet i en konjugeretklasse er divisor i $|G|$.

Lad os endelig bemærke, at disse begreber er trivielle for en kommutativ gruppe. Hvis G er kommutativ, er ${}^g x = gxg^{-1} = gg^{-1}x = x$, så konjugering er den trivielle virkning. For hvert element $x \in G$ består konjugeretklassen gennem x alene af x, og centralisatoren for x er hele gruppen G. En kommutativ gruppe er lig med sit eget centrum.

(7.18) Konjugerede permutationer. *To permutationer af en endelig mængde X er konjugerede, hvis og kun hvis de har samme cykeltype.*

Bevis. Lad μ være en permutation af X, og lad γ være en p-cykel, $\gamma = (x_1 \ \dots \ x_p)$. Vi påstår først, at for den konjugerede permutation ${}^\mu\gamma = \mu\gamma\mu^{-1}$ har vi ligningen,

$$\mu\gamma\mu^{-1} = (\mu(x_1) \ \dots \ \mu(x_p)). \tag{7.18.1}$$

Det skal vises, at ligningens to sider er den samme afbildning $X \to X$, altså at de antager samme værdi i ethvert element $x \in X$. Sæt $y := \mu^{-1}(x)$. Antag først, at x ikke er et af elementerne $\mu(x_i)$. Højresidens værdi i x er da x. Videre er y ikke et af elementerne x_i, så venstresidens værdi er $\mu\gamma(y) = \mu(y) = x$. Antag dernæst, at $x = \mu(x_i)$. Højresidens værdi er da $\mu(x_{i+1})$ (hvor indices regnes modulo p). Videre er $y = x_i$, så venstresidens værdi er $\mu\gamma x_i = \mu(x_{i+1})$. I begge tilfælde har ligningens to sider altså samme værdi i x.

Antag nu, at to permutationer σ og σ' af X er konjugerede, altså at $\sigma' = \mu\sigma\mu^{-1}$ med en permutation μ. Ifølge cykelsætningen har vi en fremstilling af σ som produkt af disjunkte cykler,

$$\sigma = \cdots (x_1 \ \ldots \ x_p) \cdots , \tag{7.18.2}$$

svarende til banerne for permutationen σ. I fremstillingen medtager vi en 1-cykel for hvert fixpunkt for σ. Typen af σ er følgen $m_1, m_2, \ldots$, hvor m_p er antallet af p-cykler, der indgår i fremstillingen. Da konjugering er en gruppehomomorfi, får vi af (7.18.1) for den konjugerede permutation fremstillingen som et produkt af cykler,

$$\sigma' = \cdots (x'_1 \ \ldots \ x'_p) \cdots , \tag{7.18.3}$$

hvor $x'_i := \mu(x_i)$. Øjensynlig er (7.18.3) fremstillingen af σ' som produkt af disjunkte cykler. Da antallet af p-cykler i de to fremstillinger er det samme, har σ og σ' samme type.

Antag omvendt, at σ og σ' har samme type. Vi har fremstillinger (7.18.2) og (7.18.3), og her ordner vi i begge fremstillinger faktorerne således, at vi først skriver 1-cyklerne, dernæst 2-cyklerne osv. Da de to permutationer har samme type, står der nu i begge fremstillinger en p-cykel under en p-cykel. I den øverste fremstilling står alle elementer i X i en bestemt rækkefølge på højresiden, og de samme elementer står i en bestemt rækkefølge på højresiden af den nederste fremstilling. Vi kan derfor bestemme en permutation μ af X ved for $x \in X$ at opsøge placeringen af x i den øverste fremstilling og så definere $\mu(x)$ som det element, der står under x i den nederste fremstilling. Med permutationen μ har vi ifølge den viste udregning, at $\sigma' = \mu\sigma\mu^{-1}$.

Hermed er resultatet bevist. □

(7.19) Eksempel. Betragt de to permutationer i S_4,

$$\sigma = (1\,2)(3\,4),$$
$$\sigma' = (1\,3)(2\,4).$$

De er begge et produkt af to disjunkte transpositioner, altså begge af type 2^2, og de er derfor konjugerede. Det fremgår af beviset for (7.18), at en permutation μ, der konjugerer σ over i σ', er bestemt ved $1 \mapsto 1$, $2 \mapsto 3$, $3 \mapsto 2$, og $4 \mapsto 4$, altså som transpositionen $\mu = (2\,3)$. Der er naturligvis andre valg af μ. I fremstillingen af σ' kan vi jo ombytte 1 og 3 og ombytte 2 og 4, og vi kan ombytte transpositionerne $(1\,3)$ og $(2\,4)$.

Som nævnt i Eksempel (2.17) er der 5 typer permutationer i S_4, og altså 5 konjugeretklasser.

(7.20) Tælleformlen. *Lad der være givet en virkning af gruppen G på mængden X. Da gælder formlen,*

$$|X| = |X^G| + \sum_j |G : G_{x_j}| , \tag{7.20.1}$$

hvor $|X^G|$ *er antallet af fixpunkter for virkningen, og hvor der i summationen er valgt ét element* x_j *fra hver bane, der ikke er en et-punkts-bane.*

Bevis. Da banerne udgør en klassedeling af X, kan elementantallet $|X|$ bestemmes som summen af banernes længder. Et-punkts-banerne svarer til elementerne $x \in X^G$; de bidrager hver med et 1-tal, altså i alt med antallet $|X^G|$. I hver bane B_j, som ikke er en et-punkts-bane, vælges et element x_j. Ifølge Baneformlen (7.15) har vi da $|B_j| = |G : G_{x_j}|$. Bidraget fra banerne B_j er altså summen på højresiden af (7.20.1). Hermed er formlen bevist. □

(7.21) Observation. Det er en pointe i Tælleformlen, for en endelig gruppe G der virker på en endelig mængde X, at leddene i summen på højresiden er divisorer i $|G|$ og større end 1. Antag for eksempel, at G er en *p-gruppe*, dvs en gruppe, hvis orden er en potens p^r af et *primtal* p. En divisor større end 1 i p^r har formen p^s med $s \geqslant 1$; specielt er en sådan divisor delelig med p. I summen i (7.20.1) er alle leddene altså delelige med p, og vi får kongruensen,

$$|X| \equiv |X^G| \pmod{p}. \tag{7.21.1}$$

Specielt ses, at hvis p ikke går op i elementantallet $|X|$, så findes der fixpunkter for virkningen. Hvis der findes fixpunkter og p går op i $|X|$, så findes der mindst p fixpunkter.

(7.22) Klasseformlen. *For enhver gruppe* G *gælder formlen,*

$$|G| = |\mathrm{Cent}(G)| + \sum_j |G : C(x_j)|,$$

hvor der i summationen er valgt ét element x_j *fra hver konjugeretklasse uden for centret.*

Bevis. Klasseformlen er blot tælleformlen anvendt på virkningen af G på sig selv givet ved konjugering. □

(7.23) Sætning. *Enhver ikke-triviel* p*-gruppe har et ikke-trivielt centrum.*

Bevis. Centret $\mathrm{Cent}(G)$ er en undergruppe af G, og som i (7.21) følger det af Klasseformlen, at $|\mathrm{Cent}(G)| \equiv |G| \equiv 0 \pmod{p}$. Det er specielt udelukket, at $|\mathrm{Cent}(G)| = 1$. Altså er $\mathrm{Cent}(G)$ ikke den trivielle undergruppe $\{1\}$. □

(7.24) Korollar. *I enhver gruppe* G *af orden* p^n*, hvor* p *er et primtal, findes en kæde af normale undergrupper,*

$$\{1\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n = G,$$

hvor G_i *har orden* p^i.

Bevis. Påstanden vises ved induktion efter n. Den er triviel for $n = 1$. Antag, at $n > 1$ og at påstanden gælder for $n - 1$. Ifølge (7.23) findes et element $h \neq 1$ i centret for G. Da G er en p-gruppe, har h en orden, der er en potens p^ν. Ved at erstatte h med $h^{p^{\nu-1}}$ kan vi antage, at h har orden p. Den cykliske undergruppe $G_1 := \langle h \rangle$ har derfor orden p. Enhver potens h^i ligger i centret, og kommuterer derfor med et vilkårligt element $g \in G$. Altså er

$gh^ig^{-1} = h^i \in G_1$. Heraf følger, at G_1 er en normal undergruppe af G. Da G_1 har orden p, har kvotientgruppen $\overline{G} := G/G_1$ orden $p^n/p = p^{n-1}$. Induktivt findes altså i $\overline{G}$ en kæde af normale undergrupper,

$$\{\bar{1}\} = \overline{G}_0 \subset \overline{G}_1 \subset \cdots \subset \overline{G}_{n-1} = \overline{G},$$

hvor $\overline{G}_i$ har orden p^i. Lad $\kappa\colon G \to \overline{G}$ være den kanoniske homomorfi, og betragt originalmængden $G_i := \kappa^{-1}(\overline{G}_{i-1})$ for $i = 1, \dots, n$. Øjensynlig er $G_{i-1} \subseteq G_i$. Det følger af Noether's anden Isomorfisætning, at G_i er normal i G, af index lig med $|\overline{G}{:}\overline{G}_{i-1}| = p^{n-1}/p^{i-1} = p^{n-i}$. Altså har G_i orden p^i, som ønsket. □

(7.25) Eksempel. Lad p være et primtal. Enhver gruppe G af orden p^2 er da abelsk. Der findes nemlig et element $g \neq 1$ i centret for G. Hvis g har orden p^2, er $G = \langle g \rangle$ cyklisk, og dermed abelsk. Antag derfor, at g har orden p. Vælg et element $h \notin \langle g \rangle$. Da g kommuterer med alle elementer i G, er undergruppen $\langle g \rangle$ specielt normal. Følgelig er $\langle h \rangle \langle g \rangle$ en gruppe. Den indeholder $\langle g \rangle$, og også elementet h, som var valgt uden for $\langle g \rangle$. Da $|G| = p^2$, må vi have $\langle h \rangle \langle g \rangle = G$. Gruppen G består derfor af alle produkter $h^i g^j$. Vilkårlige to sådanne produkter kommuterer, fordi g og h kommuterer. Altså er G abelsk.

Det følger af Struktursætningen, og faktisk også let af overvejelserne ovenfor, at G er isomorf med enten C_{p^2} eller med $\mathrm{C}_p \times \mathrm{C}_p$.

(7.26) Burnside's Formel. *Lad der være givet en virkning af en endelig gruppe G på mængden X. Antallet af baner, altså tallet $|X/G|$, er da bestemt ved formlen,*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|, \tag{7.26.1}$$

hvor $X^g = \{x \in X \mid g.x = x\}$.

Bevis. Lad $R \subseteq G \times X$ betegne delmængden,

$$R := \{(g, x) \mid g.x = x\}.$$

Vi viser formlen ved at tælle antallet af elementer i R på to måder.

Mængden R er en delmængde af produktmængden $G \times X$. Vi har derfor to projektioner, $p\colon R \to G$ og $q\colon R \to X$, bestemt ved $p(g, x) = g$ og $q(g, x) = x$. Hvert element af R ligger i præcis én originalmængde $p^{-1}(g)$ for $g \in G$. Elementantallet $|R|$ kan derfor bestemmes som summen, over $g \in G$, af elementantallene $|p^{-1}(g)|$. Tilsvarende kan $|R|$ bestemmes ud fra afbildningen q. Vi har derfor ligningerne,

$$\sum_{g \in G} |p^{-1}(g)| = |R| = \sum_{x \in X} |q^{-1}(x)|.$$

For et givet element $g \in G$ består $p^{-1}(g)$ af alle par (g, x), for hvilke $g.x = x$. Sådanne par, med et givet g, svarer til de elementer $x \in X$, for hvilke $g.x = x$, altså til elementerne i X^g. Vi har derfor ligningen,

$$|R| = \sum_{g \in G} |X^g|. \tag{7.26.2}$$

For et givet element $x \in X$ består $q^{-1}(x)$ af alle par (g, x) således, at $g.x = x$. Sådanne par, med et givet x, svarer til de elementer $g \in G$, for hvilke $g.x = x$, altså til elementerne i isotropigruppen G_x. Vi har derfor ligningen,

$$|R| = \sum_{x \in X} |G_x|. \tag{7.26.3}$$

Banerne for virkningen udgør en klassedeling af X. Vi kan derfor opnå summen i (7.26.3) ved først for hver bane B at beregne delsummen af leddene $|G_x|$ hørende til elementer $x \in B$, og dernæst addere delsummerne. Betragt en bane B og leddet $|G_x|$ hørende til et element $x \in B$. Vi har da ligningerne,

$$|G_x| = \frac{|G|}{|G : G_x|} = \frac{|G|}{|B|},$$

thi den første følger af Lagrange's Indexsætning (4.2), og den anden af Baneformlen (7.15). Heraf ses, at leddene $|G_x|$ for $x \in B$ alle er ens, og lig med $|G|/|B|$. Da antallet af led, svarende til $x \in B$, er lig med $|B|$, slutter vi, at delsummen af led $|G_x|$ for $x \in B$ er lig med $|G|$. Leddene i (7.26.3) svarende til elementer x i en given bane bidrager altså med tallet $|G|$ til summen. Antallet af baner er $|X/G|$. Altså får vi af (7.26.3) ligningen,

$$|R| = |X/G| \cdot |G|. \tag{7.26.4}$$

Burnside's formel følger af (7.26.2) og (7.26.4) efter division med $|G|$. □

(7.27) Bemærkning. I Burnside's formel er funktionen $g \mapsto |X^g|$ konstant på hver konjugeretklasse. Er nemlig to elementer $g, g' \in G$ konjugerede, så er $g' = hgh^{-1}$ med $h \in G$, og det er nemt at se, at afbildningen $x \mapsto h.x$ definerer en bijektiv afbildning $X^g \xrightarrow{\sim} X^{g'}$.

Ved beregningen af summen $\sum_{g \in G} |X^g|$ er det derfor ofte naturligt at inddrage delingen af G i konjugeretklasser. Er disse klasser bestemt, kan vi for hver konjugeretklasse K betragte delsummen $\sum_{g \in K} |X^g|$. Vælges et element $g_1 \in K$, er leddene i delsummen alle lig med $|X^{g_1}|$ og antallet af led er $|K| = |G{:}C(g_1)| = |G|/|C(g_1)|$. Delsummen $\sum_{g \in K} |X^g|$ er altså lig med $|G| \cdot |X^{g_1}|/|C(g_1)|$, hvor g_1 er et element i konjugeretklassen K. Indsættelse i Burnside's Formel giver derfor ligningen,

$$|X/G| = \sum_i \frac{|X^{g_i}|}{|C(g_i)|}, \tag{7.27.1}$$

hvor der i summen er valgt ét element g_i fra hver konjugeretklasse i G.

(7.28) Polya's Formel. *Antag, at gruppen G er endelig og virker på den endelige mængde X. Lad F være en vilkårlig endelig mængde, og betragt virkningen af G på mængden $\mathcal{F} := F^X$ af afbildninger $\eta \colon X \to F$. Da gælder formlen,*

$$|\mathcal{F}/G| = \frac{1}{|G|} \sum_{g \in G} |F|^{m(g_X)}, \tag{7.28.1}$$

hvor $m(g_X)$ er antallet af baner for den til g svarende permutation $g_X = \rho_g$ af X.

Bevis. Virkningen af G på mængden $\mathcal{F} = F^X$ af afbildninger er beskrevet i (7.8). For at bevise formlen er det nok at vise, for hvert element $g \in G$, at

$$|\mathcal{F}^g| = |F|^{m(g_X)}, \tag{7.28.2}$$

thi så følger (7.28.1) umiddelbart af Burnside's Formel (7.26.1), med $X := \mathcal{F}$.

Mængden $\mathcal{F}^g$ består af de afbildninger $\eta\colon X \to F$, som er fixpunkter for g, dvs opfylder $g.\eta = \eta$ eller, ækvivalent, at $\eta(g^{-1}.x) = \eta(x)$ for alle x.

Hvis $\eta(g^{-1}.x) = \eta(x)$ for alle x, så får vi, ved at sætte $x := g^i.x$ for $i = 1, 2, \dots,$ ligningerne,

$$\eta(x) = \eta(g.x) = \eta(g^2.x) = \cdots .$$

Omvendt følger af den første af disse ligninger, for $x := g^{-1}.x$, at $\eta(g^{-1}.x) = \eta(x)$. Afbildningen $\eta\colon X \to F$ tilhører altså $\mathcal{F}^g$, hvis og kun hvis ligningerne er opfyldt for alle $x \in X$. Elementet $g^i.x$ er billedet $g_X^i(x)$ ved potensen af permutationen g_X, så elementerne $g^i.x$ udgør banen gennem x for permutationen g_X. Altså er $\eta \in \mathcal{F}^g$, hvis og kun hvis afbildningen η er konstant på hver bane for permutationen g_X. Der er $m(g_X)$ baner, og for hver bane er der $|F|$ muligheder for værdien af η. Antallet af afbildninger $\eta\colon X \to F$, der er konstante på hver bane for g_X, er derfor $|F|^{m(g_X)}$.

Hermed er formlen bevist. □

(7.29) Mønstre. Polya's Formel tæller mønstre i følgende forstand: Mængden X opfattes som en mængde af pladser eller felter, og F opfattes som en mængde af farver. En afbildning $\eta\colon X \to F$ knytter til hvert felt x en farve $\eta(x)$. Afbildninger $\eta\colon X \to F$ kan altså opfattes som *farvelægninger* af X: værdien $\eta(x)$ fortæller, hvilken farve der er lagt på feltet x. Når gruppen G virker på X, vil permutationerne g_X, for $g \in G$, typisk være interessante symmetrier af felterne. Farvelægningen $g.\eta$ fremkommer af farvelægningen η ved at flytte farven $\eta(x)$ på feltet x hen på feltet $g.x$. Ækvivalensklasser af farvelægninger kaldes også *mønstre*. Polya's Formel er altså en formel for antallet af mønstre.

(7.30) Eksempel. Hvor mange forskellige mønstre kan der males på en terning, når hver af terningens 6 sider kan males med en af N mulige farver? Her består mængden X af felter af terningens 6 sider, og mængden F af farver har N elementer. Terningen kan altså farvelægges på N^6 måder. Dette antal er naturligvis korrekt, men om det er svaret på spørgsmålet afhænger af hvad vi lægger i, at der spørges om *forskellige* mønstre. Det er naturligt at opfatte to farvelægninger som ens, hvis den ene fremgår af den anden ved en drejning af terningen. Efter denne opfattelse skal vi altså bestemme antallet af mønstre under virkningen af hexaedergruppen H på terningen. Hexaedergruppen består af 24 drejninger. De kan deles i 5 klasser bestående af identiteten, af 6 stk $\frac{1}{2}$-drejninger om en kantakse, af 8 stk $\frac{1}{3}$-drejninger om en hjørneakse, af 3 stk $\frac{1}{2}$-drejninger om en sideakse, og af yderligere 6 stk $\frac{1}{4}$-drejninger om en sideakse. Hexaedergruppen virker på mængden X bestående af de 6 sider, og dermed på farvelægningerne. I tabellen herunder har vi for hver klasse af drejninger g i H anført antallet af drejninger i klassen, og typen af den tilhørende permutation g_X. Tallet i den sidste søjle er gruppens orden, 24, delt med antallet af drejninger i klassen. Det er velkendt, at klasserne netop er konjugeretklasserne i H, så tallene i sidste søjle er faktisk ordenen af centralisatoren.

Drejning g	antal	cykelbillede	type	$m(g_X)$	$\|C(g)\|$
identiteten	1	$(*)(*)(*)(*)(*)(*)$	1^6	6	24
$\frac{1}{2}$-drejning om kant	6	$(**)(**)(**)$	2^3	3	4
$\frac{1}{3}$-drejning om hjørne	8	$(***)(***)$	3^2	2	3
$\frac{1}{2}$-drejning om side	3	$(*)(*)(**)(**)$	$1^2 2^2$	4	8
$\frac{1}{4}$-drejning om side	6	$(*)(*)(****)$	$1^2 4^1$	3	4

Indsættelse i Polya's Formel giver nu for antallet af forskellige mønstre udtrykket,

$$\frac{1}{24}\big(N^6+6N^3+8N^2+3N^4+6N^3\big)=\frac{N^6}{24}+\frac{N^3}{4}+\frac{N^2}{3}+\frac{N^4}{8}+\frac{N^3}{4}.$$

Det er naturligvis smart at checke, at udtrykket for $N=1$ giver værdien 1.

(7.31) Opgaver.

1. Diedergruppen $G := \mathrm{D}_n$ virker på planen $\mathbb{R}^2$, og specielt på delmængden X bestående af de n hjørner $p_1, \dots, p_n$ i n-kanten, jfr (1.21). Vis, at de n hjørner udgør én bane. Bestem isotropigruppen for hvert af hjørnerne. Bestem de vektorer v i planen, for hvilke isotropigruppen G_v har orden 1.

2. Den specielle ortogonale gruppe $\mathrm{O}^+(3)$ virker på rummet $\mathbb{R}^3$. Beskriv banerne og isotropigrupperne.

3. Den symmetriske gruppe S_n virker på mængden $\{1, \dots, n\}$. Talrummet $\mathbb{R}^n$ kan opfattes som mængden af afbildninger $\{1, \dots, n\} \to \mathbb{R}$, og følgelig virker S_n på talrummet $\mathbb{R}^n$. Angiv vektoren $\gamma.(a, b, c, d)$, når γ er 3-cyklen $(2\,3\,4)$. Hvilke vektorer i $\mathbb{R}^4$ er invariante under dobbelttranspositionen $(1\,3)(2\,4)$? Hvilke vektorer i $\mathbb{R}^n$ er invariante under n-cyklen $(1\;2\;\dots\;n)$ og hvilke er invariante under virkningen af S_n?

4. Betragt vektoren $(0, 0, 0, 0, 1, 1)$ i $\mathbb{R}^6$. Beskriv, for virkningen af S_6 på $\mathbb{R}^6$, isotropigruppen for vektoren og banen gennem vektoren.

5. Den cykliske gruppe C_n virker på de n hjørner i en regulær n-kant, og dermed også på mængden af delmængder af hjørnerne. Specielt virker C_n på mængden $\mathcal{X}$ bestående af alle delmængder med k hjørner, hvor $k \geqslant 1$ er givet. Antag, at k er primisk med n. Vis, at isotropigruppen for hvert element $K \in \mathcal{X}$ er den trivielle undergruppe $\{1\}$ af C_n. Slut heraf, at binomialkoefficienten $\binom{n}{k}$ er delelig med n. (Det er nu også ret let at vise direkte.)

6. En virkning af gruppen G på X kaldes *fixpunktsfri*, hvis gruppeelementet $1 \in G$ er det eneste, der har fixpunkter. Vis, at virkningen af G på sig selv ved translation er fixpunktsfri. Kan den symmetriske gruppe S_4 virke fixpunktsfrit på en mængde med 36 elementer?

7. Antag, at G er en gruppe af orden n, og at $g \in G$ har orden d. Afbildningen $\rho_g : x \mapsto gx$ er en permutation af G. Vis, at ρ_g er et produkt af n/d disjunkte cykler af orden d. Permutationen ρ_g er i øvrigt billedet af g ved repræsentationen $G \to \mathrm{Perm}(G)$ bestemt ved translation.

8. Lad G være en endelig gruppe af orden n. For $g \in G$ sættes $\chi(g) := (-1)^{(d-1)n/d}$, hvor d er ordenen af g. Vis, at $\chi\colon G \to \{\pm 1\}$ er en homomorfi. Vis, at en gruppe af orden $2u$, hvor u er ulige, har en undergruppe af index 2.

9. En virkning af gruppen G på mængden X kaldes *transitiv*, hvis der kun er én bane, altså hvis der for alle x', x i X findes et gruppeelement g således, at $x' = g.x$. Vis, at når en kommutativ gruppe virker transitivt, så har hvert element $g \in G$ enten alle elementer eller ingen elementer i X som fixpunkter.

10. Bestem centralisatoren for transpositionen $(1\,2)$ i S_4.

11. I en *partition* $n = \lambda_1 + \cdots + \lambda_k$, hvor $\lambda_i \in \mathbb{N}$, skelner man ikke rækkefølgen af leddene, og partitionen kan enten angives ved følgen af addender *altid ordnet aftagende*, $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_k > 0$, eller ved *typen* $1^{m_1}2^{m_2}3^{m_3}\cdots$, hvor m_1 er antallet af 1-taller blandt λ_i'erne, m_2 er antallet af 2-taller osv. Fx kan partitionen $18 = 1+1+3+3+3+3+4$ angives som $(4, 3, 3, 3, 3, 1, 1)$ eller som $1^2 3^4 4^1$ (det er et „formelt“ produkt, som *ikke* skal regnes ud).

For en klassedeling af en mængde X med n elementer i k klasser udgør klassernes elementantal en partition $(\lambda_1, \dots, \lambda_k)$, som kaldes klassedelingens *type*. Bemærk, at antallet af klassedelinger af en given type $(\lambda_1, \dots, \lambda_k)$ *ikke* er givet ved multinomialkoefficienten,

$$\binom{n}{\lambda_1, \dots, \lambda_k} = \frac{n!}{\lambda_1! \cdots \lambda_k!}.$$

Multinomialkoefficienten ovenfor angiver nemlig antallet af opdelinger af X i *nummerede* delmængder $X_1, \dots, X_k$ med $|X_i| = \lambda_i$; hvis vi, som her, antager at $\lambda_i \geqslant 1$ for alle i, så fås de nummerede opdelinger blot ved at nummerere klasserne i en klassedeling (under kravet $|X_i| = \lambda_i$). Slut heraf, at det søgte antal klassedelinger af en given type $(\lambda_1, \dots, \lambda_k)$ er bestemt at dividere multinomialkoefficienten med $m_1!m_2!\cdots$. Vis herved: Antallet af klassedelinger af den givne type $(\lambda_1, \lambda_2, \dots, \lambda_k)$ er bestemt som tallet

$$\frac{n!}{m_1!m_2!\cdots\lambda_1!\cdots\lambda_k!} = \frac{n!}{m_1!m_2!\cdots(1!)^{m_1}(2!)^{m_2}\cdots},$$

og antallet af permutationer i S_n af denne type er bestemt som tallet

$$\frac{n!}{m_1!m_2!\cdots\lambda_1\cdots\lambda_k} = \frac{n!}{m_1!m_2!\cdots 1^{m_1}2^{m_2}\cdots}.$$

Hvor mange permutationer kommuterer med en permutation af den givne type?

12. Vis, at to permutationer i A_n af samme cykeltype ikke nødvendigvis er konjugerede i gruppen A_n.

13. Beskriv konjugeretklasserne i planens flytningsgruppe $\mathrm{O}(2)$.

14. Beskriv konjugeretklasserne i diedergruppen D_4 og i kvaterniongruppen Q_8.

15. Bestem centrum i hver af grupperne D_4, D_5 og Q_8.

16. En perlekæde har k perler. Overvej, at perlekædens symmetrigruppe er diedergruppen D_k. Hvor mange perlekæder kan der laves med 6 perler, når der er perler af N farver at vælge imellem? Vis, at med 6 perler af 2 farver kan der laves 13 forskellige kæder. På hvor mange forskellige måder kan man smykke en hals med en af disse kæder?

17. Bestem antallet af perlekæder med 8 perler, som indeholder 4 hvide og 4 røde perler.

18. På hvor mange måder kan man nummerere en ternings seks sider? Hvor mange af disse nummereringer opfylder, at numrene på modstående sider altid har summen 7?

19. Vis, at der ved ${}^{S}A := SAS^{-1}$ defineres en virkning af gruppen $G := \mathrm{GL}_n(\mathbb{R})$ på mængden $X := \mathrm{Mat}_n(\mathbb{R})$. Matricer, der er ækvivalente under denne virkning, kaldes *regulær-ækvivalente* eller *similære*. Lad $f\colon V \to V$ være en lineær afbildning af et n-dimensionalt vektorrum ind i sig selv. Vis, at matricerne, der beskriver f mht de forskellige baser for V, udgør én bane.

20. Vis, at der ved ${}^{S}A := SAS^{\mathrm{t}}$ defineres en virkning af gruppen $G := \mathrm{GL}_n(\mathbb{R})$ på mængden $X := \mathrm{Mat}_n(\mathbb{R})$. Vis, at delmængden $Y \subseteq \mathrm{Mat}_n(\mathbb{R})$ bestående af alle symmetriske matricer er invariant under virkningen.

21. Vis for et primtal p, at gruppen $\mathrm{UT}_3(\mathbb{Z}/p)$ af uni-triangulære 3×3-matricer (1 i diagonalen og 0 under) med koefficienter i $\mathbb{Z}/p$ har orden p^3. Bestem i gruppen normale undergrupper af ordener p og p^2. Vis, at $\mathrm{UT}_3(\mathbb{Z}/2)$ er diedergruppen D_4. Vis, når $p > 2$, at alle matricer (på nær 1) i $\mathrm{UT}_3(\mathbb{Z}/p)$ har orden p.

22. For en undergruppe H af en endelig gruppe G virker G ved translation på mængden $X = G/H$ af sideklasser. Bestem isotropigruppen for en given sideklasse xH. Bestem kernen for den tilhørende repræsentation $G \to \mathrm{Perm}(G/H)$. Vis, at kernen er den største undergruppe af H, som er normal i G.

23. Antag, at p er den mindste primdivisor i ordenen af G, og at H er en undergruppe af index p. Vis, at H er normal.

24. Til en julefrokost deltager 20 personer, som sidder ligeligt fordelt omkring et rundt bord. Hver person har medbragt en pakke og lægger den på bordet foran sig. Under den obligatoriske pakkeleg permuteres pakkerne. Efter pakkelegen er der imidlertid 2 personer, der har fået deres egen pakke.

a. Vis, at man kan dreje bordet således, at ingen får sin egen pakke.
b. *Samme opgave i tilfældet, hvor kun 1 person har fået sin egen pakke.
c. *Gælder det samme, hvis der er 25 deltagere?

25. Lad $U_1, \dots, U_k$ være delmængder af en fast endelig mængde U. Sæt

$$N_r := \sum_{\{i_1,\dots,i_r\}} |U_{i_1} \cap \cdots \cap U_{i_r}|;$$

summen er over alle delmængder med r elementer af indices. Leddet svarende til $i_1, \dots, i_r$ er antallet af elementer $u \in U$, som ligger i alle de r delmængder $U_{i_1}, \dots, U_{i_r}$ (og måske i flere af delmængderne U_i). For $r = 0$ er det den tomme delmængde af indices, og fællesmængden på højresiden fortolkes som hele U, altså $N_0 = |U|$.

Lad E_t betegne antallet af elementer $u \in U$, som opfylder $u \in U_i$ for præcis t værdier af i. Specielt er så $N_k = E_k = |U_1 \cap \cdots \cap U_k|$, og

$$N_0 = |U|, \quad E_0 = |U \setminus (U_1 \cup \cdots \cup U_k)|, \text{ og } N_0 - E_0 = |U_1 \cup \cdots \cup U_k|.$$

Vis, for $r = 0, \dots, k$, at

$$N_r = \sum_{r \leqslant t \leqslant k} \binom{t}{r} E_t; \text{ specielt } N_0 = E_0 + \cdots + E_k.$$

Vis, at disse ligninger kan udtrykkes som en enkelt ligning mellem polynomierne $N(x) := \sum N_r x^r$ og $E(x) := \sum_r E_r x^r$, nemlig $N(x) = E(x+1)$. Slut heraf, at $E(x) = N(x-1)$, og dermed, at

$$E_r = \sum_{r \leqslant t \leqslant k} (-1)^{t-r} \binom{t}{r} N_t.$$

Ligningerne udtrykker princippet om *tælling ved inklusion–eksklusion*. Specielt er

$$E_0 = N_0 - N_1 + \cdots + (-1)^k N_k \quad \text{og} \quad N_0 - E_0 = N_1 - N_2 + \cdots + (-1)^{k-1} N_k.$$

26. En farvelægning af $\{1, \dots, n\}$, med farver fra en ordnet mængde F med k farver, er et n-sæt $(f_1, \dots, f_n)$ med $f_i \in F$. Lad U være mængden af farvelægninger og lad U_i være delmængden af farvelægninger, som *ikke* bruger den i'te farve. Vis, med standardbetegnelser for inklusion-eksklusion, at for $0 \leqslant r \leqslant k$ er

$$N_{k-r} = \binom{k}{r} r^n, \quad E_{k-r} = \left\{ {n \atop r} \right\} k^{\underline{r}} .$$

hvor $\left\{ {n \atop r} \right\}$ er antallet af klassedelinger af en mængde med n elementer i r klasser (*Stirling-tallene af anden art*), og $k^{\underline{r}} := k(k-1)\cdots(k-r+1)$. Udled formlerne:

$$k^n = \sum\nolimits_{r=0}^{k} \left\{ {n \atop r} \right\} k^{\underline{r}}, \qquad \left\{ {n \atop k} \right\} = \frac{1}{k!} \sum\nolimits_{r=0}^{k} (-1)^{k-r} \binom{k}{r} r^n.$$

Hvilken ligning mellem polynomier udledes af den første formel? [Vink: højresiden ændres ikke, hvis man erstatter $\sum_{r=0}^{k}$ med $\sum_{r=0}^{n}$.]

27. Den symmetriske gruppe S_n virker på farvelægninger $(f_1, \dots, f_n)$ med farver fra en mængde med k farver ved at permutere koordinaterne. Banerne svarer til k-sæt af antal, $(a_1, \dots, a_k)$, hvor a_j er antallet af koordinater af den j'te farve. Vis, at Polya's formel er følgende formel:

$$\binom{n+k-1}{n} = \frac{1}{n!} \sum\nolimits_{r=0}^{n} \left[{n \atop r} \right] k^r,$$

hvor $\left[{n \atop r} \right]$ er antallet af permutationer i S_n med r baner (*Stirling-tallene af første art*). Hvilken ligning mellem polynomier udledes af formlen?

[Vink: Begge formlens sider kræver en overvejelse. Venstresiden er antallet af heltalsløsninger til ligningen $a_1 + \cdots + a_k = n$ med $a_j \geqslant 0$.]

28. Bestem antallet af fixpunktfri permutationer i S_k.

[Vink: Sæt, med standardbetegnelser for inklusion-eksklusion, $U := \mathrm{S}_k$ og lad U_i, for $i = 1, \dots, k$, være delmængden af U bestående af de permutationer, der har i som fixpunkt. Tallet E_0 er så antallet af fixpunktfri permutationer. Vis, at $N_r = \binom{k}{r}(k-r)!$, og brug formlen $E_0 = \sum_i (-1)^r N_r$.]

8. Sylow's sætninger.

(8.1) Indledning. Lad G være en fast (multiplikativt skrevet) endelig gruppe. For en undergruppe H af G følger det af Lagrange's Sætning, at H's orden er divisor i $|G|$. Omvendt gælder det ikke i almindelighed, jfr Eksempel (4.18), at der for hver divisor d i $|G|$ findes en undergruppe af G af orden d. Det er et fundamentalt resultat, at hvis divisoren d i $|G|$ er en primtalspotens, så eksisterer der en undergruppe af orden d af G.

For hvert primtal p, der går op i ordenen $|G|$, findes altså specielt en undergruppe af orden p, eller, ækvivalent, der findes i G et element af orden p. Mere interessant er det faktisk, at der i G findes undergrupper, hvis orden er den største potens af p, som går op i $|G|$. I dette kapitel viser vi eksistensen af disse undergrupper, der kaldes *Sylow-undergrupper*. De spiller en stor rolle i klassifikationen af endelige grupper, og vi giver en række anvendelser.

(8.2) Definition. Lad p være en primdivisor i $|G|$, og skriv $|G| = n_0 p^\nu$, hvor p ikke går op i n_0. En undergruppe S af G af orden p^ν kaldes da en *Sylow-p-undergruppe*. Potensen p^ν er den største potens af p, der går op i $|G|$. Sylow-p-undergrupperne er altså undergrupper, der er p-grupper af denne størst mulige orden.

For hvert element $g \in G$ er konjugering med g, dvs afbildningen $x \mapsto gxg^{-1}$, som bekendt en bijektiv homomorfi af gruppen G på sig selv. Heraf ses, at for enhver undergruppe H af G er også gHg^{-1} en undergruppe, og af samme orden som H; undergruppen gHg^{-1} er *konjugeret* med H. Når S er en Sylow-p-undergruppe, så er altså også enhver konjugeret undergruppe gSg^{-1} en Sylow-p-undergruppe.

(8.3) Eksempel. Lad G være en kommutativ gruppe af orden n, og lad $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ være primopløsningen af n. For hvert i har vi i (6.6) betragtet undergruppen $G(p_i)$ bestående af elementer g, hvis orden er en potens af p_i, og vi har vist, at G er det direkte produkt af undergrupperne $G(p_i)$. Som bemærket i (6.11) har $G(p_i)$ orden $p_i^{\nu_i}$, så $G(p_i)$ er en Sylow-p_i-undergruppe. Hvis en undergruppe $H \neq \{e\}$ er en p-undergruppe, må p være et af primtallene p_i. Yderligere har hvert element i H en orden, som er en potens af p_i, så det følger, at $H \subseteq G(p_i)$. Specielt følger det, at $H = G(p_i)$, hvis H er en Sylow-p_i-undergruppe. Undergrupperne $G(p_i)$ er altså samtlige Sylow-undergrupper i G.

(8.4) Eksempel. Betragt diedergruppen D_7. Den består af de 7 potenser af drejningen med vinklen $2\pi/7$ og af 7 spejlinger. Dens orden er $14 = 2 \cdot 7$. Sylow-undergrupperne er altså undergrupperne af orden 2 og 7. Drejningen frembringer en cyklisk undergruppe af orden 7, og den er altså Sylow-7-undergruppen. Hver af de 7 spejlinger frembringer en Sylow-2-undergruppe. Der er altså 7 Sylow-2-undergrupper.

Betragt i stedet diedergruppen D_6, af orden $12 = 2^2 \cdot 3$. Den består af de 6 potenser af drejningen δ med vinklen $2\pi/6$ og 6 spejlinger. Sylow-2-undergrupperne er undergrupperne af orden 4 og Sylow-3-undergrupperne er undergrupperne af orden 3. Flytningerne af orden 3 er δ^2 og δ^4, så der er én Sylow-3-undergruppe, nemlig den cykliske undergruppe $\langle\delta^2\rangle$. Potensen $\varepsilon := \delta^3$ er halvdrejningen (multiplikation med -1); den har orden 2, og den kommuterer med alle elementer. Det følger, at for enhver spejling σ udgør de 4 flytninger $\mathrm{id}, \varepsilon, \sigma, \varepsilon\sigma$ en undergruppe af D_6, altså en Sylow-2-undergruppe. Flytningen $\varepsilon\sigma$ er selv en spejling, nemlig spejlingen i aksen vinkelret på aksen for σ. Der er således 3 Sylow-2-undergrupper af formen $\{\mathrm{id}, \varepsilon, \sigma, \varepsilon\sigma\}$. Det er ikke svært at vise, at de er samtlige Sylow-2-undergrupper.

(8.5) Eksempel. Den symmetriske gruppe S_4 har orden $24 = 2^3 \cdot 3$. Sylow-undergrupperne er altså undergrupperne af orden 8 og af orden 3. Diedergruppen D_4 af orden 8 kan opfattes som undergruppe i S_4, jfr Eksempel (7.10). Den er altså en Sylow-2-undergruppe i S_4. Det er klart, at undergruppen frembragt af en 3-cykel er en Sylow-3-undergruppe.

Den alternerende gruppe A_5 har orden $60 = 2^2{\cdot}3{\cdot}5$. Sylow-2-undergrupper er altså af orden 4, Sylow-3-undergrupper er af orden 3 og Sylow-5-undergrupper af orden 5. Fx er undergruppen bestående af identiteten og de tre dobbelttranspositioner på 4 af tallene $1, 2, 3, 4, 5$ en Sylow-2-undergruppe, undergruppen frembragt af en 3-cykel er en Sylow-3-undergruppe, og undergruppen frembragt af en 5-cykel er en Sylow-5-undergruppe. Det er ikke svært at vise, at de beskrevne undergrupper er samtlige Sylow-undergrupper i A_5.

(8.6) Lemma. *Lad n_0 være et naturligt tal, og lad p være et primtal. Da gælder kongruensen,*

$$\binom{n_0 p^\nu}{p^\nu} \equiv n_0 \pmod{p}. \tag{8.6.1}$$

Bevis. Lad N være binomialkoefficienten, og sæt $k := p^\nu - 1$. Da har vi ligningen,

$$N = \binom{n_0 p^\nu}{p^\nu} = \prod_{i=0}^{k} \frac{n_0 p^\nu - i}{p^\nu - i}\,.$$

De $k + 1$ faktorer på højresiden er brøker, og deres produkt er det hele tal N. Faktoren for $i = 0$ er $n_0 p^\nu / p^\nu = n_0$. For de øvrige faktorer er $i \geqslant 1$, og vi kan skrive $i = i_0 p^\iota$, hvor $p \nmid i_0$; da $i < p^\nu$, er $0 \leqslant \iota < \nu$. Herefter kan vi forkorte den i'te faktor:

$$\frac{n_0 p^\nu - i}{p^\nu - i} = \frac{n_0 p^\nu - i_0 p^\iota}{p^\nu - i_0 p^\iota} = \frac{n_0 p^{\nu-\iota} - i_0}{p^{\nu-\iota} - i_0}\,.$$

Lad a_i/s_i være brøken på højresiden. Da $\nu - \iota \geqslant 1$, har vi $a_i \equiv -i_0 \pmod{p}$ og $s_i \equiv -i_0 \pmod{p}$ og p går ikke op i i_0. Specielt er altså $a_i \equiv s_i \not\equiv 0 \pmod{p}$. Af ligningen $N = n_0 \prod_{i=1}^{k}(a_i/s_i)$ får vi ligningen,

$$N s_1 \cdots s_k = n_0 a_1 \cdots a_k. \tag{*}$$

Af det viste følger specielt, at produkterne $a_1 \cdots a_k$ og $s_1 \cdots s_k$ har samme restklasse modulo p, og yderligere, at denne restklasse er en primisk restklasse. Af ligningen (*) følger derfor, at $N \equiv n_0 \pmod{p}$. □

(8.7) Sylow's Sætninger. *Lad p være en primdivisor i ordenen $|G|$. Da gælder følgende tre sætninger:*

(1) *Der eksisterer Sylow-p-undergrupper af G.*

(2) *Sylow-p-undergrupperne af G er indbyrdes konjugerede og enhver p-undergruppe af G er indeholdt i en Sylow-p-undergruppe.*

(3) *Antallet af Sylow-p-undergrupper er kongruent med 1 modulo p og divisor i $|G|$.*

Bevis. Skriv $|G| = n_0 p^\nu$, hvor $p \nmid n_0$. Sylow-p-undergrupperne er altså undergrupperne af orden p^ν. Lad d være antallet af Sylow-p-undergrupper. Det er altså påstanden i Sylow's første Sætning, at $d \geqslant 1$.

Gruppen G virker på sig selv ved translation. Den virker derfor også på mængden af delmængder af G. Specielt virker G på mængden $\mathcal{X}$ bestående af alle delmængder $A \subseteq G$ med p^ν elementer. Virkningen af G på $\mathcal{X}$ er bestemt ved

$$gA := \{ga \mid a \in A\}.$$

Elementantallet $N := |\mathcal{X}|$, altså antallet af delmængder af G med p^ν elementer, er binomialkoefficienten $\binom{n_0 p^\nu}{p^\nu}$. Det følger derfor af Lemma (8.6), at $|\mathcal{X}| \equiv n_0 \pmod p$. Da p ikke går op i n_0, følger det specielt, at p ikke går op i elementantallet $|\mathcal{X}|$.

Betragt nu klassedelingen af $\mathcal{X}$ i baner hørende til virkningen. Hvis alle baner havde længde delelig med p, ville summen af længderne, altså $|\mathcal{X}|$, være delelig med p. Der findes derfor baner $\mathcal{B}$, hvis længde er primisk med p.

Lad $\mathcal{B}$ være en sådan bane. Betragt et element A i banen $\mathcal{B}$, og lad T være isotropigruppen for A. Vi beviser først, at T er en Sylow-p-gruppe.

Banen $\mathcal{B}$ består af alle translaterede delmængder gA, for $g \in G$, og T består af de elementer $h \in G$, for hvilke $hA = A$. Vælg et element $a \in A$. Af $hA = A$ følger specielt, at $ha \in A$. Altså er $Ta \subseteq A$. Delmængden Ta er en højresideklasse modulo T, og den har derfor samme antal elementer som T. Da $Ta \subseteq A$ og A har p^ν elementer, får vi uligheden,

$$|T| \leqslant p^\nu. \tag{*}$$

På den anden side gælder ifølge Baneformlen og Lagrange's Indexsætning, at $|G| = |T| \cdot |\mathcal{B}|$. Specielt er p^ν divisor i $|T| \cdot |\mathcal{B}|$. Desuden er p^ν primisk med $|\mathcal{B}|$, idet p ikke gik op i $|\mathcal{B}|$. Følgelig er p^ν divisor i $|T|$. Af (*) slutter vi derfor, at $|T| = p^\nu$. Isotropigruppen T er derfor en Sylow-p-gruppe. Specielt er Sylow's første Sætning hermed vist.

Da $Ta \subseteq A$, og da vi nu ved, at de to delmængder har det samme elementantal, nemlig p^ν, slutter vi at $Ta = A$. Banen $\mathcal{B}$ har som elementer alle translaterede mængder gA, for $g \in G$. Specielt, for $g := a^{-1}$, følger det, at $T' := a^{-1}Ta$ er element i $\mathcal{B}$. Delmængden $T' = a^{-1}Ta$ er selv en undergruppe, nemlig konjugeret til T; den er altså også en Sylow-p-undergruppe. Den ligger i banen $\mathcal{B}$, og $\mathcal{B}$ består derfor af samtlige sideklasser gT' modulo Sylow-p-gruppen T'.

Vi har således vist, for virkningen af G på $\mathcal{X}$, at enhver bane, hvis længde er primisk med p, består af samtlige sideklasser gS modulo en Sylow-p-undergruppe S. Omvendt er det klart for hver Sylow-p-undergruppe S, at $S \in \mathcal{X}$ og at banen gennem S består af sideklasserne gS. Specielt er længden af en sådan bane lig med index $|G{:}S|$, og dermed lig med $n_0 p^\nu / p^\nu = n_0$. Banerne, hvis længde er primisk med p, er altså netop banerne gennem Sylow-p-undergrupperne S, og disse baner har alle længden n_0. Der er én bane for hver af de d Sylow-p-undergrupper. Banerne udgør en klassedeling af $\mathcal{X}$. De d baner af længde n_0 bidrager med dn_0 til elementantallet i $\mathcal{X}$, og de øvrige baner har en længde, der er delelig med p. Altså er $|\mathcal{X}| \equiv dn_0 \pmod{p}$. Desuden så vi, at $|\mathcal{X}| \equiv n_0 \pmod{p}$. Altså er

$$n_0 \equiv |\mathcal{X}| \equiv dn_0 \pmod{p}.$$

Da n_0 er primisk med p, følger det, at $d \equiv 1 \pmod{p}$. Hermed er den første del af Sylow's tredie Sætning bevist.

For at vise Sylow's anden Sætning betragtes en vilkårlig Sylow-p-gruppe S og en vilkårlig p-undergruppe H. Lad $\mathcal{B}$ være banen gennem S, bestående af alle sideklasser gS. Gruppen G virker på $\mathcal{B}$, så ved restriktion fås en virkning af H på $\mathcal{B}$. Gruppen H er en p-gruppe og elementantallet n_0 af $\mathcal{B}$ er primisk med p. Af Tælleformlen, jfr Observation (7.21), følger derfor, at der i $\mathcal{B}$ findes et element, der er fixpunkt for virkningen af H. Med andre ord findes en sideklasse gS således, at vi for alle $h \in H$ har ligningen,

$$hgS = gS.$$

Øjensynlig gælder $hgS = gS$, hvis og kun hvis $h \in gSg^{-1}$. Vi har derfor $h \in gSg^{-1}$ for alle $h \in H$, altså inklusionen,

$$H \subseteq gSg^{-1}.$$

Med S er også gSg^{-1} en Sylow-p-undergruppe. Inklusionen viser derfor specielt, at H er indeholdt i en Sylow-p-gruppe. Hvis H selv er en Sylow-p-gruppe, må inklusionen være en lighed; vilkårlige to Sylow-p-undergrupper H og S er derfor konjugerede. Hermed er Sylow's anden Sætning bevist.

Vi mangler nu kun at bevise den sidste del af Sylow's tredie Sætning. Hertil bemærker vi, at gruppen G virker på mængden af alle undergrupper af G ved konjugering: for $g \in G$ og en undergruppe H af G er ${}^gH := gHg^{-1}$ igen en undergruppe. Af Sylow's anden Sætning følger, at hvis S er en given Sylow-p-undergruppe, så er banen gennem S ved denne virkning, altså de med S konjugerede undergrupper, samtlige Sylow-p-undergrupper. Antallet af Sylow-p-undergrupper er altså længden af denne bane, og derfor lig med index af isotropigruppen for S. Specielt er antallet divisor i $|G|$.

Hermed er Sylow's tre sætninger bevist. □

(8.8) Observation. Antag, at primtallet p er divisor i $|G|$, og skriv $|G| = n_0 p^\nu$, hvor p ikke går op i n_0. Lad d være antallet af Sylow-p-grupper. Ifølge Sylow's tredie Sætning er $d \equiv 1 \pmod{p}$ og $d \mid n_0 p^\nu$. Specielt er d primisk med p^ν, og følgelig er d divisor i n_0. Antallet d skal altså søges blandt de tal, som er divisorer i n_0 og kongruente med 1 modulo p.

Følgende to betingelser er ækvivalente:

(i) *Der er en og kun én Sylow-p-undergruppe i G.*
(ii) *Der findes i G en normal Sylow-p-undergruppe.*

Lad nemlig S være en Sylow-p-undergruppe. Enhver konjugeret undergruppe gSg^{-1} er da ligeledes en Sylow-p-undergruppe. Hvis (i) er opfyldt, er altså $S = gSg^{-1}$ for alle g, og så er S normal. Antag omvendt, at S er normal. Da er $S = gSg^{-1}$ for alle g, og da alle Sylow-p-undergrupperne er konjugerede med S ifølge Sylow's anden Sætning, er de derfor alle lig med S. Altså gælder (i).

I en kommutativ gruppe er alle undergrupper normale. Hvis G er kommutativ, findes altså for hver primdivisor p_i i $|G|$ netop én Sylow-p_i-undergruppe af G. Det er undergruppen $G(p_i)$, således som vi så det i Eksempel (8.3).

(8.9) Observation. Antag, at p er en primdivisor i $|G|$, og at $|G| = n_0 p^\nu$, hvor $p \nmid n_0$. For en undergruppe H af G er $|H|$ divisor i $|G|$, så vi har $|H| = m_0 p^\mu$, hvor $m_0 | n_0$ og $\mu \leqslant \nu$. En Sylow-p-undergruppe af H er en undergruppe af orden p^μ, og den er kun en Sylow-p-undergruppe af G, hvis $\mu = \nu$. Det er klart, at $\mu = \nu$, hvis og kun hvis H's index i G er primisk med p.

Antag, at H's index i G er primisk med p, og dermed at enhver Sylow-p-undergruppe af H er en Sylow-p-undergruppe af G. Hvis H desuden er normal i G, så gælder det også omvendt, at enhver Sylow-p-undergruppe af G er indeholdt i H. Der findes nemlig en Sylow-p-undergruppe S af H, og den er en Sylow-p-undergruppe af G. Enhver Sylow-p-undergruppe T af G er så konjugeret med S, dvs af formen $T = gSg^{-1}$, og så er $T \subseteq gHg^{-1} = H$.

Det følger specielt, når H er normal i G, at H har en normal Sylow-p-undergruppe, hvis og kun hvis G har en normal Sylow-p-undergruppe.

(8.10) Sætning. *Lad G være en gruppe af orden n, og lad $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ være primopløsningen af n. Antag for alle i, at G har en normal Sylow-p_i-undergruppe S_i. Da er G lig med produktet af sine Sylow-undergrupper:*

$$S_1 \times \cdots \times S_r = G.$$

Bevis. Det er nok at vise, ved induktion efter $j = 1, \dots, r$, at delmængden $G_j := S_1 \cdots S_j$, bestående af alle produkter $g_1 \cdots g_j$ med $g_i \in S_i$, er en normal undergruppe og at G_j er produktet af sine Sylow-undergrupper, $G_j = S_1 \times \cdots \times S_j$.

Påstanden er triviel for $j = 1$. Antag, at $1 < j \leqslant r$, og at påstanden gælder for $j - 1$. Gruppen G_{j-1} er produktet af sine Sylow-grupper $S_1, \dots, S_{j-1}$, så ordenen af G_{j-1} lig med produktet af potenserne $p_i^{\nu_i}$ for $1 \leqslant i \leqslant j - 1$. Specielt er ordenen af G_{j-1} primisk med p_j. Betragt delmængden G_j. Øjensynlig er $G_j = G_{j-1} S_j$. Da G_{j-1} er en undergruppe og S_j er normal, er G_j en undergruppe, jfr Noether's første Isomorfisætning. Yderligere er G_{j-1} normal ifølge induktionsantagelsen og S_j er forudsat normal. Heraf følger klart, at også $G_j = G_{j-1} S_j$ er normal. Fællesmængden $G_{j-1} \cap S_j$ er en undergruppe af en orden, der er divisor i $|S_j|$ (hvis orden er en potens af p_j) og i $|G_{j-1}|$ (hvis orden var primisk med p_j). Fællesmængden har derfor orden 1, dvs $G_{j-1} \cap S_j = \{e\}$. Nu er betingelsen (6.4)(ii) opfyldt, med $G := G_j$, $H := G_{j-1}$, og $K := S_j$. Det følger derfor, at $G_j = G_{j-1} \times S_j$. Da vi induktivt har, at $G_{j-1} = S_1 \times \cdots \times S_{j-1}$, er påstanden hermed vist for j.

Hermed er induktionsskridtet fuldført, og beviset afsluttet. ▯

(8.11) Korollar. *Der er kun én gruppe af orden qp, hvor $q < p$ er to primtal og $p \not\equiv 1 \pmod{q}$, nemlig den cykliske gruppe* C_{qp}.

Bevis. Antallet af Sylow-p-undergrupper i en sådan gruppe G er nemlig divisor i q og kongruent med 1 modulo p. Da $q < p$, må antallet være 1. Der findes altså én Sylow-p-undergruppe S, og den må derfor være normal. Antallet af Sylow-q-undergrupper er divisor i p, og altså enten 1 eller p. Desuden er antallet kongruent med 1 modulo q. Af forudsætningen følger derfor, at antallet ikke kan være p. Der er altså én Sylow-q-undergruppe T, og den må være normal. Af Sætning (8.10) følger nu, at $G = T \times S$. Gruppen T har orden q og q er et primtal, så $T = \mathrm{C}_q$. Tilsvarende er $S = \mathrm{C}_p$. Følgelig er

$$G = \mathrm{C}_q \times \mathrm{C}_p = \mathrm{C}_{qp},$$

hvor det sidste lighedstegn for eksempel følger af (3.20). □

(8.12) Note. Forudsætningen i (8.11), at $p \not\equiv 1 \pmod{q}$, er aldrig opfyldt, hvis $q = 2$, idet primtallet $p > q$ må være ulige. Vi kender jo også en ikke-kommutativ gruppe af orden $2p$, nemlig diedergruppen D_p. Lad os vise her, for et ulige primtal p, at der er præcis to grupper af orden $2p$, nemlig den cykliske gruppe C_{2p} og diedergruppen D_p.

Betragt en sådan gruppe G, af orden $2p$. Det følger, at G har én Sylow-p-undergruppe S. Undergruppen S har orden p, og den må derfor være cyklisk, altså $S = \langle\sigma\rangle$, hvor σ har orden p. Da S er den eneste Sylow-p-undergruppe, er potenserne σ^i, for $i = 1, \dots, p-1$, samtlige elementer af orden p. Lad nu τ være et element af orden 2. Da er G foreningsmængden af højresideklasserne S og $S\tau$, så elementerne i G er de $2p$ elementer af formen σ^i eller $\sigma^i\tau$. Det konjugerede element $\tau\sigma\tau$ har igen orden p, så vi har en ligning $\tau\sigma\tau = \sigma^i$, med $1 \leqslant i \leqslant p - 1$. Konjuger ligningen med τ. Da τ har orden 2 og konjugering er en homomorfi, får vi ligningen $\sigma = (\sigma^i)^i$. Altså er $i^2 \equiv 1 \pmod{p}$. Primtallet p er altså divisor i $i^2 - 1 = (i+1)(i-1)$, og følgelig går p op i enten $i - 1$ eller $i + 1$. Da vi har antaget $1 \leqslant i \leqslant p - 1$, følger det, at enten er $i = 1$ eller $i = p - 1$. I det første tilfælde er $\tau\sigma = \sigma\tau$. Heraf følger, at G er kommutativ, og så er $G = \mathrm{C}_{2p}$. I det andet tilfælde er $\tau\sigma = \sigma^{-1}\tau$. Her genkender vi reglerne for regning i diedergruppen. I dette tilfælde er altså $G = \mathrm{D}_p$.

(8.13) Definition. En gruppe G kaldes *simpel*, hvis G ikke er den trivielle gruppe og hvis de to trivielle undergrupper G og $\{e\}$ er de eneste normale undergrupper.

Simple grupper spiller en vigtig rolle i klassifikationen af endelige grupper. Som vi skal se herunder, er det let at bestemme de kommutative simple grupper. I princippet er alle simple grupper bestemt. En del af den generelle bestemmelse er indeholdt i Feit–Thompson's Sætning: *De eneste simple grupper af ulige orden er de cykliske grupper* C_p, *hvor p er et ulige primtal.*

Der er flere uendelige familier af simple grupper af lige orden. Den enkleste familie består af de alternerende grupper A_n for $n \geqslant 5$, som vi behandler nedenfor.

(8.14) Sætning. *De simple (endelige) kommutative grupper er grupperne* C_p, *hvor p er et primtal.*

Bevis. For et primtal p følger det af Lagrange's Indexsætning, at gruppen C_p kun har trivielle undergrupper; specielt er C_p en simpel gruppe.

Antag omvendt, at G er en simpel, kommutativ gruppe af orden n. Da $G \neq \{e\}$, findes et element $g \neq e$ i G. Den cykliske undergruppe $\langle g \rangle$ er normal, da G er kommutativ. Da G er simpel og $\langle g \rangle \neq \{e\}$, er $\langle g \rangle = G$. Altså er G cyklisk. Hvis d er en ikke-triviel divisor i n, har G derfor en ikke-triviel undergruppe af orden d. Eksistensen af en sådan er udelukket, da G er simpel. Følgelig er $n = p$ et primtal, og $G = \mathrm{C}_p$. □

(8.15) Eksempel. Den symmetriske gruppe S_n for $n \geqslant 3$ og diedergruppen D_n for $n \geqslant 2$ er ikke simple. Den alternerende gruppe A_n er nemlig en ikke-triviel normal undergruppe i S_n og C_n er en ikke-triviel normal undergruppe i D_n.

En p-gruppe er kun simpel, hvis den har orden p. Af Korollar (7.24) følger nemlig, at en gruppe af orden p^ν har en normal undergruppe af orden p.

(8.16) Eksempel. En gruppe af orden $n_0 p^\nu$, hvor p er et primtal og $1 < n_0 < p$ (og $\nu \geqslant 1$) kan ikke være simpel. Antallet af Sylow-p-undergrupper er nemlig divisor i n_0, og dermed mindre end p, og da det desuden er kongruent med 1 modulo p, må antallet være 1. Sylow-p-undergruppen er derfor en ikke-triviel normal undergruppe.

Specielt gælder, at en gruppe af orden $2{\cdot}3$ har en normal Sylow-3-undergruppe, og en gruppe af orden $2{\cdot}5$, eller $3{\cdot}5$, eller $4{\cdot}5$, har en normal Sylow-5-undergruppe. Specielt kan grupper af disse ordener ikke være simple.

En gruppe af orden $12 = 2^2{\cdot}3$ har enten en normal Sylow-2-undergruppe eller en normal Sylow-3-undergruppe. Dette vises ved et såkaldt tælleargument: Sylow-2-undergrupperne er undergrupperne af orden 4, og antallet af dem er ulige og divisor i 3; antallet er altså 1 eller 3. Sylow-3-undergrupperne er undergrupperne af orden 3, og antallet af dem er kongruent med 1 modulo 3 og divisor i 2^2. Antallet af dem er altså enten 1 eller 4. Antag, at en Sylow-3-undergruppe ikke er normal. Der er da 4 Sylow-3-undergrupper. Hver Sylow-3-undergruppe S er af orden 3, og indeholder altså ud over det neutrale element 2 elementer af orden 3. Hvis S_1 og S_2 er forskellige Sylow-3-undergrupper, er fællesmængden $S_1 \cap S_2$ en ægte undergruppe af S_1; ordenen af $S_1 \cap S_2$ er derfor en ægte divisor i 3, altså lig med 1, og så er $S_1 \cap S_2 = \{e\}$. De fire Sylow-3-undergrupper dækker derfor i alt $4{\cdot}2 = 8$ elementer af orden 3. Ingen af disse 8 elementer kan ligge i en undergruppe af orden 2^2, så en Sylow-2-undergruppe T må være disjunkt med delmængden af disse 8 elementer. Men det betyder, at de resterende 4 elementer må udgøre T. Specielt er T den eneste Sylow-2-undergruppe, og T er derfor normal i G.

Specielt kan en gruppe af orden 12 ikke være simpel.

(8.17) Sætning. *Den alternerende gruppe* A_n *er simpel for* $n \geqslant 5$.

Bevis. Lad $N \neq \{e\}$ være en normal undergruppe af A_n. Vi skal vise, at $N = \mathrm{A}_n$. Vi skal flere steder i beviset benytte, at $n \geqslant 5$.

Cykler af længde 3 (i S_n) er lige. De tilhører altså A_n. Vi viser først, at alle 3-cykler er konjugerede i gruppen A_n. Hertil udnyttes, at $n \geqslant 5$.

Det er klart, jfr (7.18), at vilkårlige to 3-cykler γ og γ' er konjugerede i S_n, altså at der findes en permutation $\mu \in \mathrm{S}_n$ således, at $\gamma' = \mu\gamma\mu^{-1}$. Mere præcist gælder jo for en 3-cykel

$\gamma = (a\,b\,c)$ og en permutation $\mu \in \mathrm{S}_n$, at den konjugerede permutation ${}^{\mu}\gamma = \mu\gamma\mu^{-1}$ er 3-cyklen $(\mu(a)\,\mu(b)\,\mu(c))$. Vi kan derfor altid løse ligningen ${}^{\mu}\gamma = \gamma'$ med en permutation $\mu \in \mathrm{S}_n$, idet vi blot skal vælge passende værdier af μ på de tre tal a, b, c. Hvis μ er ulige, kan vi opnå en lige permutation med de samme værdier på a, b, c ved at ombytte værdierne på 2 af de resterende $n-3$ tal. Altså findes en permutation $\mu \in \mathrm{A}_n$ således, at $\gamma' = {}^{\mu}\gamma$.

Videre er det er nok at vise, at N indeholder en 3-cykel. Antag nemlig, at 3-cyklen γ tilhører N. Da N er normal i A_n, følger det, at enhver konjugeret permutation $\mu\gamma\mu^{-1}$ for $\mu \in \mathrm{A}_n$ ligeledes tilhører N. Altså vil enhver 3-cykel tilhøre N. Enhver lige permutation er et produkt af 3-cykler ifølge Sætning (2.24)(1). Enhver lige permutation tilhører derfor N. Følgelig er $N = \mathrm{A}_n$.

Vi mangler at vise, at der findes en 3-cykel i N. Da $N \neq \{\mathrm{id}\}$, findes en permutation $\sigma \neq \mathrm{id}$ i N. Betragt nu, for $\alpha \in \mathrm{A}_n$, kommutatoren $[\sigma, \alpha] := \sigma\alpha\sigma^{-1}\alpha^{-1}$. Vi kan skrive $[\sigma, \alpha] = \sigma(\alpha\sigma^{-1}\alpha^{-1})$; den første faktor, σ, ligger i N og den anden faktor, $\alpha\sigma^{-1}\alpha^{-1}$ ligger i N, da N er normal. Altså er $[\sigma, \alpha] \in N$. Det er påstanden, at vi ved en eller to gange at erstatte σ med en permutation af formen $[\sigma, \alpha]$ for $\alpha \in \mathrm{A}_n$ kan opnå en 3-cykel.

Hertil bemærker vi først, at vi jo også kan skrive $[\sigma, \alpha] = (\sigma\alpha\sigma^{-1})\alpha^{-1}$, altså

$$[\sigma, \alpha] = {}^{\sigma}\alpha\,\alpha^{-1}. \tag{1}$$

Heraf fremgår, at hvis vi fx som α vælger en 3-cykel, så er $[\sigma, \alpha]$ produktet af to 3-cykler. Specielt kan $[\sigma, \alpha]$ højst flytte 6 af de n tal.

Vi viser først, at vi kan bestemme en 3-cykel α således, at $[\sigma, \alpha]$ højst flytter 5 tal; vi må naturligvis også sørge for at $[\sigma, \alpha]$ ikke er identiteten. Hertil vælges et tal a, som ikke er fixpunkt for σ. Vi sætter $a_1 := a$, og induktivt $a_{i+1} := \sigma(a_i)$. Da er $a_2 \neq a_1$ (men det er ikke udelukket, at $a_3 = a_1$). Vælg nu et tal $b \notin \{a_1, a_2, a_3\}$, sæt $b_1 := b$ og induktivt $b_{i+1} := \sigma(b_i)$. Lad α være 3-cyklen $\alpha = (a_1\,a_2\,b_1)$. Af (1) får vi, at

$$[\sigma, \alpha] = {}^{\sigma}(a_1\,a_2\,b_1)(a_1\,a_2\,b_1)^{-1} = (a_2\,a_3\,b_2)(a_1\,b_1\,a_2) = (b_1\,a_3\,\ldots\,;$$

højresiden er ikke afsluttet, idet vi ikke kan bestemme billedet af a_3 før vi ved, om $a_3 = a_1$ eller $a_3 \neq a_1$. Det fremgår imidlertid af udregningen, at $[\sigma, \alpha]$ ikke kan være identiteten. Desuden kan $[\sigma, \alpha]$ højst flytte tallene a_1, a_2, a_3, b_1, b_2 (som ikke behøver at være forskellige). Idet vi kan erstatte σ med $[\sigma, \alpha]$, kan vi herefter antage, at σ højst flytter 5 af de n tal.

Nu er der tre tilfælde: σ flytter 3, 4, eller 5 tal. Hvis σ flytter 3 tal, er σ nødvendigvis en 3-cykel, og vi har fundet den ønskede 3-cykel i N. I de to andre tilfælde erstatter vi igen σ med $[\sigma, \alpha]$ med en 3-cykel α som ovenfor; når vi ved at σ flytter 4 eller 5 tal, kan vi være lidt mere snedige i valget af b.

Antag, at σ flytter præcis 4 tal. Da σ også er en lige permutation, må σ være en dobbelttransposition. Specielt er så $a_3 = a_1$. Da $n \geqslant 5$, har σ et fixpunkt. Vi vælger som b et fixpunkt for σ. Med 3-cyklen $\alpha = (a_1, a_2, b)$ finder vi,

$$[\sigma, \alpha] = {}^{\sigma}(a_1\,a_2\,b)(a_1\,a_2\,b)^{-1} = (a_2\,a_1\,b)(a_1\,b\,a_2) = (a_1\,a_2\,b).$$

Permutationen $[\sigma, \alpha]$ er altså en 3-cykel i N.

Antag endelig, at σ flytter præcis 5 tal. Da σ også er en lige permutation, må σ være en 5-cykel, og dermed 5-cyklen $(a_1\, a_2\, a_3\, a_4\, a_5)$. Som α vælger vi 3-cyklen $\alpha := (a_1\, a_2\, a_5)$. Herefter er

$$[\sigma, \alpha] = {}^{\sigma}(a_1\, a_2\, a_5)(a_1\, a_2\, a_5)^{-1} = (a_2\, a_3\, a_1)(a_1\, a_5\, a_2) = (a_1\, a_5\, a_3).$$

Permutationen $[\sigma, \alpha]$ er altså en 3-cykel i N.

Hermed er der i alle tilfælde bestemt en 3-cykel i N, som ønsket. □

(8.18) Opgaver.

1. Hvor mange Sylow-2-undergrupper findes der i diedergruppen D_4?

2. Lad p være et primtal. Vis, at en endelig gruppe G er en p-gruppe, hvis og kun hvis hvert element i G har en orden, som er en potens af p.

3. Vis, at en gruppe af orden 1.088 ikke kan være simpel.

4. Vis, at en gruppe af orden pq, hvor p og q er primtal, ikke kan være simpel.

5. Lad H være en undergruppe af en gruppe G. Vis, at $N(H) := \{g \in G \mid gHg^{-1} = H\}$ er en undergruppe af G. Vis, at H er en normal undergruppe af $N(H)$. Vis, at antallet af undergrupper, der er konjugerede med H, er index $|G : N(H)|$.

6. Vis, at en gruppe G af orden $2u$, hvor $u > 1$ er ulige, ikke kan være simpel. [Vink: hvorfor findes en surjektiv homomorfi $\chi : G \to \{\pm 1\}$?]

7. Vis, at der kun er én gruppe af orden 15.

8. Vis, at en gruppe af orden 45 har en normal Sylow-5-undergruppe og en normal Sylow-3-undergruppe. Vis, at der er to grupper af orden 45, og angiv dem.

9. Vis, at enhver Sylow-2-undergruppe i S_5 er isomorf med D_4.

10. Vis, at en gruppe af orden 56 ikke kan være simpel. [Vink: vis, ved at tælle elementer af orden 7, at hvis Sylow-7-undergruppen ikke er normal, så er der kun plads til én Sylow-2-undergruppe.]

11. Vis, for $n \geqslant 5$, at A_n er den eneste ikke-trivielle normale undergruppe af S_n.

12. Bestem for $n = 1, 2, \dots, 11$ alle grupper af orden n.

13. Lad G være en simpel, ikke-kommutativ gruppe af orden n, og lad d være antallet af Sylow-p-undergrupper, for en primdivisor p i $|G|$. Vis, at $n \mid d!$. [Vink: virkningen af G på Sylow-p-undergrupperne definerer en repræsentation $G \to S_d$.]

14. *Vis, at de eneste ikke-kommutative grupper af orden 12 er de tre grupper beskrevet i en af opgaverne i (5.18).

15. *Vis, at en gruppe G af orden $2^{\nu}\cdot 3$ enten har en normal undergruppe af index 3 eller en normal undergruppe af index 6. [Vink: Antag, at S og T er forskellige Sylow-2-undergrupper. Vis, ved at betragte elementantallet i ST, at $H := S \cap T$ har index 2 i S. Slut heraf, at $S \subseteq N(H)$, hvor $N(H) := \{g \in G \mid gHg^{-1} = H\}$. Tilsvarende er $T \subseteq N(H)$, og følgelig er $N(H) = G$.]

16. Lad G være en gruppe af orden n. Vis, at for hver primdivisor p i n findes i G et element af orden p (Cauchy's Sætning). Vis mere generelt, at for hver primtalspotens p^ν, som går op i n, findes i G en undergruppe af orden p^ν.

17. Lad $V \subseteq \mathrm{S}_4$ være undergruppen bestående af identiteten og de 3 dobbelt-transpositioner. Vis, at for vilkårlige to forskellige Sylow-2-undergrupper H, K af S_4 er $H \cap K = V$.

18. Lad G være en endelig gruppe, lad p være en primdivisor i $|G|$, og lad $N \subseteq G$ være fællesmængden af alle Sylow-p-undergrupper af G. Vis, at N er den største normale p-undergruppe af G. Hvad bliver N for $p = 2$ og $G = \mathrm{S}_4$? – og for $G = \mathrm{S}_5$?

Symmetrier

1. Ortogonale afbildninger.

(1.1) Sætning. *Lad der være givet en ortonormal basis $(e_1, \dots, e_n)$ for vektorrummet $\mathbb{R}^n$. Lad $T\colon \mathbb{R}^n \to \mathbb{R}^n$ være en lineær afbildning og lad A være matricen for T med hensyn til den givne basis. Da er følgende seks betingelser ækvivalente:*

(i) *Den lineære afbildning T bevarer det indre produkt: $\langle Tx, Ty\rangle = \langle x, y\rangle$.*
(ii) *Den lineære afbildning T bevarer normen: $\|Tx\| = \|x\|$.*
(iii) *Den lineære afbildning T er en isometri: $\|Tx - Ty\| = \|x - y\|$.*
(iv) *Billedvektorerne $(Te_1, \dots, Te_n)$ udgør et ortonormalt sæt af vektorer i $\mathbb{R}^n$.*
(v) *Søjlerne i matricen A udgør et ortonormalt sæt af vektorer i $\mathbb{R}^n$.*
(vi) *Der gælder ligningen $A^{\mathrm{t}}A = 1$, hvor 1 er enhedsmatricen i $\mathrm{Mat}_n(\mathbb{R})$.*

Bevis. Det indre produkt i $\mathbb{R}^n$ kan som bekendt udtrykkes ved normen, idet der gælder ligningen,

$$\langle x, y\rangle = \frac{1}{2}\big(\|x + y\|^2 - \|x\|^2 - \|y\|^2\big).$$

Afbildningen T er specielt additiv. Det følger, at hvis T bevarer normen, så ændres højresiden i ligningen ikke, hvis x, y erstattes med Tx, Ty. Altså vil T så også bevare det indre produkt.

Normen $\|x\|$ er kvadratroden af det indre produkt $\langle x, x\rangle$. Det følger, at hvis T bevarer det indre produkt, så vil T også bevare normen.

Endelig er afstanden mellem x og y lig med normen $\|x - y\|$ og normen $\|x\|$ er afstanden mellem x og nul-vektoren 0. Da T er lineær følger det, at T bevarer normen, hvis og kun hvis T er en isometri.

Hermed er vist, at de første tre betingelser (i), (ii) og (iii) er ækvivalente.

Hvis (i) er opfyldt, så slutter vi specielt, at vektorerne $(Te_1, \dots, Te_n)$ udgør et ortonormalt system, altså at (iv) er opfyldt. Antag omvendt, at (iv) gælder. Da er vektorerne $(Te_1, \dots, Te_n)$ en ortonormal basis for $\mathbb{R}^n$. Med hensyn til en given ortonormal basis kan det indre produkt af to vektorer beregnes som prik-produktet af deres koordinatsæt. Det indre produkt $\langle Tx, Ty\rangle$ er altså lig med prik-produktet af koordinatsættene for Tx og Ty med hensyn til basen $(Te_1, \dots, Te_n)$. De to koordinatsæt er lig med koordinatsættene for x og y med hensyn til basen $(e_1, \dots, e_n)$. Heraf følger, at $\langle Tx, Ty\rangle = \langle x, y\rangle$. Altså gælder (i).

Hermed er vist, at (iv) er ækvivalent med (i).

Den i'te søjle i A er koordinatsættet for Te_i med hensyn til den givne ortonormale basis. Det er derfor klart, at (iv) og (v) er ækvivalente.

For at vise ækvivalensen af (v) og (vi) bemærkes, at i en produktmatrix BA er elementet på plads (i, j) lig med prik-produktet af den i'te række i B og den j'te søjle i A. Anvendt med $B = A^{\mathrm{t}}$ følger det, at produktmatricen $A^{\mathrm{t}}A$ på plads (i, j) har prik-produktet af den i'te søjle og den j'te søjle i A. Heraf fremgår, at betingelserne (v) og (vi) er ækvivalente.

Hermed er ækvivalensen af alle seks betingelser bevist. $\square$

(1.2) Definition. En lineær afbildning $T : \mathbb{R}^n \to \mathbb{R}^n$, som opfylder de ækvivalente betingelser i Sætning (1.1), kaldes en *ortogonal afbildning*.

Af de seks ækvivalente betingelser i Sætning (1.1) er de tre første uafhængige af den givne ortonormale basis. Det følger derfor af ækvivalensen, at hvis en af de tre sidste betingelser er opfyldt med hensyn til en given ortonormal basis, så er de alle opfyldt med hensyn til enhver ortonormal basis.

De lineære afbildninger $\mathbb{R}^n \to \mathbb{R}^n$ er netop afbildningerne af formen $x \mapsto Ax$, hvor $A \in \mathrm{Mat}_n(\mathbb{R})$, og A er afbildningens matrix med hensyn til den kanoniske basis for $\mathbb{R}^n$. Den kanoniske basis er ortonormal. Afbildningen $x \mapsto Ax$ er altså ortogonal, hvis og kun hvis matricen A opfylder de ækvivalente betingelser (v) og (vi). Er disse betingelser opfyldt, siges A at være en *ortogonal matrix*.

Af en ligning $BA = 1$ for kvadratiske matricer følger som bekendt, at A er invertibel med B som den inverse; specielt er også $AB = 1$. Af ligningen i (vi) følger derfor, at en ortogonal matrix A er invertibel med den transponerede A^{t} som den inverse, og at der gælder ligningen $AA^{\mathrm{t}} = 1$. Den sidste ligning betyder, at også A^{t} er ortogonal. Der gælder altså, at hvis søjlerne i en matrix A er et ortonormalt system, så er også rækkerne et ortonormalt system.

Hvis A og B er ortogonale matricer, så er

$$(AB)^{\mathrm{t}}(AB) = B^{\mathrm{t}}A^{\mathrm{t}}AB = B^{\mathrm{t}}B = 1;$$

altså er også AB en ortogonal matrix. Videre er enhedsmatricen 1 øjensynlig ortogonal. Endelig så vi ovenfor, at en ortogonal matrix er invertibel og at den inverse igen er ortogonal. De ortogonale matricer udgør derfor en undergruppe af den generelle lineære gruppe $\mathrm{GL}_n(\mathbb{R})$. Denne undergruppe kaldes den *ortogonale gruppe* af grad n, og den betegnes $\mathrm{O}_n(\mathbb{R})$ eller blot $\mathrm{O}(n)$. Af Sætning (1.1) fremgår, at den ortogonale gruppe $\mathrm{O}(n)$ kan opfattes som gruppen af lineære isometrier af $\mathbb{R}^n$.

Af ligningen $A^{\mathrm{t}}A = 1$ følger, at $(\det A)^2 = 1$. En ortogonal matrix har derfor determinant ± 1. De ortogonale matricer med determinant 1 udgør en undergruppe af $\mathrm{O}(n)$. Denne undergruppe kaldes den *specielle ortogonale gruppe* og den betegnes $\mathrm{SO}(n)$ eller $\mathrm{O}^+(n)$. Øjensynlig er $\mathrm{SO}(n)$ kernen for homomorfien $\det\colon \mathrm{O}(n) \to \{\pm 1\}$. Det følger, at $\mathrm{SO}(n)$ er en normal undergruppe af index 2 i $\mathrm{O}(n)$. De matricer i $\mathrm{O}(n)$, der har determinant -1, udgør altså én sideklasse, betegnet $\mathrm{O}^-(n)$, og $\mathrm{O}(n) = \mathrm{O}^+(n) \cup \mathrm{O}^-(n)$.

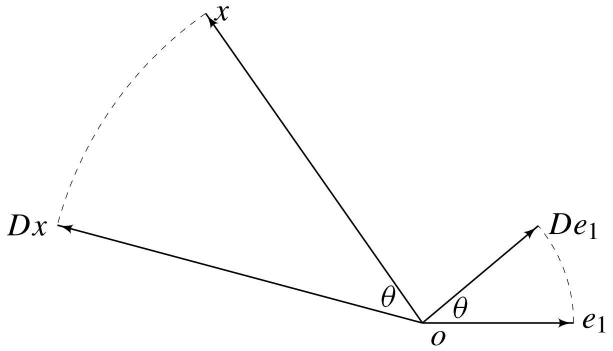
(1.3) Planen. Betragt en matrix A i den ortogonale gruppe $\mathrm{O}(2)$,

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Da søjlerne er ortonormale, har vi $a^2 + b^2 = 1$ og $c^2 + d^2 = 1$ og $ac + bd = 0$. Vektoren (a, b) ligger altså på enhedscirklen, og den har derfor formen $(a, b) = (\cos\theta, \sin\theta)$ med en passende reel vinkel θ. Tilsvarende ligger vektoren (c, d) på enhedscirklen, og (c, d) er ortogonal på (a, b). Det følger, at vi har $(c, d) = (-b, a)$ eller $(c, d) = (b, -a)$. Matricen A har derfor en af følgende to former:

$$D_\theta := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \qquad S_\theta := \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

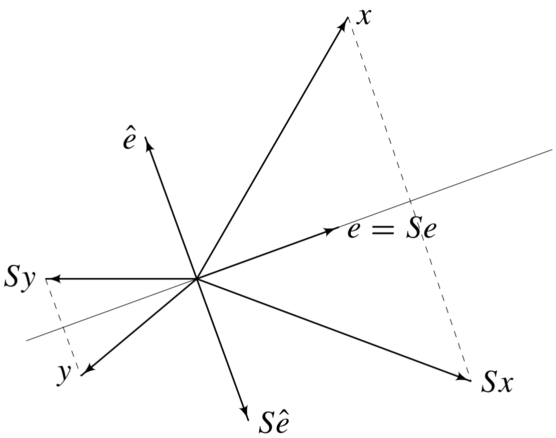
Matricen D_θ af den første form beskriver en *drejning*, D, med vinklen θ omkring *origo* (origo er blot nul-vektoren, betegnet o eller 0, i $\mathbb{R}^2$).



Betragt den lineære afbildning hørende til matricen S_θ af den anden form. Øjensynlig har vi matrixligningen,

$$S_\theta = D_\theta \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

så afbildningen er sammensat af spejlingen i aksen bestemt ved den første basisvektor $(1, 0)$ efterfulgt af drejningen med vinklen θ. Enhedsvektoren $e := (\cos\frac{1}{2}\theta, \sin\frac{1}{2}\theta)$ afbildes ved spejlingen på $(\cos\frac{1}{2}\theta, -\sin\frac{1}{2}\theta)$, som ved drejningen afbildes tilbage på e. Altså er e egenvektor for S_θ med egenværdien 1 og den ortogonale enhedsvektor $\hat{e} := (-\sin\frac{1}{2}\theta, \cos\frac{1}{2}\theta)$ er egenvektor hørende til egenværdien -1. Afbildningen hørende til S_θ er altså selv en *spejling*, S, i aksen gennem o bestemt ved enhedsvektoren e.

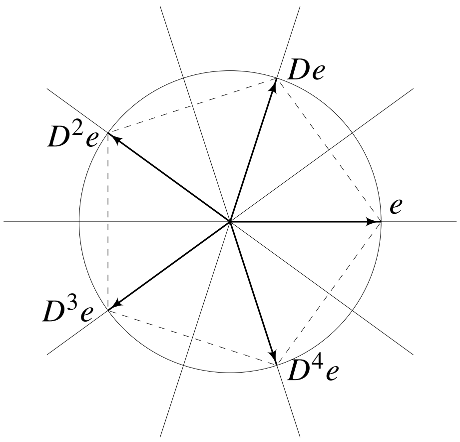


Matricerne af de to former har determinanter henholdsvis 1 og -1. Matricerne i $\mathrm{O}^+(2)$ er altså matricerne D_θ af den første form, og de beskriver drejningerne omkring origo. Matricerne i $\mathrm{O}^-(2)$ er matricerne S_θ af den anden form, og de beskriver spejlingerne i linier gennem origo.

Bemærk, at den specielle ortogonale gruppe $\mathrm{SO}(2)$ er kommutativ. Produktet $D_\theta D_\psi$ er matricen $D_{\theta+\psi}$, der beskriver drejningen med vinklen $\theta + \psi$.

(1.4) Diedergruppen. For $k = 1, 2, \dots$ er drejningen med vinklen $2\pi/k$ den ortogonale afbildning givet ved matricen $D_{2\pi/k}$. Det er klart, at denne matrix har orden k i gruppen $\mathrm{SO}(2)$. Den frembringer altså en cyklisk undergruppe C_k af $\mathrm{SO}(2)$.

Lad $k \geqslant 3$ være fast, og lad $D := D_{2\pi/k}$ være drejningen med vinklen $2\pi/k$. For en enhedsvektor e vil de k vektorer $D^j e$, for $j = 0, 1, \dots, k-1$, udgøre de k hjørner i en regulær k-kant indskrevet i enhedscirklen. Symmetrigruppen for denne k-kant er da undergruppen i $\mathrm{O}(2)$ frembragt af drejningen D og spejlingen S i linien bestemt ved enhedsvektoren e. Den består af de $2k$ matricer D^j og $D^j S$, for $j = 0, \dots, k-1$. Den kaldes *diedergruppen* af grad k, og den betegnes D_k. Bemærk, at der for givet k er én undergruppe C_k, men uendelig mange undergrupper D_k (afhængig af placeringen af enhedsvektoren e). Bemærk videre, at diedergrupperne også er defineret for $k = 1$ og 2: Diedergruppen D_1 er gruppen af orden 2 frembragt af en spejling og diedergruppen D_2 er gruppen af orden 4 frembragt af en spejling og halvdrejningen (dvs drejningen med vinklen π).



(1.5) Sætning. *De cykliske grupper* C_k *og diedergrupperne* D_k *er de eneste endelige undergrupper af* $\mathrm{O}(2)$.

Bevis. Antag nemlig, at H er en endelig undergruppe i $\mathrm{O}(2)$. Fællesmængden $H^+ := H \cap \mathrm{O}^+(2)$, bestående af matricer i H med determinant 1, er en undergruppe i $\mathrm{O}^+(2)$. Hvis H er indeholdt i $\mathrm{O}^+(2)$, har vi $H = H^+$. Hvis H ikke er indeholdt i $\mathrm{O}^+(2)$, så er H^+ en undergruppe af index 2 i H, og komplementærmængden $H^- := H \setminus H^+$ består af én sideklasse. Matricerne i H^- har determinant -1, så de er spejlinger.

Hvis $|H^+| = 1$, så er enten $|H| = |H^+| = 1$, eller $|H| = 2|H^+| = 2$. I det første tilfælde er H den (trivielle) cykliske gruppe C_1, i det andet tilfælde består H af enhedsmatricen og en spejling, og vi har $H = \mathrm{D}_1$.

Antag derfor, at $|H^+| > 1$. Lad $D := D_{\theta_0}$ være drejningen i H^+ med den mindste positive vinkel θ_0. Specielt er så $0 < \theta_0 < 2\pi$. Antag nu for et reelt tal θ, at drejningen D_θ tilhører H. Lad l være det hele tal bestemt ved ulighederne $l\theta_0 \leqslant \theta < (l+1)\theta_0$ eller, ækvivalent,

$$0 \leqslant \theta - l\theta_0 < \theta_0. \tag{*}$$

Da D_θ tilhører H, vil også $D_\theta D^{-l}$ tilhøre H. Den sidste matrix er drejningen med vinklen $\theta - l\theta_0$. Af valget af θ_0 og (*) følger derfor, at $\theta = l\theta_0$. Altså er $D_\theta = D^l$. Heraf ses, at H^+ er den cykliske undergruppe frembragt af D. Matricen $D_{2\pi}$ er enhedsmatricen, og derfor i H. Af det lige viste følger derfor, at vi med et passende naturligt tal k har $2\pi = k\theta_0$. Altså er $D = D_{2\pi/k}$, og H^+ er derfor den cykliske gruppe C_k.

Hvis $H = H^+$, har vi $H = \mathrm{C}_k$, som ønsket. Antag, at $H \supset H^+$. Da findes en spejling S i H. Hvis S' er endnu en spejling i H, så er produktet $S'S$ en drejning, og dermed i H^+. Altså er $S'S = D^j$, og følgelig er $S' = D^j S$. Heraf ses, at H er diedergruppen D_k. ▯

(1.6) Rummet. *Enhver ortogonal afbildning $T : \mathbb{R}^3 \to \mathbb{R}^3$ beskrives i en passende ortonormal basis (e_1, e_2, e) ved en matrix af formen,*

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}, \quad \textit{hvor } \varepsilon = \pm 1.$$

Hvis $\varepsilon = 1$, så er T en drejning med en vinkel θ omkring e (dvs omkring linien gennem origo bestemt ved enhedsvektoren e). Hvis $\varepsilon = -1$, så er T sammensat af drejningen omkring e og spejlingen i planen gennem origo vinkelret på e.

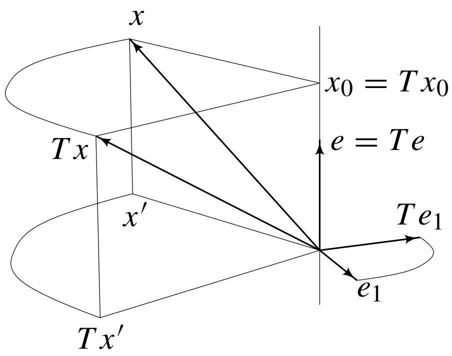
Bevis. Afbildningen T har formen $x \mapsto Ax$ med en 3×3-matrix A. Det karakteristiske polynomium for A er et trediegradspolynomium, og det har derfor en reel rod. Følgelig findes en reel egenværdi ε for T og en tilhørende egenvektor $e \neq 0$. Vi kan normere e, og altså antage, at $\|e\| = 1$. Da T er en isometri og $Te = \varepsilon e$, slutter vi, at $\|\varepsilon e\| = \|e\|$, og dermed at $|\varepsilon| = 1$. Altså er $\varepsilon = \pm 1$. Da T er ortogonal og $Te = \pm e$, har vi for enhver vektor w ligningen,

$$\langle Tw, e\rangle = \pm\langle Tw, Te\rangle = \pm\langle w, e\rangle. \tag{*}$$

Lad nu W være planen bestående af vektorer w, som er ortogonale på e. Hvis $w \in W$, så er $\langle w, e\rangle = 0$, og af ligningen (*) følger, at $\langle Tw, e\rangle = 0$; altså er $Tw \in W$. Heraf ses, at underrummet W er invariant under afbildningen T. Restriktionen af T til dette underrum er altså en lineær isometri $T|W$ i underrummet W. Vælg nu en ortonormal basis (e_1, e_2) for W. I denne basis beskrives restriktionen $T|W$ ved en ortogonal 2×2 matrix. Hvis denne matrix har determinant 1, så har den formen D_θ angivet i (1.3). Det følger, at T i basen (e_1, e_2, e) beskrives ved en matrix af den ønskede form.

Antag i stedet, at matricen for $T|W$ har determinant -1. Det følger af overvejelserne i (1.3), at $T|W$ så er en spejling i en linie i planen W. Vi kan derfor vælge de to vektorer e_1 og e_2 i W således, at den ene er egenvektor for T svarende til egenværdien 1 og den anden er egenvektor svarende til egenværdien -1. Af de tre basisvektorer e_1, e_2, e er altså to egenvektorer for T svarende til samme egenværdi og den tredie er egenvektor svarende til den modsatte egenværdi. Omdøber vi de tre vektorer, kan vi antage, at e_1 og e_2 er egenvektorer svarende til samme egenværdi. I denne basis beskrives T ved en diagonalmatrix, hvor de tre diagonalelementer er ± 1 og hvor de to første har samme fortegn. Øjensynlig har denne matrix den ønskede form, med $\theta = 0$ eller $\theta = \pi$.

Det er klart, og det fremgår af beviset, at en matrix af den anførte form med $\varepsilon = 1$ beskriver en drejning med vinklen θ omkring e.



Matricen med $\varepsilon = -1$ fås fra matricen med $\varepsilon = 1$ ved at multiplicere med den diagonalmatrix, der har $1, 1, -1$ i diagonalen. Heraf fremgår det sidste resultat. ∎

(1.7) Lemma. *Enhver isometrisk afbildning $f\colon \mathbb{R}^n \to \mathbb{R}^n$, der har nul-vektoren som fixpunkt, er lineær, og dermed af formen $x \mapsto Ax$ med en ortogonal matrix A.*

Bevis. Det påstås først, at f bevarer det indre produkt. Betragt hertil ligningen, jfr (1.1),

$$\langle x, y\rangle = \frac{1}{2}\big(\|x\|^2 + \|y\|^2 - \|x-y\|^2\big).$$

Normen $\|x-y\|$ er afstanden mellem x og y, og den ændres derfor ikke, når x og y erstattes med fx og fy. Da $f0 = 0$, følger det specielt, at $\|fx\| = \|x\|$ og $\|fy\| = \|y\|$. Altså ændres ligningens højreside ikke, når x og y erstattes med fx og fy. Af ligningen følger derfor, at f bevarer det indre produkt.

Den kanoniske basis $(e_1, \dots, e_n)$ for $\mathbb{R}^n$ er en ortonormal basis. Da f bevarer det indre produkt, følger det, at også sættet $(fe_1, \dots, fe_n)$ er en ortonormal basis. Derfor gælder for hver vektor $y \in \mathbb{R}^n$ ligningen,

$$y = \langle y, fe_1\rangle fe_1 + \dots + \langle y, fe_n\rangle fe_n\,. \tag{*}$$

Denne ligning gælder specielt, når $y = fx$ for $x \in \mathbb{R}^n$. Da f bevarer det indre produkt, er $\langle fx, fe_i\rangle = \langle x, e_i\rangle$. Af ligningen (*), for $y := fx$, fås derfor ligningen,

$$fx = \langle x, e_1\rangle fe_1 + \dots + \langle x, e_n\rangle fe_n\,.$$

Af den sidste ligning fremgår, at f er lineær. ∎

(1.8) Opgaver.

1. Vis, at $S^2 = 1$ for enhver matrix $S \in \mathrm{O}^-(2)$. Gælder den samme ligning for matricer i $\mathrm{O}^-(n)$ for $n > 2$?

2. For hvilke værdier af α ligger følgende matrix i $\mathrm{O}^+(3)$:

$$\begin{bmatrix} 2/3 & 1/3 & 2/3 \\ 3\alpha & 0 & -3\alpha \\ -\alpha & 4\alpha & -\alpha \end{bmatrix}.$$

3. Kan du bestemme en matrix i SO(3) således, at alle 9 koefficienter er rationale tal forskellige fra 0 og ± 1?

4. Hvis de første $n - 1$ søjler i en matrix i $\mathrm{SO}(n)$ er givet, hvor mange muligheder er der så for den sidste søjle?

5. Vis, at matricerne i $\mathrm{O}_n(\mathbb{R})$ med heltalskoefficienter udgør en undergruppe, og bestem dens orden.

6. Lad L være linien i $\mathbb{R}^3$ bestemt ved en enhedsvektor e, og lad D være drejningen omkring L med en given vinkel θ. Vis, at

$$D(x) = \langle x, e\rangle e + \cos\theta\,\big(x - \langle x, e\rangle e\big) + \sin\theta\,\big(e \times x\big).$$

[Vink: Lad $L^\perp$ være planen vinkelret på L. Vis, for $x \in \mathbb{R}^3$, at vektoren $x_0 := \langle x, e\rangle e$ er projektionen af x på L, vektoren $x' = x - x_0$ er projektionen af x på $L^\perp$, og vektoren $x'' := e \times x$ er tværvektoren til x' i planen $L^\perp$ set fra e.]

7. For komplekse vektorer (søjler) $x, y \in \mathbb{C}^n$ er *det komplekse skalarprodukt* (*Hermitiske skalarprodukt eller indre produkt*) tallet

$$\langle x, y\rangle := \bar{x}_1 y_1 + \cdots + \bar{x}_n y_n.$$

Bemærk, at $\langle x, y\rangle$ er lineært i y, men „konjugeret" lineært i x. Tallet $\langle x, x\rangle = |x_1|^2 + \cdots + |x_n|^2$ er øjensynlig reelt og ikke-negativt; dets kvadratrod er *normen* af x, altså $\|x\|^2 = \langle x, x\rangle$. I $\mathbb{C}^n$ er vektorer x, y *ortogonale*, hvis $\langle x, y\rangle = 0$, og x er en *enhedsvektor*, hvis $\langle x, x\rangle = 1$. Vis, idet A^* for en matrix A betegner den transponerede, komplekst konjugerede matrix, at

$$\langle x, y\rangle = x^* y.$$

Vis for en kvadratisk matrix $A \in \mathrm{Mat}_n(\mathbb{C})$, at søjlerne i A er enhedsvektorer og parvis ortogonale, hvis og kun hvis $A^*A = 1_n$. En matrix med denne egenskab kaldes *unitær*. Vis, at de unitære matricer udgør en undergruppe $\mathrm{U}_n(\mathbb{C})$ af $\mathrm{GL}_n(\mathbb{C})$. Vis for en unitær matrix A, at $|\det A| = 1$. Genkender du gruppen $\mathrm{U}_1(\mathbb{C})$? Beskriv de unitære (2×2)-matricer. Hvad forstås ved gruppen $\mathrm{SU}_2(\mathbb{C})$?

8. Vis, at gruppen $\mathrm{SO}(2) = \mathrm{O}^+(2)$ er kommutativ. Lad $D_\theta \in \mathrm{O}^+(2)$ være drejningen med vinklen θ og lad $U \in \mathrm{O}(2)$. Vis, at $UD_\theta U^{-1} = D_\theta$ for $U \in \mathrm{O}^+(2)$ og $UD_\theta U^{-1} = D_{-\theta}$ for $U \in \mathrm{O}^-(2)$. Beskriv geometrisk, når U er en spejling (dvs $U \in \mathrm{O}^-(2)$), spejlingen hørende til matricen $D_\theta U D_\theta{}^{-1}$.

2. Flytninger.

(2.1) Hovedsætning. *De isometriske afbildninger $\mathbb{R}^n \to \mathbb{R}^n$ er netop afbildningerne af formen $x \mapsto Ax + b$, hvor A er en ortogonal matrix og b er en vektor i $\mathbb{R}^n$.*

Bevis. En afbildning af formen $x \mapsto Ax + b$ er den sammensatte afbildning $t_b T_A$, hvor T_A er den *lineære afbildning* $x \mapsto Ax$ og t_b er *translationen* $x \mapsto x+b$. Translationen er øjensynlig en isometri. Hvis A er ortogonal, så er T_A en isometri; følgelig er også den sammensatte afbildning $t_b T_A$ en isometri. Hermed er vist, at afbildninger af den anførte form er isometrier.

Antag omvendt, at $f:\mathbb{R}^n \to \mathbb{R}^n$ er en isometri. Sæt $b := f(o)$. Translationen t_{-b} afbilder da $f(o)$ på $f(o)-b = o$. Det følger, at den sammensatte afbildning $t_{-b}f$, dvs $x \mapsto f(x)-b$, har o som fixpunkt. Den sammensatte afbildning er desuden en isometri. Af Lemma (1.7) følger derfor, at den sammensatte afbildning har formen $x \mapsto Ax$ med en ortogonal matrix A. Vi har således for alle x ligningen $f(x) - b = Ax$, og det betyder netop, at afbildningen f har formen $x \mapsto Ax + b$. □

(2.2) Definition. En isometrisk afbildning $f:\mathbb{R}^n \to \mathbb{R}^n$ kaldes også en *flytning*. Ifølge Hovedsætningen er flytningerne netop afbildningerne af formen $x \mapsto Ax + b$, hvor A er ortogonal og $b \in \mathbb{R}^n$. Når A er enhedsmatricen, fås afbildningen $x \mapsto x + b$, der kaldes *translationen* med *forskydning* b; den betegnes t_b. For $b = 0$ fås afbildningen $x \mapsto Ax$, der er den ortogonale afbildning bestemt ved den ortogonale matrix A; den betegnes T_A. Translationer t_b med $b \neq 0$ har ingen fixpunkter. Flytningerne, der har nul-vektoren o som fixpunkt, er ifølge Hovedsætningen netop de ortogonale afbildninger T_A. Det følger, at enhver flytning f er en sammensætning, $f = t_b T_A$, af en ortogonal afbildning T_A og en translation t_b.

Det er klart, at en afbildning, der er sammensat af to flytninger, selv er en flytning. Øjensynlig er den identiske afbildning en flytning. En flytning af formen $x \mapsto Ax+b$ er øjensynlig bijektiv med den inverse bestemt ved $y \mapsto A^{-1}y - A^{-1}b$. Den inverse afbildning er altså ligeledes en flytning. Det er således vist, at flytningerne i $\mathbb{R}^n$ udgør en undergruppe i den fulde permutationsgruppe for $\mathbb{R}^n$. Gruppen af flytninger kaldes den *euklidiske transformationsgruppe* for $\mathbb{R}^n$, og den betegnes $\mathrm{E}(n)$.

Ifølge den associative lov er $x + (b + c) = (x + b) + c$. Heraf følger for translationer ligningen $t_{b+c} = t_c t_b$. Addition af vektorer svarer altså til sammensætning af translationer. Ækvivalent betyder det, at afbildningen, der til en vektor $b \in \mathbb{R}^n$ lader svare translationen t_b, er en homomorfi fra den additive gruppe $\mathbb{R}^n$ til gruppen $\mathrm{E}(n)$. Homomorfien er øjensynlig injektiv. Billedgruppen er *translationsgruppen* $\mathrm{T}(n)$ bestående af alle translationer i $\mathrm{E}(n)$. Translationsgruppen er altså isomorf med den additive gruppe $\mathbb{R}^n$.

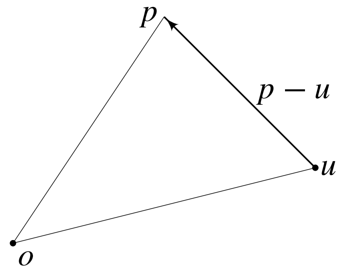
For en flytning $f:\mathbb{R}^n \to \mathbb{R}^n$, af formen $f(x) = Ax + b$, er matricen A og søjlen b entydigt bestemte. Søjlen b er nemlig værdien $f(o)$, og flytningen $x \mapsto f(x) - f(o)$ har o som fixpunkt; den er derfor lineær, og A er den tilhørende matrix. Den ortogonale matrix A siges at være matricen *hørende til* flytningen f, og den betegnes $\bar{f}$. Afbildningen $f \mapsto \bar{f}$, der til en flytning $f(x) = Ax + b$ knytter den tilhørende matrix A, definerer altså en afbildning $\mathrm{E}(n) \to \mathrm{O}(n)$. Denne afbildning er surjektiv, idet matricen A for eksempel hører til flytningen

$x \mapsto Ax$. Yderligere er $f \mapsto \bar{f}$ en homomorfi af grupper. Er nemlig $g(x) = Bx + c$ endnu en flytning, har vi
$$fg(x) = A(Bx + c) + b = ABx + (Ac + b).$$
Heraf fremgår, at matricen hørende til den sammensatte flytning fg er produktet AB af de tilhørende matricer.

At en flytning $f(x) = Ax + b$ ligger i kernen for homomorfien $f \mapsto \bar{f}$, betyder, at A er enhedsmatrix, altså at $f(x) = x + b$ er en translation. Specielt er translationsundergruppen $\mathrm{T}(n)$ en normal undergruppe i $\mathrm{E}(n)$, og af Isomorfisætningen fås en isomorfi,
$$\mathrm{E}(n)/\,\mathrm{T}(n) \xrightarrow{\sim} \mathrm{O}(n).$$

En flytning $x \mapsto Ax + b$ kaldes *egentlig* eller *uegentlig* eftersom determinanten af den tilhørende matrix A er 1 eller -1. De egentlige flytninger udgør øjensynlig en undergruppe, betegnet $\mathrm{E}^+(n)$, af $\mathrm{E}(n)$. De uegentlige flytninger udgør én sideklasse, $\mathrm{E}^-(n)$.

(2.3) Definition. I den geometriske beskrivelse af flytninger tildeles elementerne i $\mathbb{R}^n$ med fordel to roller: som punkter og som vektorer. Flytninger foregår i $\mathbb{R}^n$ opfattet som en mængde af punkter. Vektorer er størrelser, der beskriver eller fastlægger punkterne. At punkter i $\mathbb{R}^n$ *er* vektorer, kan opfattes som beskrivelsen af punkterne set ud fra nulpunktet o i $\mathbb{R}^n$ som origo. En anden beskrivelse fås ved at *translatere nulpunktet*, dvs ved at vælge et andet fast punkt u som *origo*. Efter et sådant valg beskrives et punkt p i $\mathbb{R}^n$ set fra origo u ved sin *stedvektor*, som blot er differensen $p - u$.



En flytning f i $\mathbb{R}^n$ kan fastlægges ved, hvordan den ændrer stedvektorerne ud fra et fast valgt punkt u som origo. Antag, at f er givet på formen $x \mapsto Ax + b$. Beskrivelsen af f set ud fra origo u angiver, hvordan stedvektoren $f(p) - u$ afhænger af stedvektoren $p - u$. Øjensynlig er
$$f(p) - u = Ap + b - u = A(p - u) + b + Au - u.$$
Stedvektoren for billedpunktet $f(p)$ fås altså ved at anvende afbildningen f' bestemt ved $x \mapsto Ax + b + Au - u$ på stedvektoren for p. Afbildningen f', der beskriver f ud fra punktet u som origo, er altså selv en flytning, nemlig afbildningen $x \mapsto Ax + b'$, hvor $b' = b + Au - u$. Øjensynlig har f og f' samme tilhørende matrix A. Det ses let, at $f' = t_u^{-1} f t_u$. Flytninger af formen $f' = t_u^{-1} f t_u$, for $u \in \mathbb{R}^n$, siges også at være *translationsækvivalente* med f.

Hvis det nye origo u kan vælges som fixpunkt for f, får den ækvivalente flytning f' den simple form $x \mapsto Ax$. Punktet u er fixpunkt for den oprindelige afbildning $f(x) = Ax + b$, hvis og kun hvis $Au + b = u$, dvs hvis og kun hvis $(1 - A)u = b$. Det er derfor af vigtighed at undersøge billedrummet for den lineære afbildning $x \mapsto (1 - A)x$.

(2.4) Lemma. *Lad $T:\mathbb{R}^n \to \mathbb{R}^n$ være en ortogonal lineær afbildning, og betragt den lineære afbildning $1-T$, altså $x \mapsto x-Tx$. Lad V være kernen for $1-T$ og lad W være billedrummet. Da er W det ortogonale komplement til V.*

Bevis. Det ortogonale komplement $V^\perp$ består af de vektorer w, der opfylder, at $\langle w, v\rangle = 0$ for alle $v \in V$. Det er velkendt, at hver vektor $x \in \mathbb{R}^n$ entydigt kan skrives som en sum,

$$x = v + v', \quad \text{hvor } v \in V,\ v' \in V^\perp; \tag{*}$$

vektoren v er den ortogonale projektion af x på V.

Det er påstanden, at $W = V^\perp$. Hertil bemærkes først, at underrummet $V^\perp$ er invariant under T. Antag nemlig, at $w \in V^\perp$. For hver vektor $v \in V$ er $Tv = v$, og dermed er $\langle Tw, v\rangle = \langle Tw, Tv\rangle = \langle w, v\rangle = 0$. Altså er $Tw \in V^\perp$.

Lad nu $x \in \mathbb{R}^n$. Skriv x på formen (*), og anvend den lineære afbildning $1 - T$ på x. Da $v \in V$, har vi $(1 - T)v = 0$. Altså er $x - Tx = v' - Tv'$. Da $V^\perp$ er invariant under T, følger det, at $x - Tx \in V^\perp$. Billedrummet for $1 - T$ er altså indeholdt i $V^\perp$, dvs $W \subseteq V^\perp$. For at vise den omvendte inklusion bemærkes, at den lineære afbildning $1 - T$ ved restriktion definerer en lineær afbildning $(1 - T)|V^\perp$ af vektorrummet $V^\perp$ ind i sig selv. Den er injektiv, idet dens kerne består af de vektorer $w \in V^\perp$ for hvilke $w = Tw$. Kernen er derfor fællesmængden $V^\perp \cap V$, som kun indeholder nul-vektoren. Da den lineære afbildning $(1 - T)|V^\perp$ er injektiv, er den også surjektiv. Specielt er $V^\perp$ indeholdt i billedrummet for $1 - T$. ▯

(2.5) Sætning. *Enhver flytning i $\mathbb{R}^n$ er translationsækvivalent med en flytning $x \mapsto Ax + c$, hvor vektoren c opfylder, at $Ac = c$.*

Bevis. Betragt en given flytning f, af formen $f(x) = Ax + b$. Det fremgår af (2.3), at de med f ækvivalente flytninger har formen,

$$x \mapsto Ax + b + Au - u,$$

for $u \in \mathbb{R}^n$. Det skal altså vises, at u kan vælges således, at vektoren $c := b + Au - u$ opfylder $Ac = c$. Med notationen i Lemma (2.4) (og $T := T_A$) skal det altså vises, at u kan vælges således, at $b + Au - u$ tilhører V. Hertil skrives $b = v + v'$, hvor $v \in V$ og $v' \in V^\perp$. Ifølge (2.4) ligger v' i billedrummet for $1 - T$, så vi kan skrive $v' = u - Au$ med en vektor $u \in \mathbb{R}^n$. Herefter ligger $b + Au - u = b - v' = v$ i underrummet V, som ønsket. ▯

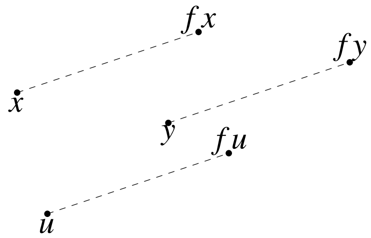
(2.6) Planens flytninger. *Enhver egentlig flytning i planen $\mathbb{R}^2$ er enten*

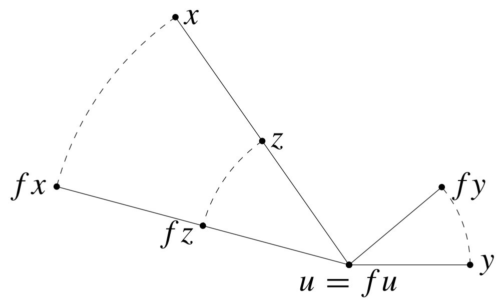
(1) *en translation, eller*
(2) *en drejning omkring et punkt.*

Enhver uegentlig flytning i planen $\mathbb{R}^2$ er enten

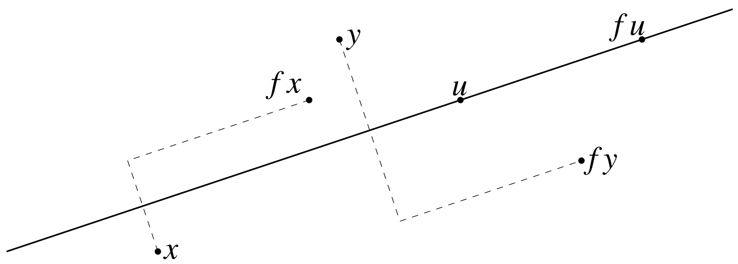
(3) *en spejling i en linie, eller*
(4) *en glidespejling, dvs en spejling i en linie efterfulgt af en translation i liniens retning.*

Bevis. En flytning f i planen har nemlig formen $x \mapsto Ax+b$, hvor $A \in \mathrm{O}(2)$. Ifølge Sætning (2.5) kan vi, efter en translation af origo, antage, at $Ab = b$. Betragt først tilfældet, hvor flytningen er egentlig, dvs $A \in \mathrm{O}^+(2)$. Da er A en *drejningsmatrix*, dvs af formen $A = D_\theta$ i (1.3). Hvis A er enhedsmatrix, så er $f(x) = x + b$, dvs f er en translation. Hvis A ikke er enhedsmatrix, så er drejningsvinklen θ ikke et heltalsmultiplum af 2π, og nul-vektoren er den eneste fiksvektor for A. Af $Ab = b$ følger derfor, at $b = 0$. Altså er $f(x) = D_\theta x$, dvs f er en drejning med vinklen θ omkring det valgte origo u.





Betragt dernæst tilfældet, hvor flytningen er uegentlig. Da er A en *spejlingsmatrix*, dvs af formen $A = S_\theta$ i (1.3). Tallet 1 er egenværdi for A, og det tilhørende egenrum er 1-dimensionalt, altså en linie gennem origo. Matricen $A = S_\theta$ beskriver da spejlingen i linien, og f er denne spejling efterfulgt af translation med b. Da $Ab = b$, ligger b i egenrummet hørende til egenværdien 1; translationsretningen b er altså parallel med linien.



Hermed er påstanden bevist. ∎

Det er lidt en smagssag, om man vil kræve at en drejning ikke er identiteten (dvs at drejningsvinklen ikke er et multiplum af 2π), og at en glidespejling ikke er en spejling (dvs at translationen i spejlingsliniens retning ikke er identiteten). Hvis man stiller disse krav (og det gør vi!), er de fire klasser af flytninger i planen disjunkte.

En række kvalitative egenskaber ved planens flytninger fremgår af klassifikationen og de foregående overvejelser: *En sammensætning af en drejning og en translation er altid en drejning. En sammensætning af to drejninger (om samme punkt eller om to forskellige punkter) er en translation, hvis de to drejningsvinkler er modsatte, og ellers en drejning. En sammensætning af to glidespejlinger (spejlinger medregnet) er en translation, hvis de to spejlingsakser er parallelle, og ellers en drejning.*

Betragt nemlig to flytninger $fx = Ax + b$ og $gx = Cx + d$. Matricen hørende til den sammensatte flytning fg er matricen AC. Hvis den ene flytning er en translation og den anden er en drejning, så er den ene matrix enhedsmatricen 1 og den anden ligger i $\mathrm{O}^+(2)$;

altså er $AC \in \mathrm{O}^+(2)$, så fg er en drejning. Hvis begge flytninger er drejninger, så ligger begge matricer i $\mathrm{O}^+(2)$; altså er $AC \in \mathrm{O}^+(2)$, så fg er en drejning, med mindre $AC = 1$. Det sidste indtræffer, netop når $C = A^{-1}$, altså netop når drejningerne f og g har modsatte drejningsvinkler. Hvis begge flytninger er glidespejlinger, så ligger begge matricer i $\mathrm{O}^-(2)$; altså er $AC \in \mathrm{O}^+(2)$, så fg er en drejning, med mindre $AC = 1$. Det sidste indtræffer, netop når $C = A$ (idet vi har $A^2 = 1$ for alle matricer i $\mathrm{O}^-(2)$), altså netop når glidespejlingerne f og g har parallelle akser.

(2.7) Rummets flytninger. *Enhver egentlig flytning i $\mathbb{R}^3$ er enten*

(1) *en translation, eller*
(2) *en drejning omkring en linie, eller*
(3) *en skruning, dvs en drejning omkring en linie efterfulgt af en translation i liniens retning.*

Enhver uegentlig flytning i $\mathbb{R}^3$ er enten

(4) *en spejling i en plan, eller*
(5) *en drejespejling, dvs en spejling i en plan efterfulgt af en drejning omkring en linie vinkelret på planen, eller*
(6) *en glidespejling, dvs en spejling i en plan efterfulgt af en translation parallel med planen.*

Bevis. Betragt nemlig en flytning f i $\mathrm{E}(3)$. Som for planen kan vi antage, at f har formen $x \mapsto Ax+b$, hvor $Ab = b$. Det følger af Sætning (1.6), at den ortogonale afbildning $x \mapsto Ax$ i en passende ortonormal basis (e_1, e_2, e) for $\mathbb{R}^3$ beskrives ved en matrix af formen angivet i (1.6). Vi kan antage, at $0 \leqslant \theta < 2\pi$. Matricens determinant er lig med ε, så flytningen er egentlig, hvis og kun hvis $\varepsilon = 1$.

Antag først, at f er en egentlig flytning, altså at $\varepsilon = 1$. Hvis $\theta = 0$, så er A enhedsmatricen, og f er translationen $x \mapsto x+b$. Antag derfor, at $\theta > 0$. Afbildningen $x \mapsto Ax$ beskriver da en *drejning* om linien gennem origo bestemt ved vektoren e. Øjensynlig er denne linie netop egenrummet svarende til egenværdien 1, så betingelsen $Ab = b$ medfører, at b er proportional med e. Hvis $b = 0$, så er f blot drejningen $x \mapsto Ax$, og hvis $b \neq 0$, så er f sammensat af drejningen og translation med b, som er en vektor parallel med drejningsaksen.

Antag dernæst, at f er en uegentlig flytning, altså at $\varepsilon = -1$. Betragt først tilfældet $\theta = 0$. Her er egenrummet for A hørende til egenværdien 1 netop planen V udspændt af e_1 og e_2. Af $Ab = b$ følger således, at $b \in V$. Hvis $b = 0$, så er $f(x) = Ax$ *spejlingen* i planen V. Hvis $b \neq 0$, så er f sammensat af spejlingen og translation med b, som ligger i planen V. I dette tilfælde er f altså en glidespejling.

Betragt endelig tilfældet, hvor $\theta \neq 0$. Her er 1 ikke egenværdi for A. Af $Ab = b$ følger således, at $b = 0$. Altså er f sammensat af en drejning med vinklen θ omkring linien bestemt ved e og spejlingen i planen vinkelret på linien. I dette tilfælde er f altså en drejespejling. □

Blandt drejningerne er medregnet halvdrejningen om en linie, der også kan opfattes som spejlingen i linien. Spejlinger i en linie er altså egentlige flytninger i $\mathbb{R}^3$.

Tilsvarende er blandt drejespejlingerne medregnet halvdrejningen om en linie efterfulgt af en spejling i en plan vinkelret på linien. En sådan flytning kan opfattes som en spejling i skæringspunktet mellem linien og planen. Punktspejlinger er af formen $x \mapsto -x + b$. De er uegentlige flytninger i $\mathbb{R}^3$.

(2.8) Lemma. *Lad $\{p_1, \dots, p_k\}$ være en endelig delmængde af $\mathbb{R}^n$ bestående af $k \geqslant 1$ forskellige punkter. Enhver flytning $f \in \mathrm{E}(n)$ vil da afbilde tyngdepunktet for punkterne p_i,*

$$m := \frac{1}{k} \sum_{i=1}^{k} p_i,$$

på tyngdepunktet for billedpunkterne $f(p_i)$.

Bevis. Hvis f er lineær, altså af formen $f(x) = Ax$, følger påstanden umiddelbart af lineariteten.

Hvis f er en translation, altså af formen $f(x) = x + b$, følger påstanden af ligningerne,

$$\frac{1}{k}\Big(\sum_{i=1}^{k} p_i\Big) + b = \frac{1}{k}\Big(\sum_{i=1}^{k} p_i\Big) + \frac{1}{k}kb = \frac{1}{k}\sum_{i=1}^{k}(p_i + b).$$

Heraf følger påstanden i almindelighed, da en flytning f er en sammensætning af en lineær afbildning og en translation. ▯

(2.9) Sætning. *For enhver endelig undergruppe G af $\mathrm{E}(n)$ gælder, at flytningerne i G har et fælles fixpunkt.*

Bevis. Betragt et vilkårligt punkt p i $\mathbb{R}^n$. Da gruppen G er endelig, udgør billederne $g(p)$, for $g \in G$, en endelig mængde af punkter $\{p_1, \dots, p_k\}$. Det påstås, at tyngdepunktet for punkterne p_i er fixpunkt for alle flytninger i G. Antag, at $f \in G$. For hvert j har vi $p_j = g(p)$ med $g \in G$, og dermed $f(p_j) = fg(p)$. Da G er en gruppe, er $fg \in G$. Billedpunktet $f(p_j)$ er altså igen et af punkterne p_i. Af Lemma (2.8) følger derfor, at tyngdepunktet for punkterne p_i er fixpunkt for f. ▯

(2.10) Definition. En undergruppe G af $\mathrm{E}(n)$ kaldes en *punktgruppe*, hvis der findes et punkt u i $\mathbb{R}^n$, som er fixpunkt for alle flytningerne i G. Hvis G er en punktgruppe, kan vi efter en translation, dvs ved at vælge fixpunktet u som nyt origo, antage at alle flytninger i G har nul-vektoren som fixpunkt. Flytningerne i G er herefter lineære, dvs G er en undergruppe af den ortogonale gruppe $\mathrm{O}(n)$. Punktgrupper af flytninger svarer således til undergrupper af den ortogonale gruppe $\mathrm{O}(n)$.

Det følger af Sætning (2.9), at enhver endelig gruppe af flytninger er en punktgruppe.

(2.11) Opgaver.

1. Betragt i planen flytningen sammensat af to drejninger omkring to forskellige punkter. Hvis de to drejningsvinkler ikke er modsatte, er flytningen igen en drejning; hvordan bestemmes fixpunktet? Hvis de to drejningsvinkler er modsatte, er flytningen en translation; hvordan bestemmes translationsvektoren?

2. Betragt i planen flytningen sammensat af spejlinger i to forskellige linier. Hvis de to linier ikke er parallelle, er flytningen en drejning; hvordan bestemmes fixpunktet og drejningsvinklen? Hvis de to linier er parallelle, er flytningen en translation; hvordan bestemmes translationsvektoren?

3. Vis, at enhver flytning i planen kan fås som en sammensætning af højst 3 spejlinger.

4. Vis, at $(n+1) \times (n+1)$-matricerne af følgende form,

$$\begin{bmatrix} A & v \\ 0 & 1 \end{bmatrix},$$

hvor $A \in \mathrm{O}(n)$ og $v \in \mathbb{R}^n$ er en søjlevektor, udgør en undergruppe af $\mathrm{GL}_{n+1}(\mathbb{R})$. Vis, at denne undergruppe er isomorf med $\mathrm{E}(n)$.

5. Antag, at en begrænset, ikke-tom delmængde $K \subseteq \mathbb{R}^n$ er invariant under flytningen T. Vis, at T har et fixpunkt. [Vink: Efter en translation af origo kan T kan skrives på formen $T(x) = Ax + c$, hvor $Ac = c$. Udnyt, at der så gælder $T^k(x) = A^k x + kc$, og lad $k \to \infty$ for $x \in K$.]

6. Betragt en gruppe $G \subseteq \mathrm{E}(2)$ af plane flytninger. Antag, at hver flytning $g \in G$ har et fixpunkt. Vis, at G er en punktgruppe, altså at flytningerne i G har et fælles fixpunkt. [Vink: Af antagelsen følger, at G ikke kan indeholde translationer eller glidespejlinger. Den sammensatte af to spejlinger er en translation eller en drejning. Derfor kan det antages, at G indeholder en drejning g, lad os sige med vinklen θ omkring drejningscentret p. Betragt en vilkårlig flytning h i G. Det skal vises, at $h(p) = p$. Antag først, at h er egentlig, og altså en drejning. Så er $hgh^{-1}g^{-1}$ en translation og derfor lig med identiteten. Altså er $hgh^{-1} = g$. På den anden side er hgh^{-1} en drejning omkring $h(p)$ med vinklen θ. Af $hgh^{-1} = g$ følger, at de to drejningscentre er ens: $h(p) = p$. Antag i stedet, at h er uegentlig, og altså en spejling. Så følger det tilsvarende, at $hgh^{-1} = g^{-1}$, og igen bliver de to drejningscentre ens: $h(p) = p$.]

7. Betragt i rummet to drejninger d_1 og d_2 omkring forskellige akser l_1 og l_2, og lad $d = d_1 d_2$ være den sammensatte flytning. Vis, at hvis de to akser l_1 og l_2 skærer hinanden i et punkt, så er d en drejning omkring en akse gennem dette punkt og ikke planen bestemt ved l_1 og l_2. Vis, at hvis l_1 og l_2 er parallelle, så er d en drejning omkring en tredie akse parallel med l_1 og l_2. Vis, at hvis l_1 og l_2 er vindskæve (dvs ikke ligger i samme plan), så er d en skruning. [Vink til det tredie tilfælde: Betragt et punkt p på l_2. Da er $d_2(p) = p$, og altså $d(p) = d_1(p)$. Hvis d var en drejning, lad os sige med akse l, ville l ligge på midtnormalen for $p\,d(p)$, og altså på midtnormalen for $p\,d_1(p)$. Denne midtnormal indeholder aksen l_1; altså vil l og l_1 ligge i samme plan, men så er ligningen $d_2 = {d_1}^{-1} d$ i modstrid med de to først behandlede tilfælde.]

8. *Betragt en gruppe $G \subseteq \mathrm{E}(3)$ af flytninger i rummet. Antag, at hver flytning $g \in G$ har et fixpunkt. Vis, at G er en punktgruppe, altså at flytningerne i G har et fælles fixpunkt. [Vink: Af antagelsen følger, at G ikke kan indeholde translationer, skruninger eller glidespejlinger. Betragt akserne for drejningerne i G. Udeluk (ud fra det plane tilfælde), at der kan være to parallelle akser. Udeluk, at der kan være to vindskæve akser. Slut så først, at akserne skærer hinanden to og to, og dernæst at de skærer hinanden i samme punkt.

Hvis der er (dreje)spejlinger $h \in G$, udnyttes blot, at hvis p er fælles fixpunkt for alle drejninger i G, så har $h(p)$ den samme egenskab.]

3. Symmetrier.

(3.1) Definition. De vigtigste flytningsgrupper i $\mathbb{R}^n$ er de såkaldte *symmetrigrupper*. Betragt en ikke-tom delmængde $K \subseteq \mathbb{R}^n$. Ved en *symmetri* af K forstås en flytning $f \in \mathrm{E}(n)$ som opfylder, at $f(K) = K$. Det er klart, at symmetrierne af K udgør en undergruppe $\mathrm{E}(K)$ af $\mathrm{E}(n)$ og at de *egentlige symmetrier* af K, dvs de symmetrier af K som er egentlige flytninger, udgør en undergruppe $\mathrm{E}^+(K)$ af $\mathrm{E}^+(n)$.

(3.2) Observation. Antag, at delmængden K er endelig. En symmetri af K er specielt en permutation af punkterne i K. Af Lemma (2.8) følger derfor, at alle symmetrier af K vil have tyngdepunktet for K som fixpunkt. Specielt er symmetrigruppen $\mathrm{E}(K)$ altså en punktgruppe. Efter en translation af origo kan det antages, at det fælles fixpunkt er nulpunktet i $\mathbb{R}^n$. Efter denne antagelse er alle symmetrier af K altså lineære, dvs af formen $x \mapsto Ax$ med en ortogonal matrix A. Symmetrigruppen $\mathrm{E}(K)$ kan derfor opfattes som en undergruppe i den ortogonale gruppe $\mathrm{O}(n)$.

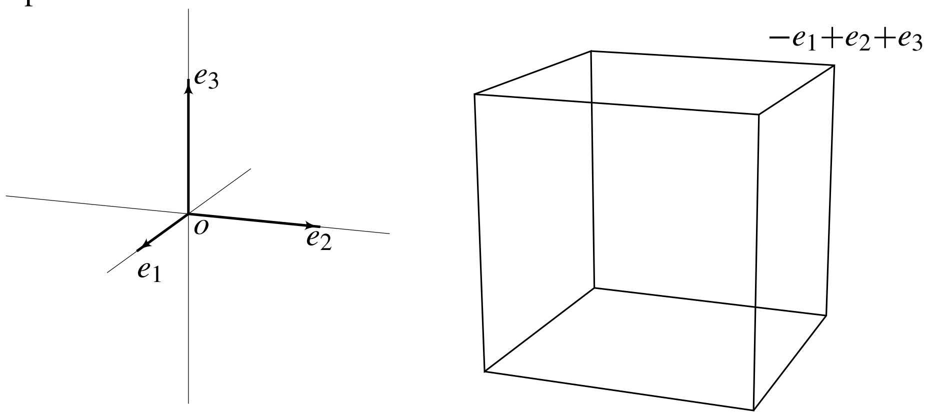
Antag yderligere, at K ikke er indeholdt i noget ægte underrum af vektorrummet $\mathbb{R}^n$. Da er symmetrigruppen $\mathrm{E}(K)$ endelig. Ifølge antagelsen findes nemlig blandt vektorerne i K en basis $(e_1, \dots, e_n)$ for $\mathbb{R}^n$. Enhver lineær afbildning $f : \mathbb{R}^n \to \mathbb{R}^n$ er så helt bestemt ved billedvektorerne $fe_1, \dots, fe_n$. Hvis f er en symmetri af K, ligger disse billedvektorer igen i K. Der er derfor kun endelig mange mulige billedvektorer, og specielt kun endelig mange symmetrier. Af argumentet følger i øvrigt, at tallet $|K|^n$ er en øvre grænse for ordenen af symmetrigruppen $\mathrm{E}(K)$.

(3.3) Eksempel. Betragt for $k \geqslant 3$ en regulær k-kant i $\mathbb{R}^2$, jfr Eksempel (1.4). Mængden K af hjørner består af de k vektorer $e_j = D^j e$ for $j = 0, 1, \dots, k-1$, der kan fås ved at dreje en given enhedsvektor e med en vinkel, der er et multiplum af $2\pi/k$. Tyngdepunktet for hjørnerne er nul-vektoren, så symmetrierne af K er lineære. Symmetrigruppen $\mathrm{E}(K)$ er altså en undergruppe i $\mathrm{O}(2)$. De to vektorer e_0 og e_1 er en basis for $\mathbb{R}^2$. En symmetri f af K er således bestemt ved de to billeder fe_0 og fe_1. Mulighederne for fe_0 er de k vektorer e_j for $j = 0, \dots, k-1$, og hvis $fe_0 = e_i$, så må fe_1 være en af de to vektorer i K, der ligger nærmest ved e_i. Der er således højst $k \cdot 2$ symmetrier af K. På den anden side er det klart, at de $2k$ matricer D^j og $D^j S$, jfr (1.4), definerer symmetrier af K. Symmetrigruppen $\mathrm{E}(K)$ er altså diedergruppen D_k. Gruppen $\mathrm{E}^+(K)$ af egentlige symmetrier er den cykliske undergruppe C_k.

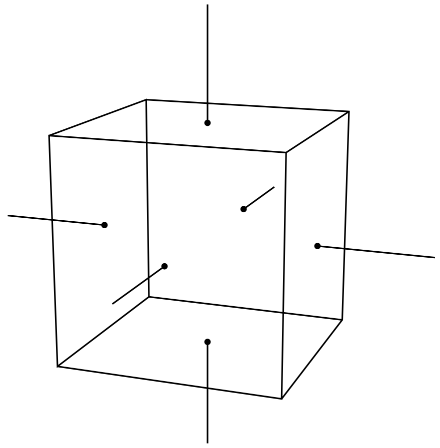
Beskrivelsen af symmetrigruppen gælder øjensynlig også for $k = 2$, hvor $K = \{\pm e\}$. Tilfældet $k = 1$ kræver en særlig definition. Her defineres diedergruppen D_1 som den (cykliske) undergruppe af orden 2, der frembringes af spejlingen S. Bemærk, at D_1 ikke er symmetrigruppen for $\{e\}$.

(3.4) Hexaedergruppen. Lad (e_1, e_2, e_3) være den kanoniske basis for $\mathbb{R}^3$. De seks vektorer i mængden $K = \{\pm e_1, \pm e_2, \pm e_3\}$ kan opfattes som midtpunkterne af siderne i et *hexaeder* (*terning*) H. Hexaederets hjørner er de 8 vektorer af formen $\pm e_1 \pm e_2 \pm e_3$. Det er klart, at symmetrigruppen for hexaederet er symmetrigruppen for mængden K af sidemidtpunkterne. Tyngdepunktet for disse midtpunkter er nul-vektoren, så symmetrierne af hexaederet er lineære. Symmetrigruppen $\mathrm{E}(H)$ er altså en undergruppe af $\mathrm{O}(3)$.

Vektorerne e_1, e_2, e_3 er en basis for $\mathbb{R}^3$, så en symmetri f af K er helt bestemt ved billederne fe_1, fe_2, fe_3. Billedvektoren fe_1 kan være en vilkårlig af de 6 vektorer i K. Billedvektoren fe_2 skal være ortogonal på fe_1, så for hvert valg af fe_1 er der 4 muligheder for fe_2. Tilsvarende er der for hvert valg af fe_1 og fe_2 præcis 2 muligheder for fe_3. Der er således højst $6{\cdot}4{\cdot}2 = 48$ mulige valg af fe_1, fe_2, fe_3. På den anden side gælder for hvert af de mulige valg, at (fe_1, fe_2, fe_3) er en ortonormal basis for $\mathbb{R}^3$, og dermed er den tilsvarende lineære afbildning f ortogonal. Symmetrigruppen $\mathrm{E}(K) = \mathrm{E}(H)$ har derfor orden 48. Det er klart, at der blandt de 48 flytninger også findes spejlinger. Gruppen $\mathrm{E}^+(H)$ bestående af egentlige symmetrier af H har derfor orden 24. Det er den sidste gruppe, der normalt kaldes *Hexaedergruppen*. Den betegnes H. Flytningerne i Hexaedergruppen er drejninger om akser gennem nulpunktet.



Det er let at identificere akserne for drejningerne i Hexaedergruppen. Koordinatakserne er de 3 *fladeakser* (dvs linier gennem origo og midtpunktet af en side); det er klart, at drejningerne på $\pi/2$, π og $-\pi/2$ omkring en af disse akser er symmetrier af hexaederet.

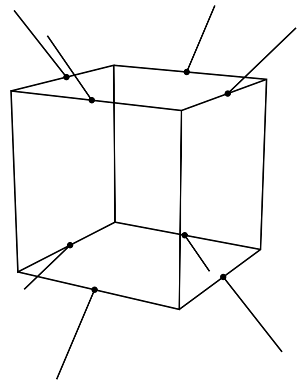


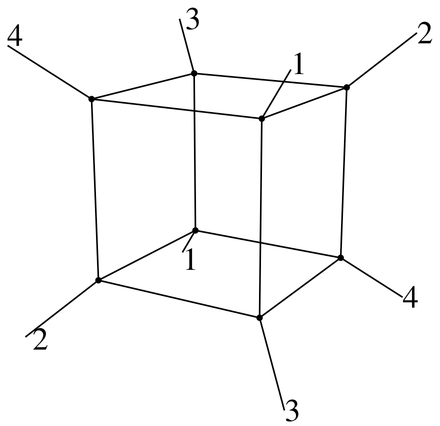
Videre er der 6 *kantakser* (dvs linier gennem origo og midtpunktet af en kant); det er klart, at halvdrejningen (dvs drejningen med vinklen π) omkring en af disse akser er en symmetri af hexaederet. Endelig er der 4 *hjørneakser* (dvs linier gennem origo og et hjørne); det er klart, at drejningerne på $2\pi/3$ og $-2\pi/3$ omkring en af disse akser er symmetrier af hexaederet.

Der er 3 fladeakser, 6 kantakser, og 4 hjørneakser. Af drejninger om disse akser er der således bestemt i alt

$$3 \cdot 3 + 6 \cdot 1 + 4 \cdot 2 = 23.$$

Øjensynlig er så identiteten den sidste symmetri i Hexaedergruppen.





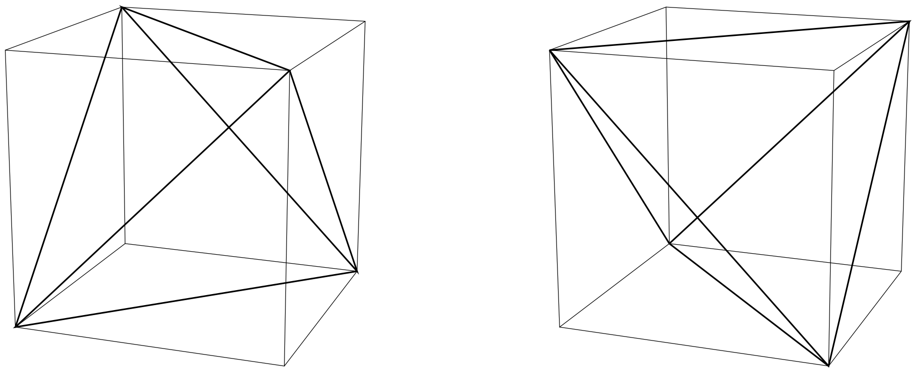
(3.5). Enhver symmetri af hexaederet permuterer de 4 hjørneakser. Herved fås en homomorfi fra Hexaedergruppen til gruppen af permutationer af de 4 hjørneakser, dvs til den symmetriske gruppe S_4. Det er nemt at se, at enhver transposition af hjørneakserne kan opnås ved en halvdrejning omkring en kantakse. Da S_4 er frembragt af transpositionerne, følger det, at homomorfien er surjektiv. Da begge grupper har orden 24, er homomorfien en isomorfi. Hexaedergruppen er altså isomorf med den symmetriske gruppe S_4.

akse	drejningsvinkel	antal	type
f	$\pm\pi/2$	$3 \cdot 2$	4^1
k	π	$6 \cdot 1$	$1^2 2^1$
h	$\pm 2\pi/3$	$4 \cdot 2$	$1^1 3^1$
f	π	$3 \cdot 1$	2^2
	identiteten	1	1^4

I tabellen herover er angivet cykeltypen af de permutationer i S_4, der svarer til drejningerne i Hexaedergruppen. Bogstaverne h, k, og f refererer til hjørneakser, kantakser og (side)fladeakser. Fx svarer drejningen på $2\pi/3$ omkring hjørneaksen med nummeret 2, orienteret ved vektoren $-e_1 + e_2 + e_3$, til 3-cyklen $(1\,4\,3)$. Permutationen er et produkt af en 1-cykel og en 3-cykel, altså af type $1^1 3^1$.

(3.6). Enhver symmetri af hexaederet permuterer de 3 fladeakser. Herved fås en homomorfi fra Hexaedergruppen til gruppen af permutationer af de 3 akser, dvs til den symmetriske gruppe S_3. Det er nemt at se, at enhver transposition af fladeakserne kan opnås ved en halvdrejning omkring en kantakse. Da S_3 er frembragt af transpositioner, følger det, at homomorfien er surjektiv. Homomorfiens kerne kaldes *Klein's Vierer-gruppe*, og den betegnes V. Den har orden $24/6 = 4$ ifølge Isomorfisætningen. Der er 3 halvdrejninger omkring en fladeakse, og disse halvdrejninger ligger øjensynlig i kernen. Det følger, at Klein's Vierer-gruppe består af identiteten og de tre halvdrejninger. Symmetrierne i V svarer til de to nederste rækker i tabellen i (3.5).

(3.7). Hexaederets 8 hjørner kan deles i to lige store delmængder, som udgør hjørnerne i to regulære *tetraedre* Δ og Δ'.



De fire hjørner i tetraederet Δ fås ud fra et enkelt hjørne i Δ ved at anvende drejningerne i Klein's Vierer-gruppe V. De 6 kanter i Δ er diagonaler i hexaederets sideflader. Hjørnerne i Δ' har formen $-v$, hvor $v \in \Delta$.

Enhver symmetri af hexaederet permuterer mængden $\{\Delta, \Delta'\}$ bestående af de to tetraedre. Herved fås en homomorfi fra gruppen $\mathrm{E}(H)$ til gruppen af permutationer af de to tetraedre, dvs til den cykliske gruppe $\mathrm{S}_2 = \mathrm{C}_2$ af orden 2. Kernen for denne homomorfi består af symmetrier f, som opfylder $f(\Delta) = \Delta$. Homomorfien er øjensynlig surjektiv, så ifølge Isomorfisætningen er kernen en normal undergruppe af index 2 i $\mathrm{E}(H)$. Specielt er kernen en gruppe af orden 24.

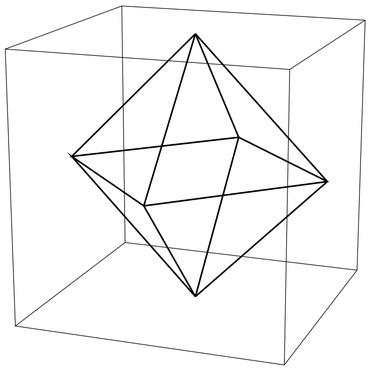
Ved restriktion fås en homomorfi fra Hexaedergruppen $\mathrm{E}^+(H)$ til C_2. Også restriktionen er surjektiv, idet fx en drejning med vinklen $\pi/2$ om en koordinatakse fører Δ over i Δ'. Kernen for restriktionen er altså en normal undergruppe af orden 12 i Hexaedergruppen. Det er nemt at se, at de 12 symmetrier af hexaederet, der svarer til de 3 nederste rækker i tabellen i (3.5), ligger i kernen, så de udgør derfor kernen. Under isomorfien mellem Hexaedergruppen og S_4 svarer denne kerne til den alternerende gruppe A_4.

(3.8) Tetraedergruppen. Betragt de 4 hjørner i delmængden Δ beskrevet i (3.7). De udgør hjørnerne i et regulært tetraeder. Hjørnernes tyngdepunkt er øjensynlig nul-vektoren, så symmetrierne af Δ er lineære. Vilkårligt valgte 3 vektorer d_1, d_2, d_3 ud af de fire vektorer i Δ udgør en basis for $\mathbb{R}^3$. En symmetri f af Δ er derfor bestemt ved sine billeder fd_1, fd_2, fd_3. Billedet fd_1 kan være en vilkårlig af de fire vektorer i Δ, billedet fd_2 skal være forskelligt fra fd_1 og billedet fd_3 skal være forskelligt fra fd_1 og fd_2. Der er derfor højst $4{\cdot}3{\cdot}2 = 24$ forskellige symmetrier af Δ. På den anden side har vi i (3.7) bestemt en undergruppe af isometrier f af H, som opfylder $f(\Delta) = \Delta$. Denne undergruppe, af orden 24, må derfor være symmetrigruppen for tetraederet Δ.

Symmetrierne af Δ er specielt permutationer af hjørnerne i Δ. Der er 4 hjørner og 24 symmetrier. Heraf ses, at den fulde symmetrigruppe $\mathrm{E}(\Delta)$ for tetraederet er isomorf med den symmetriske gruppe S_4.

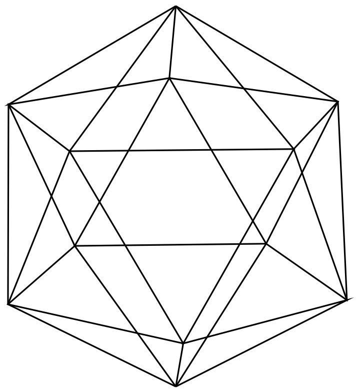
Blandt de 24 symmetrier af Δ findes spejlinger. Gruppen $\mathrm{E}^+(\Delta)$ bestående af egentlige symmetrier af Δ har derfor orden 12. Det er den sidste gruppe, der normalt kaldes *Tetraedergruppen*; den betegnes T. Den er en undergruppe af index 2 i gruppen $\mathrm{E}(\Delta)$, og $\mathrm{E}(\Delta)$ er isomorf med S_4. Tetraedergruppen er derfor isomorf med den alternerende gruppe A_4. I (3.7) har vi identificeret Tetraedergruppen med en undergruppe i Hexaedergruppen, nemlig med undergruppen svarende til de 12 symmetrier angivet i de tre nederste rækker i tabellen i (3.5).

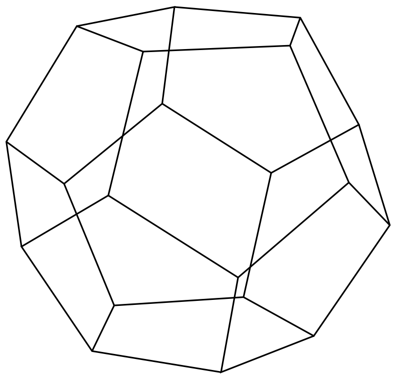
(3.9) Oktaedergruppen. Betragt mængden $K = \{\pm e_1, \pm e_2, \pm e_3\}$, beskrevet i (3.4). De 6 vektorer i K udgør midtpunkterne af hexaederets seks sideflader. De kan opfattes som hjørnerne i et regulært *oktaeder*.



I (3.4) har vi identificeret gruppen af symmetrier af hexaederet med symmetrigruppen $\mathrm{E}(K)$. Hexaederet og det indskrevne oktaeder har altså de samme symmetrier. Specielt kan Hexaedergruppen identificeres med gruppen af egentlige symmetrier af oktaederet. Den kaldes derfor også *Oktaedergruppen*, og den betegnes både O og H.

(3.10) Ikosaedergruppen og Dodekaedergruppen. De beskrevne rumlige figurer, tetraederet, hexaederet og oktaederet, er såkaldte *regulære polyedre*. Tetraederet er en 4-side og de fire sideflader er regulære 3-kanter. Hexaederet er en 6-side, og de seks sideflader er regulære 4-kanter, dvs kvadrater. Oktaederet er en 8-side, og de otte sideflader er regulære 3-kanter.





Der findes yderligere to regulære polyedre i rummet, nemlig *ikosaederet* og *dodekaederet*. Ikosaederet er en 20-side, og de tyve sideflader er regulære 3-kanter. Dodekaederet er en 12-side, og de tolv sideflader er regulære 5-kanter. Man kan vise, at ikosaederet og dodekaederet har den samme gruppe af symmetrier. Undergruppen af egentlige symmetrier, der kan kaldes *Ikosaedergruppen* eller *Dodekaedergruppen*, er isomorf med den alternerende gruppe A_5 af orden 60. Den betegnes ofte I.

Endelig skal det nævnes, at en (plan) regulær k-kant i rummet kan opfattes som et *dieder*, en 2-side. Diederet har to (sammenfaldende) sider, der er regulære k-kanter. De plane symmetrier af k-kanten er dels drejninger, der kan opfattes som drejninger i rummet om en akse vinkelret på k-kanten, dels spejlinger, der kan opfattes som halvdrejninger i rummet. Diedergruppen D_k kan altså opfattes som gruppen af egentlige (rumlige) symmetrier af et dieder, hvis side er en regulær k-kant.

(3.11) Opgaver.

1. Bestem symmetrigruppen for et skakbræt.

2. Bestem symmetrigruppen for en (uendelig) jernstang med gevind.

3. Bestem symmetrigruppen for kugleskallen. Bestem symmetrigruppen for en ellipsoide.

4. Bestem symmetrigruppen for en valnød og for en hasselnød.

5. Bestem symmetrigruppen for et rektangel. Og for en rektangulær kasse.

6. Bestem symmetrigruppen for en (uendelig) cirkulær cylinder.

7. *Bestem symmetrigruppen for dodekaederet.

8. Betragt i $\mathbb{R}^3$ en endelig punktmængde K, som ikke er indeholdt i en linie. Vis, at symmetrigruppen $\mathrm{E}(K)$ er endelig.

9. For enhver begrænset, ikke-tom delmængde K af $\mathbb{R}^n$ gælder, at symmetrigruppen $\mathrm{E}(K)$ er en punktgruppe. Vis denne påstand for $n = 2$ og $n = 3$. [Vink: se tidligere opgaver om punktgrupper.]

4. Punktgrupper og translationsgrupper.

(4.1) Definition. Undergrupper i den euklidiske transformationsgruppe $\mathrm{E}(n)$ kaldes også *flytningsgrupper*. Lad G være en flytningsgruppe. Ved *punktgruppen* for G forstås billedet af G ved homomorfien $f \mapsto \overline{f}$ defineret i (2.2). Punktgruppen, der sædvanligvis betegnes $\overline{G}$, er således en undergruppe i den ortogonale gruppe $\mathrm{O}(n)$. Den består af de ortogonale matricer, der hører til flytningerne i G. En matrix $A \in \mathrm{O}(n)$ ligger altså i punktgruppen $\overline{G}$, hvis og kun hvis der i G findes en flytning af formen $x \mapsto Ax + b$ med en passende vektor b.

Ved *translationsgruppen* for G forstås undergruppen $\mathrm{T}_G := G \cap T(n)$ bestående af de translationer, der tilhører G. Via isomorfien mellem $\mathrm{T}(n)$ og $\mathbb{R}^n$ opfattes translationsgruppen T_G altid som en (additiv) undergruppe i $\mathbb{R}^n$. En vektor $u \in \mathbb{R}^n$ tilhører altså translationsgruppen T_G, hvis og kun hvis translationen t_u tilhører G.

Det skal understreges, at translationsgruppen T_G er en undergruppe af G, hvorimod punktgruppen $\overline{G}$ snarere skal opfattes som en kvotientgruppe af G. Ifølge konstruktionen er afbildningen $f \mapsto \overline{f}$ nemlig en surjektiv homomorfi $G \to \overline{G}$, og kernen er netop translationsgruppen T_G. Det følger derfor af Isomorfisætningen, at T_G er en normal undergruppe af G og at $\overline{G}$ er isomorf med kvotientgruppen $G/\,\mathrm{T}_G$.

(4.2) Eksempel. I (2.10) har vi defineret, at en flytningsgruppe G er en punktgruppe, hvis flytningerne i G har et fælles fixpunkt. Det er klart, at sådan gruppe er lig med sin egen punktgruppe i den forstand, at homomorfien $f \mapsto \overline{f}$ er en isomorfi $G \to \overline{G}$.

I almindelighed er homomorfien $G \to \overline{G}$ en isomorfi, netop når translationsgruppen T_G kun består af nul-vektoren (svarende til translation med 0, som er den identiske afbildning).

Betragt for eksempel den cykliske undergruppe $G = \langle g \rangle$ i $\mathrm{E}(3)$ frembragt af en skruning g med en drejningsvinkel, der er et irrationalt multiplum af 2π. Irrationaliteten sikrer, at alle potenser g^i med $i \neq 0$ er skruninger. Specielt er translationsgruppen T_G triviel, og G er altså „lig med“ sin punktgruppe $\overline{G}$. Men G er ikke selv en punktgruppe, idet identiteten er den eneste flytning i G, der har fixpunkter.

(4.3) Observation. Lad G være en flytningsgruppe i $\mathrm{E}(n)$. Da er, som nævnt i (4.1), translationsgruppen T_G en normal undergruppe i G. Der gælder med andre ord, at hvis t_v er en translation i G og f er en vilkårlig flytning i G, så er også ft_vf^{-1} en translation i G. Antag, at $f(x) = Ax + b$, hvor A er matricen hørende til f. Da er

$$ft_vf^{-1}(x) = A\big(A^{-1}x - A^{-1}b + v\big) + b = x + Av = t_{Av}(x). \tag{4.3.1}$$

Flytningen ft_vf^{-1} er altså translationen t_{Av}. Det ses derfor, at hvis A er en ortogonal matrix i punktgruppen $\overline{G}$ og v er en vektor i translationsgruppen T_G, så vil vektoren Av igen tilhøre translationsgruppen T_G.

(4.4). Det er nærliggende at spørge, for en given (additiv) undergruppe L af $\mathbb{R}^n$ og en given undergruppe H af $\mathrm{O}(n)$, om der findes flytningsgrupper G således, at $\mathrm{T}_G = L$ og $\overline{G} = H$. Det fremgår af udregningen i (4.3), at følgende betingelse er en nødvendig betingelse for eksistensen af G:

(†) Hvis $v \in L$ og $A \in H$, så er $Av \in L$.

Betingelsen er også tilstrækkelig. Antag nemlig, at betingelsen (†) er opfyldt. Betragt i $\mathrm{E}(n)$ delmængden G bestående af alle flytninger g af formen,

$$g = t_v T_A \quad \text{for } v \in L,\ A \in H. \tag{*}$$

Af udregningen i (4.3.1) fremgår, at når A er matricen hørende til en flytning f og v er en vektor i $\mathbb{R}^n$, så er $f t_v = t_{Av} f$. Hvis $h = t_u T_B$ er endnu en flytning af formen (*), får vi derfor

$$gh = t_v T_A t_u T_B = t_v t_{Au} T_A T_B = t_{v+Au} T_{AB}.$$

Det følger af (†), at vektoren $v + Au$ tilhører undergruppen L, og produktet AB tilhører undergruppen H. Altså har produktet gh formen (*). Delmængden G er derfor en stabil delmængde af $\mathrm{E}(n)$. Den identiske afbildning har formen (*) med $v := 0$ og $A := 1$. Endelig ses, når g har formen (*), at

$$g^{-1} = (t_v T_A)^{-1} = T_{A^{-1}} t_{-v} = t_{-A^{-1}v} T_{A^{-1}}.$$

Den inverse g^{-1} har derfor igen formen (*). Heraf følger, at delmængden G er en undergruppe i $\mathrm{E}(n)$. Det er klart, at $\mathrm{T}_G = L$ og $\overline{G} = H$. Hermed er vist, at betingelsen (†) er tilstrækkelig.

(4.5) Definition. Lad der være givet en flytningsgruppe G i $\mathbb{R}^n$. For ethvert punkt $p \in \mathbb{R}^n$ defineres *isotropigruppen* for p som undergruppen G_p bestående af de flytninger g i G, der har p som fixpunkt, dvs opfylder $g(p) = p$. Ved homomorfien $f \mapsto \overline{f}$ afbildes isotropigruppen G_p injektivt ind i $\overline{G}$. Hertil er det nemlig nok at bemærke, at en flytning f, som opfylder $\overline{f} = 1$, er en translation, og hvis en sådan har et fixpunkt p, må det være den identiske afbildning.

Flytningsgruppen G kalder vi (med et sprogligt misfoster) *split*, hvis der findes et punkt p i $\mathbb{R}^n$ således, at isotropigruppen G_p afbildes surjektivt (og dermed isomorft) på punktgruppen $\overline{G}$. Hvis G er split, består G af alle flytninger g, der er produkter,

$$g = t_u h, \qquad \text{hvor } u \in \mathrm{T}_G \quad h \in G_p.$$

Da G er split, findes nemlig for hver flytning $g \in G$ en flytning $h \in G_p$ således, at $\overline{h} = \overline{g}$. Flytningen gh^{-1} ligger så i kernen for homomorfien $f \mapsto \overline{f}$, og den er derfor en translation t_u. Da $t_u = gh^{-1}$ tilhører G, har vi altså $u \in \mathrm{T}_G$. Øjensynlig er $g = t_u h$.

For gruppen G i (4.4), konstrueret ud fra givne undergrupper L af $\mathbb{R}^n$ og H af $\mathrm{O}(n)$ under forudsætning af betingelsen (4.4)(†), har vi øjensynlig, at isotropigruppen G_o for nul-vektoren består af de ortogonale afbildninger T_A for $A \in H$. Gruppen er altså split. Omvendt fremgår det af analysen ovenfor, at enhver flytningsgruppe, der er split, efter en passende translation af origo er af formen konstrueret i (4.4).

(4.6) Eksempel. Det er nemt at angive en flytningsgruppe, som ikke er split. For eksempel er en flytningsgruppe G med $\mathrm{T}_G = \{0\}$ split, netop når G er en punktgruppe. Specielt er undergruppen G af $\mathrm{E}(3)$ fra Eksempel (4.2) ikke split, da identiteten er den eneste flytning i G, der har et fixpunkt.

Som endnu et eksempel betragtes en glidespejling $g = t_u s$ i planen, sammensat af en spejling s i en linie gennem origo efterfulgt af en translation med forskydning $u \neq 0$ i liniens retning. Lad $G := \langle g \rangle$ være den cykliske undergruppe frembragt af g i E(2). Øjensynlig er $t_u s = s t_u$. Heraf følger let, at

$$g^i = \begin{cases} t_{iu} s & \text{hvis } i \text{ er ulige,} \\ t_{iu} & \text{hvis } i \text{ er lige.} \end{cases}$$

Potensen g^i er altså en translation, hvis og kun hvis eksponenten i er lige. Translationsundergruppen T_G er derfor den cykliske undergruppe frembragt af translationen med forskydning $2u$, og punktgruppen $\overline{G}$ er den cykliske undergruppe (af orden 2) i O(2) frembragt af s. Øjensynlig er den identiske afbildning den eneste flytning i G, der har fixpunkter. Specielt er G ikke split.

5. Tapetgrupper.

(5.1) Definition. En (additiv) undergruppe L i $\mathbb{R}^n$ kaldes et *gitter* eller et *lattice*, hvis der findes en basis $(e_1, \dots, e_n)$ for vektorrummet $\mathbb{R}^n$ således, at vektorerne i L netop er de vektorer, der har heltalskoordinater med hensyn til basen, dvs

$$L = \{x_1e_1 + \cdots + x_ne_n \mid x_1, \dots, x_n \in \mathbb{Z}\}.$$

Basen $(e_1, \dots, e_n)$ siges også at være en *basis* for gitteret. Et gitter i $\mathbb{R}^n$ for $n > 1$ har altid uendelig mange baser. Bemærk, at det ikke antages, at baserne er ortonormale.

(5.2) Lemma. *Lad L være et gitter i $\mathbb{R}^n$. Da vil enhver begrænset delmængde K af $\mathbb{R}^n$ kun indeholde endelig mange vektorer fra L.*

Bevis. Lad $(e_1, \dots, e_n)$ være en basis for gitteret L. Der findes da en positiv konstant c således, at der for alle $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ gælder uligheden,

$$c(x_1^2 + \cdots + x_n^2) \leqslant \|x_1e_1 + \cdots + x_ne_n\|^2. \tag{*}$$

Højresiden i uligheden, som funktion af $x \in \mathbb{R}^n$, er nemlig kontinuert. Den er positiv, når $x \neq 0$, idet vektorerne e_i er lineært uafhængige. Specielt er højresiden positiv på enhedskuglen i $\mathbb{R}^n$. Da enhedskuglen er begrænset og afsluttet, antager højresiden, som funktion defineret på enhedskuglen, sin mindsteværdi. Lad c være denne mindsteværdi. Da er højresiden større end eller lig med c, når x ligger på enhedskuglen. Med andre ord gælder uligheden (*), når x er en enhedsvektor. En vektor forskellig fra nul-vektoren kan normeres til en enhedsvektor. Heraf følger let, at uligheden (*) gælder for alle $x \neq 0$. Og trivielt gælder den, når $x = 0$.

Antag nu, at $K \subseteq \mathbb{R}^n$ er begrænset, fx med $\|v\|^2 \leqslant C$ for alle $v \in K$, med en positiv konstant C. Lad $v = x_1e_1 + \cdots + x_ne_n$ være en vektor i $L \cap K$. Da $v \in L$, er koefficienterne x_i hele tal, og da $v \in K$, følger det af (*), at $c(x_1^2 + \cdots + x_n^2) \leqslant C$. Dette er øjensynlig kun muligt for endelig mange $x_1, \dots, x_n$. Altså er $L \cap K$ en endelig mængde af vektorer. ▯

(5.3) Observation. Af Lemma (5.2) følger specielt, at der blandt vektorerne i et gitter L findes en vektor af mindst mulig positiv norm. Denne mindste positive norm er samtidig den mindste afstand mellem to forskellige vektorer i L. Afstanden mellem u og v er jo normen af $u - v$, og hvis $u, v \in L$, så er også $u - v$ i L.

(5.4) Definition. En flytningsgruppe $G \subseteq \mathrm{E}(n)$ vil vi kalde en *krystallografisk gruppe*, hvis translationsgruppen T_G for G er et gitter.

Antag, at et gitter L er translationsgruppen for en krystallografisk gruppe G. Lad $H = \overline{G}$ være punktgruppen for G. Som vi har set i (4.4) gælder der så, at gitteret L er invariant under gruppen H i følgende forstand:

(†) $A \in H,\ v \in L \implies Av \in L.$

Denne betingelse, der kaldes den *krystallografiske betingelse*, medfører restriktioner på hvilke par H, L, betående af en undergruppe H og et gitter L, der kan være af formen $\overline{G}$, T_G for en krystallografisk gruppe G.

(5.5) Sætning. *Punktgruppen $\overline{G}$ for en krystallografisk gruppe er endelig.*

Bevis. Lad $(e_1, \dots, e_n)$ være en basis for gitteret T_G. Af Lemma (5.2) følger specielt, at for hvert i findes der i T_G kun endelig mange vektorer af samme norm som e_i. Betragt nu en matrix A i punktgruppen $\overline{G}$. Af den krystallografiske betingelse følger, at Ae_i tilhører T_G. Som lineær afbildning er $x \mapsto Ax$ helt bestemt ved sine værdier Ae_i på basisvektorerne. Yderligere er $x \mapsto Ax$ en isometri, så Ae_i har specielt samme norm som e_i. Der er derfor kun endelig mange muligheder for billederne Ae_i. Altså er der kun endelig mange muligheder for matricen A. Punktgruppen $\overline{G}$ er derfor endelig. ▯

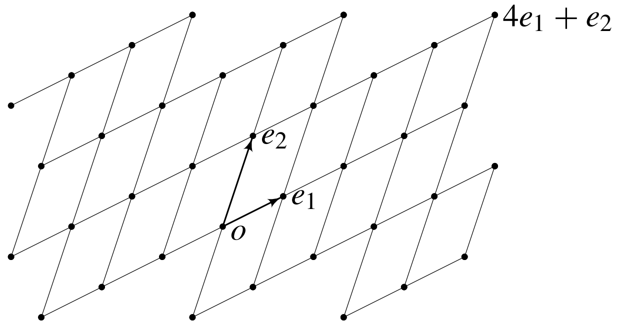
(5.6) Definition. Krystallografiske grupper i rummet $\mathbb{R}^3$ kaldes også *rumgrupper*. De svarer til symmetrigrupper for uendelige krystalstrukturer, og klassifikationen af dem svarer til klassifikation af krystaller. Vi vil i det følgende kun betragte forholdene i planen $\mathbb{R}^2$. Her kaldes en krystallografisk gruppe også en *tapetgruppe*. For en sådan er translationsundergruppen altså et plant gitter, dvs en additiv undergruppe $L \subseteq \mathbb{R}^2$ frembragt af 2 lineært uafhængige vektorer e_1, e_2,

$$L = \{x_1e_1 + x_2e_2 \mid x_1, x_2 \in \mathbb{Z}\}.$$

Et givet gitter har altid uendelig mange baser. For eksempel gælder, at hvis (e_1, e_2) er en basis, så er også $(e_1, e_2 + me_1)$ en basis for alle $m \in \mathbb{Z}$. Vi har nemlig

$$x_1e_1 + x_2e_2 = (x_1 - mx_2)e_1 + x_2(e_2 + me_1),$$

og her er x_1 og x_2 hele tal, hvis og kun hvis $x_1 - mx_2$ og x_2 er hele tal.

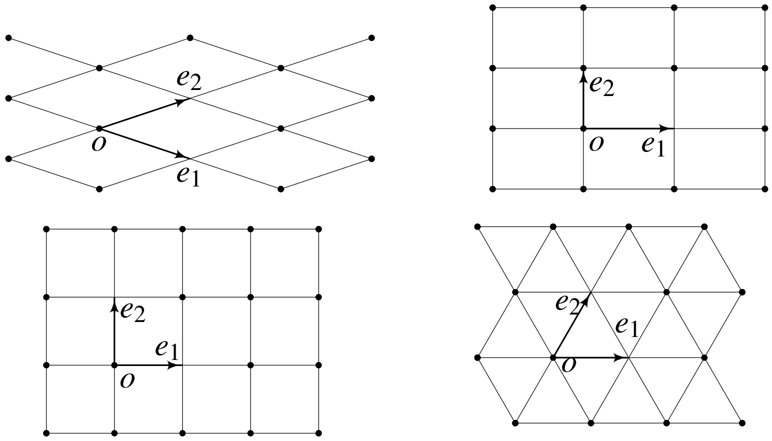


Det skal understreges, at linierne på figuren *ikke* er en del af gitteret. Det er liniernes skæringspunkter, der udgør gitteret.

Et plant gitter kaldes *rombisk*, hhv *rektangulært*, hhv *kvadratisk*, hhv *hexagonalt*, hvis det har en basis (e_1, e_2), hvor vektorerne e_1 og e_2 opfylder, at de har samme norm, hhv er ortogonale, hhv har samme norm og er ortogonale, hhv har samme norm og har en indbyrdes vinkel på $\pi/3$.

Bemærk, at gitteret på figuren ovenfor faktisk er et kvadratisk gitter: vektorene e_1 og $e_2 - e_1$ er ortogonale og af samme længde, og de er også en basis.

Et kvadratisk gitter er både rektangulært og rombisk, et hexagonalt gitter er også rombisk.

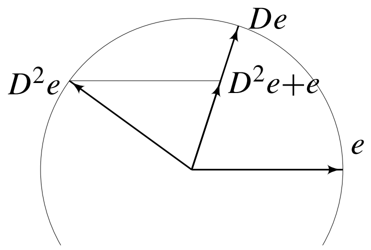


(5.7) Sætning. *Punktgruppen $\overline{G}$ for en tapetgruppe G må være en af grupperne C_k eller D_k for $k = 1, 2, 3, 4, 6$. Hvis punktgruppen er C_1 eller C_2 kan gitteret T_G være vilkårligt. Hvis punktgruppen er D_1 eller D_2 må gitteret T_G være rombisk eller rektangulært. Hvis punktgruppen er C_4 eller D_4 må gitteret T_G være kvadratisk. Hvis punktgruppen er C_3, D_3, C_6 eller D_6, må gitteret T_G være hexagonalt.*

Bevis. Punktgruppen $\overline{G}$ er en undergruppe i $\mathrm{O}(2)$. Af Sætning (5.5) følger, at $\overline{G}$ er endelig. Af Lemma (1.5) følger derfor, at $\overline{G}$ er enten den cykliske undergruppe C_k eller en diedergruppe D_k, for passende k. Det skal først vises, at $k \leqslant 6$ og at $k = 5$ er udelukket.

Vælg $e \neq 0$ blandt vektorerne i T_G med mindst mulig positiv norm. Drejningen D med vinklen $2\pi/k$ tilhører $\overline{G}$. Af Observation (4.3) følger derfor for hver vektor $v \in \mathrm{T}_G$, at vi har $Dv \in \mathrm{T}_G$ og dermed også $Dv - v \in \mathrm{T}_G$. Idet vi antager $k \geqslant 3$, er vektorerne 0, e og De hjørnerne i en trekant. Den er ligebenet, idet to sider har længden $\|e\| = \|De\|$. Den tredie side har længden $\|De - e\|$, og $De - e$ tilhører gitteret. Valget af e sikrer derfor, at den tredie sides længde mindst er lig med længden af de to andre. Heraf følger, at topvinklen $2\pi/k$ mindst er $\pi/3$. Altså er $k \leqslant 6$.

For at udelukke $k = 5$ betragter vi vektoren $D^2e + e$. Den er proportional med De, og når $k = 5$ er den af mindre længde. Men da $D^2e + e \in \mathrm{T}_G$ og $\|De\| = \|e\|$, er dette i modstrid med valget af e.



Hermed er det vist, at punktgruppen er en af de 10 angivne grupper. En del af argumenterne for de resterende påstande samler vi i et hjælperesultat om gitre $L \subseteq \mathbb{R}^2$:

Lemma. (1) *Antag, at der i L er to vektorer e, f, der begge har den mindste positive norm, med $f \neq \pm e$. Da er (e, f) en basis for L.*

(2) *Antag, at* L *er invariant under en lineær spejling* $v \mapsto Sv$*. Da har* L *enten* (i) *en basis af formen* (e, Se)*, eller* (ii) *en basis af formen* (e, f)*, hvor* e*,* f *er ortogonale, og* $Se = e$*.*

Bevis. (1) Af antagelsen følger specielt, at e, f ikke kan være proportionale, så det skal vises, at en vilkårlig vektor $u \in L$ kan skrives som en linearkombination,

$$u = \lambda e + \mu f, \tag{*}$$

med heltalskoefficienter λ, μ. Hertil bemærkes, at da (e, f) er en basis for vektorrummet $\mathbb{R}^2$, har u en fremstilling (*), hvor λ, μ er reelle tal. Subtraheres fra u en passende heltalslinearkombination af e, f, kan vi opnå en ny vektor $u \in L$ således, at der i fremstillingen (*) gælder, at $0 \leqslant \lambda < 1$ og $0 \leqslant \mu < 1$. Det er nok at vise, at $u = 0$, altså at $\lambda = \mu = 0$. De antagne uligheder for λ, μ medfører, at u ligger i romben med hjørnerne $0, e, f, e+f$. Afstanden fra u til det nærmeste af rombens 4 hjørner er derfor højst sidelængden divideret med $\sqrt{2}$; specielt er afstanden strengt mindre end sidelængden $\|e\|$. På den anden side er afstanden normen af differensvektoren, og det er normen af en vektor i gitteret. Valget af e sikrer derfor, at afstanden må være 0, altså at u er et af de fire hjørner. Ulighederne for λ, μ sikrer nu, at $u = 0$, som ønsket. Hermed er (1) bevist.

For at bevise (2) vælger vi en vektor $e \neq 0$ i L af mindst mulig positiv norm. Det er let at se, at e kan suppleres med en vektor $f \in L$ til en basis (e, f). Hvis $Se \neq \pm e$, så følger det i øvrigt af (1), at (e, Se) er en sådan basis. Altså indtræffer mulighed (i).

Antag derfor, at $Se = \pm e$, og først, at $Se = e$. Vektoren e bestemmer så aksen for spejlingen S. Vektoren $f + Sf$ ligger på aksen, og i gitteret. Altså er $f + Sf = \lambda e$ med $\lambda \in \mathbb{Z}$. Erstattes f med $f - e$, ændres λ til $\lambda - 2$. Derfor kan vi antage, at $\lambda = 0, 1$. Hvis $\lambda = 0$, så er $Sf = -f$, og så er f vinkelret på e, og gitteret er rektangulært; specielt indtræffer (ii). Hvis $\lambda = 1$, så er $Sf + f = e$, og så er også (f, Sf) en basis for gitteret; specielt indtræffer (i) (med $e := f$).

Hvis $Se = -e$, så er e vinkelret på spejlingsaksen. Det følger nu tilsvarende først, at $f - Sf = \lambda e$ med $\lambda \in \mathbb{Z}$, og dernæst, at vi kan antage $\lambda = 0, 1$. Hvis $\lambda = 0$, så er $f = Sf$, og derfor indtræffer (ii) (med $(e, f) := (f, e)$). Hvis $\lambda = 1$, så er også (f, Sf) en basis, og derfor indtræffer (i) (med $e := f$).

Hermed er hjælperesultaterne bevist. ▯

Nu følger påstandene i Sætningen: Hvis $\overline{G}$ indeholder en drejningsmatrix D med vinklen $2\pi/k$ og $k \geqslant 3$, kan (1) anvendes, idet e vælges som en vektor i T_G med den mindste positive norm, og $f := De$. Det følger, for $k = 3, 6$, at gitteret er hexagonalt, og for $k = 4$, at det er kvadratisk. Hvis $\overline{G}$ indeholder en spejlingsmatrix S, så følger det af (2), at gitteret må være rombisk eller rektangulært. Hermed er sætningen bevist. ▯

(5.8). Sætning (5.7) udsiger, at der højst er 10 undergrupper H af $\mathrm{O}(2)$, der kan forekomme som punktgruppe $\overline{G}$ for en tapetgruppe G, og mere præcist, at der højst er følgende 12 muligheder for kombinationer H, L, der kan forekomme som $\overline{G}, \mathrm{T}_G$ for en tapetgruppe G:

C_1, vilkårligt	C_2, vilkårligt	C_3, hexagonalt	C_4, kvadratisk
C_6, hexagonalt			
D_1, rektangulært	D_1, rombisk	D_2, rektangulært	D_2, rombisk
D_3, hexagonalt	D_4, kvadratisk	D_6, hexagonalt	

For hver af de 12 kombinationer H, L *kan* gitteret af den anførte form vælges således, at den krystallografiske betingelse er opfyldt, dvs således, at L er invariant under gruppen H. Gruppen C_1 består kun af identiteten, så ethvert gitter er invariant under C_1. Gruppen C_2 består af identiteten og halvdrejningen $v \mapsto -v$. Ethvert gitter er derfor også invariant under C_2. Gruppen C_4 er frembragt af drejningen på $\pi/2$. Følgelig er ethvert kvadratisk gitter invariant under C_4. Endelig er ethvert hexagonalt gitter invariant under C_3 og under C_6.

Betragt dernæst de tilsvarende diedergrupper D_k. Gruppen D_1 er den cykliske gruppe af orden 2 frembragt af en spejling, og gruppen D_2 er frembragt af en spejling og halvdrejningen $x \mapsto -x$. Det er klart, at et rektangulært gitter er invariant under spejlingen i linien bestemt ved en af basisvektorerne og at et rombisk gitter er invariant under spejlingen i linien bestemt ved summen af de to basisvektorer. Både et rombisk gitter og et rektangulært gitter er således invariante under D_1 og under D_2. Endelig er det klart, at et kvadratisk gitter naturligt er invariant under D_4 og at et hexagonalt gitter er invariant under D_3 og under D_6. For gruppen D_3 er der endda *to forskellige* muligheder for beliggenheden af det hexagonale gitter: D_3 er symmetrigruppen for en regulær trekant med midtpunkt i origo, og gitteret kan vælges enten med basis i 2 af trekantens hjørner, eller drejet $2\pi/12$ i forhold hertil. Den første mulighed er øjensynlig karakteriseret ved, at de to basisvektorer ligger på akser for spejlingerne i D_3.

Hvis den krystallografiske betingelse for H, L er opfyldt, findes der altid en tapetgruppe G således, at $\overline{G} = H$ og $\mathrm{T}_G = L$. Det følger nemlig af konstruktionen i (4.4), at flytningerne i E(2) af formen,

$$x \mapsto Ax + v, \quad \text{hvor } A \in H \text{ og } v \in L,$$

udgør en sådan gruppe G. Den herved bestemte tapetgruppe G er split, og det følger af overvejelserne i (4.5), at enhver split tapetgruppe, bortset fra en translation af origo, er af denne form.

Der er derfor splitte tapetgrupper svarende til de 12 kombinationer, og med de to forskellige muligheder for D_3 som punktgruppe fås i alt 13 klasser af splitte tapetgrupper.

Den fulde klassifikation er følgende: *Der er* 17 *klasser af tapetgrupper, nemlig de* 13 *klasser af splitte tapetgrupper og yderligere* 4 *klasser af ikke-splitte grupper:* 1 *klasse for* D_1 *med et rektangulært gitter,* 2 *klasser for* D_2 *med et rektangulært gitter, og* 1 *klasse for* D_4 *med et kvadratisk gitter.*

Tapetgrupperne er de krystallografiske grupper i planen. For rummet $\mathbb{R}^3$ kan man tilsvarende vise, at der er 230 klasser af rumgrupper.

(5.9) Bemærkning. Lad os skitsere et bevis for klassifikationen af tapetgrupperne. Vi antager, at G er en ikke-split tapetgruppe, og vi skal vise, at der er 4 muligheder for G, og at de forekommer. I beviset bruges, at homomorfien $G \to \overline{G}$ er surjektiv: hver matrix $A \in \overline{G}$ kan altså *løftes* til en flytning $f \in G$, dvs en flytning af formen $f(x) = Ax + b$.

For det første må $\overline{G}$ være en diedergruppe D_k. Er nemlig $\overline{G}$ den cykliske gruppe C_k, kan vi løfte drejningen D med vinklen $2\pi/k$ til en flytning $d \in G$. Det følger af klassifikationen i (2.6), at d er en drejning med vinklen $2\pi/k$ omkring et fixpunkt $p \in \mathbb{R}^2$. Isotropigruppen G_p indeholder så den cykliske undergruppe $\langle d \rangle$, og denne undergruppe afbildes surjektivt, og derfor bijektivt på $\overline{G}$. Altså er G split.

Der findes altså spejlinger S i $\overline{G}$. Betragt en sådan spejling S, og en flytning $s(x) = Sx + b$ i G, som løfter S. Ifølge klassifikationen i (2.6) er s en glidespejling, så efter en eventuel translation af origo kan vi antage, at b ligger på spejlingsaksen.

Antag først, at mulighed (i) (nævnt i beviset for Sætning (5.7)) indtræffer for S og gitteret T_G. Det påstås, at S så kan løftes til en spejling i G. Ifølge antagelsen har T_G nemlig en basis af formen (e, Se), så spejlingsaksen er bestemt ved vektoren $e + Se$. Altså er $b = \lambda(e + Se)$. Vi kan sammensætte s med en translation i G; specielt kan vi fra b trække et heltalsmultiplum af $e+Se$. Derfor kan vi antage, at $0 \leqslant \lambda < 1$. Kvadratet s^2 ligger igen i G, og det er translationen med forskydning $2b$. Altså ligger $2b \in T_G$, dvs $2\lambda \in \mathbb{Z}$. Det giver mulighederne $\lambda = 0$ og $\lambda = \frac{1}{2}$. I det første tilfælde er $b = 0$, og så er s en spejling, som ønsket. I det andet tilfælde er $s(x) = Sx + \frac{1}{2}e + \frac{1}{2}Se$. Den sammensatte flytning $s' := t_{-e}s$ er også en løftning af S, af formen $s'(x) = Sx - \frac{1}{2}e + \frac{1}{2}Se$. Øjensynlig er $\frac{1}{2}Se$ et fixpunkt for s'. Derfor er s' en spejling, som ønsket.

Antag dernæst, at mulighed (ii) indtræffer, altså at der findes en ortogonal basis (e, f) for T_G med $Se = e$. Da er e spejlingens akse, så $b = \lambda e$. Fra b kan trækkes et passende heltalsmultiplum af e, så det kan antages, at $0 \leqslant \lambda < 1$. Da kvadratet s^2 er translation med $2b$, er $2b \in \mathrm{T}_G$, og følgelig er $2\lambda \in \mathbb{Z}$. Altså er $\lambda = 0$ eller $\lambda = \frac{1}{2}$. Hvis $\lambda = 0$, er $b = 0$ og s er en spejling. Hvis $\lambda = \frac{1}{2}$, så er s en glidespejling af formen,

$$s(x) = Sx + \tfrac{1}{2}e. \tag{*}$$

Vi kan altså løfte S enten til en spejling s, eller til en glidespejling af formen (*).

Betragt nu den ikke-splitte tapetgruppe G, med $\overline{G} = \mathrm{D}_k$. Punktgruppen $\overline{G}$ er frembragt af én spejling, hvis $k = 1$, og af to spejlinger, hvis $k \geqslant 2$. Hvis de frembringende spejlinger i $\overline{G}$ kunne løftes til spejlinger i G, ville G være split. Det er nemlig klart for $k = 1$, og hvis $k \geqslant 2$ ville skæringspunktet p for de to løftede spejlingers akser være et fælles fixpunkt, og isotropigruppen G_p ville afbildes surjektivt og dermed bijektivt på $\overline{G}$.

Der er altså mindst én spejling S i $\overline{G}$, som ikke kan løftes til en spejling i G. Af de foregående overvejelser følger derfor, at (ii) indtræffer: Vi kan konkludere, at gitteret T_G er rektangulært, med basis e, f, hvor $Se = e$, og S kan løftes til en glidespejling s i G af formen (*).

Herefter er $k = 3, 6$ udelukket. For $k = 1$ er der kun én spejling i $\overline{G} = \mathrm{D}_1$, og den kan altså løftes til en glidespejling af formen (*). For $k = 2$ er der to spejlinger i $\overline{G}$, og det giver to muligheder: ingen af dem kan løftes til spejling eller én af dem kan. Betragt endelig $k = 4$. Vælg en spejling S i $\overline{G}$, som ikke kan løftes til en spejling i G, og løft S til en glidespejling af formen (*), med en ortogonal basis (e, f) for gitteret. Da gitteret er invariant under drejningen med vinklen $\pi/2$, er gitteret ortogonalt: e og f har samme norm. Betragt nu spejlingen $\tilde{S}$ i D_4 med aksen drejet $-\pi/4$ i forhold til aksen for S. Vi har allerede fastlagt basen for T_G, så det er udelukket, at T_G har en ortogonal basis med en basisvektor på aksen for $\tilde{S}$. Derfor kan mulighed (ii) ikke indtræffe for $\tilde{S}$. Af overvejelserne ovenfor følger så, at $\tilde{S}$ kan løftes til spejling $\tilde{s}$. Vi kan fx vælge origo som skæringspunkt mellem akserne for s og $\tilde{s}$. Herefter er G fastlagt.

Det skal yderligere vises, at der faktisk findes tapetgrupper i hver af de ikke-splitte klasser. Vi vælger som eksempel her at beskrive de tapetgrupper G, som indeholder en kvartdrejning, dvs en drejning med vinklen $\pi/2$ omkring et punkt. Det følger af Sætning (5.7), at punktgruppen $\overline{G}$ må være C_4 eller D_4, og af diskussionen i (5.8) fremgår, at der er tre muligheder: en split gruppe med punktgruppe C_4, en split gruppe med punktgruppe D_4, samt en ikke-split gruppe med punktgruppe D_4.

I alle tilfælde må gitteret T_G være kvadratisk. Vi kan antage, at det er gitteret $\mathbb{Z}^2$ frembragt af den kanoniske basis (e_1, e_2) for $\mathbb{R}^2$. Vektorerne i gitteret er altså vektorer $u = (u_1, u_2)$ med heltalskoordinater u_1, u_2, og translationerne i G er translationerne med sådanne vektorer. Gruppen G skal indeholde en drejning d med vinklen $\pi/2$ omkring et punkt. Vi kan antage, at det er omkring origo, altså at $d(x) = Dx$, hvor D er matricen,

$$D = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

(a) Antag først, at $\overline{G}$ er den cykliske gruppe C_4 bestående af de fire potenser D^j for $j = 0, 1, 2, 3$. I dette tilfælde er G som nævnt split, og G består af alle flytninger af formen,

$$x \mapsto D^j x + u, \quad \text{for } j = 0, 1, 2, 3 \text{ og } u \in \mathbb{Z}^2. \tag{5.9.1}$$

Flytningerne er translationer for $j = 0$, drejninger med vinkel $\pm\pi/2$ for $j = 1, 3$, og halvdrejninger for $j = 2$. For at få et overblik over drejningerne i G bestemmes deres fixpunkter.

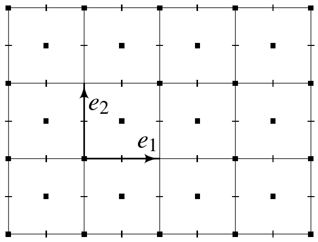
Fixpunkter p for flytningen $x \mapsto D^j x + u$ bestemmes ved at løse ligningen $p = D^j p + u$. For $j = 1$ har vi $(1 - D)p = u$, og

$$1 - D = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \quad \text{og} \quad \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} u_1 \\ u_2 \end{pmatrix}.$$

Fixpunkterne er således alle punkter $(v_1/2, v_2/2)$, hvor $v_1 = u_1 - u_2$ og $v_2 = u_1 + u_2$ med hele tal u_1, u_2, dvs hvor v_1, v_2 er hele tal *af samme paritet*. Punkterne er altså dels vektorerne i gitteret $\mathbb{Z}^2$, dels midtpunkterne af de enhedskvadrater, som gitterpunkterne deler planen i. Det er klart, at det er de samme punkter, som er fixpunkter for flytningerne af formen $x \mapsto D^3 x + u$.

For $j = 2$ har vi, at $1 - D^2$ er 2 gange enhedsmatrix. Fixpunkterne for flytninger af formen $x \mapsto D^2 x + u$ er derfor netop punkterne $(u_1/2, u_2/2)$, hvor u_1, u_2 er hele tal.

Gruppen G består således af alle translationer med en heltalsvektor, af alle drejninger på et multiplum af $\pi/2$ omkring et punkt $(v_1/2, v_2/2)$, hvor v_1 og v_2 er hele tal af samme paritet, samt af alle halvdrejninger omkring et punkt $(u_1/2, u_2/2)$, hvor u_1 og u_2 er hele tal.



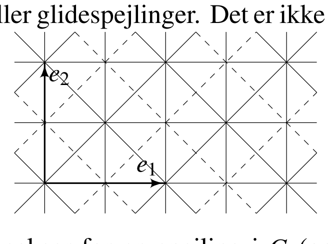
(b0) Betragt dernæst tilfældet, hvor G er split med $\overline{G} = \mathrm{D}_4$. Vi kan antage, at det er isotropigruppen i origo, der afbildes bijektivt på $\overline{G}$, og at denne isotropigruppe er symmetrigruppen for kvadratet med hjørnerne $\pm e_1, \pm e_2$. I G ligger så drejningen $x \mapsto Dx$ med vinklen $\pi/2$ og spejlingen $x \mapsto Sx$ i førsteaksen, bestemt ved matricen

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Gruppen G er så gruppen af af alle flytninger af formen (5.9.1) eller af følgende form:

$$x \mapsto SD^j x + u, \quad \text{for } j = 0, 1, 2, 3 \text{ og } u \in \mathbb{Z}^2. \tag{5.9.2}$$

Flytningerne i (5.9.2) er spejlinger eller glidespejlinger. Det er ikke svært at bestemme deres spejlingsakser:

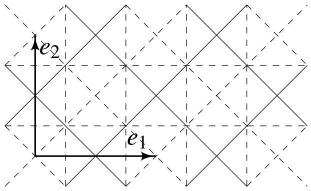


De fuldt optrukne linier er spejlingsakser for en spejling i G (og uendelig mange glidespejlinger). De stiplede linier er akser for uendelig mange glidespejlinger i G, hvoraf ingen er spejlinger.

(b1) Betragt endelig tilfældet, hvor G er ikke-split, med $\overline{G} = \mathrm{D}_4$. Med notationen ovenfor har vi i G glidespejlingen s i (*), der løfter S, og spejlingen $\tilde{s}$, som løfter $\tilde{S}$. Produktet $S\tilde{S}$ er drejningen D med vinklen $\pi/2$, og den løftes af den sammensatte flytning $d = s\tilde{s}$. Vi kan antage, at $(e, f) = (e_1, e_2)$. Vælges origo som skæringspunktet mellem spejlingsakserne (for glidespejlingen s og for spejlingen $\tilde{s}$), så er vektoren $-\frac{1}{4}e_1 - \frac{1}{4}e_2$ fixpunktet for d. Vælges omvendt denne vektor som origo, så beskrives d ved den lineære drejning $d(x) = Dx$ og glidespejlingen s får formen $s(x) = Sx + c$ med $c := \frac{1}{2}e_1 + \frac{1}{2}e_2$. Altså må G så bestå af alle flytninger af formen (5.9.1) eller af følgende form:

$$x \mapsto SD^j x + c + u, \quad \text{for } j = 0, 1, 2, 3 \text{ og } u \in \mathbb{Z}^2. \tag{5.9.3}$$

Omvendt er det ikke svært at vise, at flytningerne af formen i (5.9.1) eller (5.9.3) udgør en gruppe. Flytningerne af den sidste form er spejlinger eller glidespejlinger:



Igen er de fuldt optrukne linier spejlingsakser for en spejling i G og de stiplede linier er akser for glidespejlinger, hvoraf ingen er spejlinger.

Bemærk, at de to grupper bestemt i (b0) og (b1) kan skelnes ved beskrivelsen af spejlingsakserne. I gruppen i (b0) findes der spejlinger, hvis akser går gennem fixpunkterne for kvartdrejningerne i G, for gruppen i (b1) går akserne for spejlingerne ikke gennem disse fixpunkter.

(5.10) Note. De betragtede grupper i planen hedder tapetgrupper, fordi de er relaterede til tapeter. Symmetrigruppen for et tapet er en tapetgruppe, og omvendt vil enhver tapetgruppe G frembringe tapeter på følgende måde. Lad F være en figur i $\mathbb{R}^2$. Vi kan tænke på F som en tegning, bestående af et antal begrænsede kurver. Dan så foreningsmængden,

$$F^* := \bigcup_{g \in G} g(F).$$

Foreningsmængden indeholder specielt alle translationer $t_u(F)$ for $u \in \mathrm{T}_G$, dvs vi „genfinder“ figuren F periodisk i F^*. Desuden indeholder F^* periodisk en række figurer, der er kongruente med F, svarende til de flytninger i G, der ikke er translationer. Foreningsmængden F^* er altså et *tapet*. Det er klart, at flytningerne i G er symmetrier af F^*: for hver flytning $g \in G$ gælder, at $g(F^*) = F^*$. Det er også næsten klart, at hvis den givne figur F er tilstrækkeligt usymmetrisk, så er G netop symmetrigruppen $\mathrm{E}(F^*)$ for tapetet F^*.

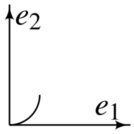
Tapetet F^* kan også fås som en foreningsmængde af translationer af en figur. Antag, at punktgruppen $\overline{G}$ har orden k, og vælg k flytninger $g_1, \dots, g_k$ i G således, at matricerne $\overline{g}_i$ er samtlige matricer i $\overline{G}$. Betragt den endelige foreningsmængde,

$$\tilde{F} := \bigcup_{i=1}^{k} g_i(F).$$

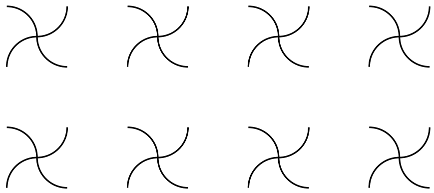
For en given flytning $g \in G$ findes et i således, at $\overline{g} = \overline{g}_i$. Altså er gg_i^{-1} en translation i G, dvs af formen t_u, hvor $u \in \mathrm{T}_G$. Det følger, at $g = t_u g_i$, og specielt er $g(F) = t_u g_i(F) \subseteq t_u(\tilde{F})$. Heraf følger, at tapetet F^* er foreningsmængden,

$$F^* = \bigcup_{u \in \mathrm{T}_G} t_u(\tilde{F}).$$

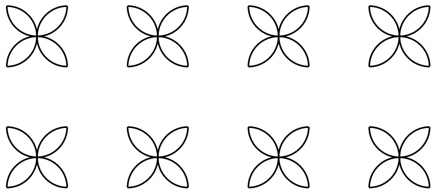
(5.11) Eksempel. Betragt de tre grupper fra Eksempel (5.9). Lad F være figuren bestående af en kvartcirkel med radius $\frac{1}{4}$ og centrum i $(0, \frac{1}{4})$:



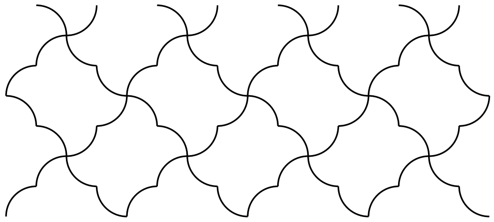
For gruppen behandlet i (5.9)(**a**) får vi det tilsvarende tapet F^*:



For gruppen i (**b0**) får vi tapetet:

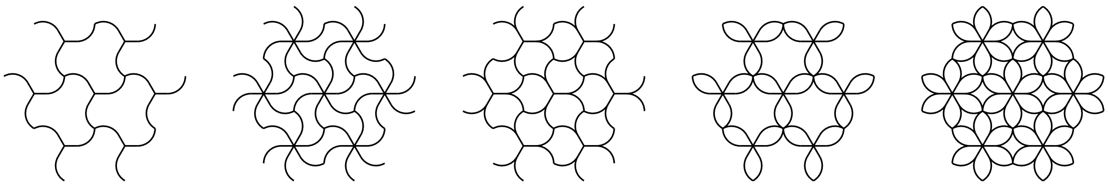


Og endelig får vi for gruppen i (**b1**):



(5.12) Eksempel. Betragt tilsvarende kurven F bestående af et stykke af førsteaksen og en kvartcirkel:

Trekanten bestemmer et hexagonalt gitter. Kurven ender midt i trekanten (som ikke er en del af kurven). Her er (en del) af tapeterne frembragt af F under de 5 tapetgrupper, der har hexagonalt gitter (med punktgrupper C_3, C_6, D_3 (2 stk), og D_6):



(5.13) Opgaver.
1. Lad $L \subseteq \mathbb{R}^2$ være et gitter med basis (e, f), og lad $u = ae + bf$ og $v = ce + df$ være vektorer i L. Vis, at (u, v) er en basis for L, hvis og kun hvis heltalsmatricen $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ har determinant ± 1. Slut heraf, at en vektor $u = ae + bf \in L$ kan suppleres med en vektor v til en basis for L, hvis og kun hvis tallene a, b er primiske.

2. Lad $L \subseteq \mathbb{R}^2$ være et gitter, som er både rombisk og rektangulært. Vis, at L er kvadratisk. [Vink. Antag, at (e, f) er en ortogonal basis for L, med $\|e\| \leqslant \|f\|$. Lad S være spejlingen defineret ved, at den ombytter to lige lange vektorer i en anden basis for L. Overvej hvilke muligheder, der er for vektoren Se.]

6. Rummets endelige drejningsgrupper.

(6.1) Indledning. I sætning (2.9) har vi vist, at enhver endelig gruppe G af flytninger er en punktgruppe, altså at flytningerne i G har et fælles fixpunkt. Vælges dette punkt som origo, er flytningerne ortogonale afbildninger. De endelige grupper af flytninger i $\mathbb{R}^n$ svarer altså til de endelige undergrupper af den ortogonale gruppe $\mathrm{O}(n)$. I Sætning (1.5) har vi bestemt de endelige flytningsgrupper for planen $\mathbb{R}^2$. I dette kapitel bestemmer vi de endelige flytningsgrupper for rummet $\mathbb{R}^3$, idet vi dog indskrænker os til egentlige flytninger.

(6.2) Sætning. *Enhver endelig undergruppe G af $\mathrm{O}^+(3)$ er en af følgende:*

Den cykliske gruppe C_k bestående af de k rotationer omkring en fast linie med vinkler, der er multipla af $2\pi/k$.

Diedergruppen D_k bestående af de $2k$ symmetrier af en regulær k-kant (for $k \geqslant 3$).

Klein's Vierer-gruppe V bestående af identiteten og de tre halvdrejninger omkring tre på hinanden vinkelrette akser.

Tetraedergruppen T bestående af de 12 symmetrier af et regulær tetraeder.

Hexadergruppen H bestående af de 24 symmetrier af et regulært hexaeder (eller et oktaeder).

Ikosaedergruppen I bestående af de 60 symmetrier af et regulært ikosaeder (eller dodekaeder).

Bevis. Den trivielle gruppe $G = \{1\}$ er den cykliske gruppe C_1. Vi kan derfor antage, at G ikke er triviel, altså at $|G| \geqslant 2$. Ved en *pol* for gruppen G forstås en enhedsvektor, som er fixpunkt for et gruppeelement $g \neq 1$. Hvert element $g \neq 1$ i G er en drejning omkring en akse gennem origo; hvert element $g \neq 1$ har altså præcis to poler, nemlig de to enhedsvektorer på drejningsaksen. Lad P være mængden af poler. Elementantallet i P er øjensynlig højst lig med $2(|G|-1)$.

Når $g, h \in G$ og p er fixpunkt for h, så er $g(p)$ fixpunkt for ghg^{-1}. Heraf følger, at gruppen G virker på mængden P af poler. Mængden P er derfor den disjunkte forening af banerne for denne virkning. Lad $P_1, \dots, P_r$ være banerne. Vi kan nummerere dem således, at $|P_1| \geqslant \cdots \geqslant |P_r|$.

Betragt en bane P_i. Banens længde er som bekendt divisor i $|G|$, og vi kan sætte $k_i := |G|/|P_i|$. Mere præcist følger det af Baneformlen, at for en vilkårlig pol $p \in P_i$ er $|P_i| = |G : G_p|$, hvor G_p er isotropigruppen for p. Tallet k_i er derfor ordenen af isotropigruppen G_p for en vilkårlig pol p i banen P_i. Da p er en pol, er isotropigruppen G_p ikke triviel; vi har altså $k_i \geqslant 2$.

Hvert element $g \neq 1$ har præcis 2 poler. Hvis vi derfor tæller for hver pol $p \in P$ hvor mange elementer $g \neq 1$, der har p som pol, og lægger tallene sammen, får vi 2 gange antallet af elementer $g \neq 1$ i G. Vi har derfor ligningen,

$$2(|G|-1) = \sum_{p \in P}(|G_p|-1). \tag{6.2.1}$$

På højresiden er $|G_p|-1$ konstant, når p tilhører en bane P_i. Mere præcist har vi, når $p \in P_i$, at $|G_p| = k_i$, og antallet af poler $p \in P_i$ er $|G|/k_i$. Af ligningen (6.2.1) får vi derfor, at

$$2(|G|-1) = \sum_{i=1}^{r} \frac{|G|}{k_i}(k_i - 1).$$

Efter division med $|G|$ opnås ligningen,

$$2\Big(1 - \frac{1}{|G|}\Big) = \sum_{i=1}^{r}\Big(1 - \frac{1}{k_i}\Big). \tag{6.2.2}$$

Som vi skal se medfører denne ligning stærke begrænsninger på de mulige værdier af $|G|$ og af tallene $k_1, \dots, k_r$.

For det første er $\frac{1}{2} \leqslant 1 - 1/|G| < 1$. Ligningens venstreside ligger derfor i intervallet: $1 \leqslant x < 2$. På højresiden ligger hvert led i intervallet: $\frac{1}{2} \leqslant x < 1$. Heraf ses, at der på højresiden må være mindst 2 led og højst 3 led. For antallet r af baner har vi altså $r = 2$ eller $r = 3$. Vi deler nu op i en række tilfælde.

To baner, altså $r = 2$. Ligningen (6.2.2) er ækvivalent med følgende:

$$\frac{2}{|G|} = \frac{1}{k_1} + \frac{1}{k_2}. \tag{6.2.3}$$

Tallene k_1 og k_2 er divisorer i $|G|$, så brøkerne på højresiden er mindst lig med $1/|G|$. Ligningen (6.2.3) medfører derfor, at $k_1 = k_2 = |G|$. Heraf ses, at hvis p er en vilkårlig pol, så har alle elementer g i G punktet p som fixpunkt. Gruppen G består altså af drejninger omkring linien gennem p. Med $k := |G|$ følger det, jfr Sætning (1.5), at $G = \mathrm{C}_k$ er den cykliske undergruppe frembragt af drejningen med vinklen $2\pi/k$ omkring denne linie.

Tre baner, altså $r = 3$. Ligningen (6.2.2) er ækvivalent med følgende:

$$\frac{2}{|G|} = \frac{1}{k_1} + \frac{1}{k_2} + \frac{1}{k_3} - 1. \tag{6.2.4}$$

Tallene k_i er divisorer i $|G|$, og specielt højst lig med $|G|$, og nummereringen var valgt således, at $2 \leqslant k_1 \leqslant k_2 \leqslant k_3$. Hvis $k_1 \geqslant 3$, ville brøkerne på højresiden højst være $1/3$, og højresiden ville altså ikke være positiv. Altså er $k_1 = 2$. Hvis $k_2 \geqslant 4$, ville højresiden højst være $1/2 + 1/4 + 1/4 - 1 = 0$. Altså er $2 \leqslant k_2 \leqslant 3$. For $k_2 = 3$ er højresiden $1/2 + 1/3 + 1/k_3 - 1$ kun positiv for $k_3 < 6$. For sættet (k_1, k_2, k_3) er der således kun mulighederne,

$$(2,2,k) \text{ for } k \geqslant 2, \ \text{ og } (2,3,k) \text{ for } 3 \leqslant k \leqslant 5.$$

Vi behandler dem enkeltvis.

Tilfældet $(2,2,k)$ hvor $k \geqslant 2$: Af (6.2.4) følger, at $|G| = 2k$. De to første baner har derfor længde $2k/2 = k$, og den tredie bane har længde $2k/k = 2$. Antag først, at $k > 2$. Betragt en pol p i den tredie bane. Isotropigruppen G_p har da orden k, og den består af drejninger omkring (aksen bestemt ved) p. Den er derfor cyklisk af orden k, frembragt af drejningen d med vinklen $2\pi/k$ omkring p. Polen $-p$ har den samme isotropigruppe, og for alle andre poler q har isotropigruppen orden 2. Heraf følger, at den tredie bane består af p og $-p$. Lad q være en af de øvrige poler. Isotropigruppen G_q har orden 2, så G indeholder halvdrejningen omkring q. Denne halvdrejning skal holde den tredie bane $\{p, -p\}$ invariant. Det følger, at polen q ligger i planen vinkelret på p. Polerne $d^i(q)$ for $0 \leqslant i < k$ udgør en regulær k-kant i denne plan, altså et dieder. Drejningerne i G er symmetrier af diederet. Da G og diedergruppen D_k har samme orden, er $G = \mathrm{D}_k$.

I tilfældet $k = 2$ vises tilsvarende, at $G = \mathrm{V}$.

Tilfældet $(2, 3, 3)$: Af (6.2.4) følger, at $|G| = 12$. Den første bane har altså længde $12/2 = 6$, de to sidste baner har længde $12/3 = 4$. Kig specielt på de 4 poler i den sidste bane. For hver sådan pol p har isotropigruppen G_p orden 3, så den består af de tre potenser 1, d og d^2 af drejningen d med vinklen $2\pi/3$ omkring p. Hvis q er en af de øvrige poler i banen, består hele banen altså af $p, q, d(q), d^2(q)$. Da polen p var vilkårligt valgt i banen følger det let, at de fire poler i banen er hjørnerne i et regulært tetraeder. De fire hjørner udgør en bane under virkningen af G. Drejningerne i G er derfor symmetrier af tetraederet. Da G og tetraeder-gruppen T har samme orden, følger det, at $G = \mathrm{T}$.

Tilfældet $(2, 3, 4)$: Af (6.2.4) følger, at $|G| = 24$. Banernes længder er altså 12, 8, og 6. Betragt de 6 poler i den sidste bane. For hver sådan pol p har isotropigruppen G_p orden 4, så den består af de 4 potenser $1, d, d^2, d^3$ af drejningen med vinklen $2\pi/4$ omkring p. Det følger, som i det foregående tilfælde, at de 6 poler udgør de 6 hjørner i et regulært oktaeder. Drejningerne i G er symmetrier af oktaederet. Da G har samme orden som oktaedergruppen $\mathrm{O} = \mathrm{H}$, følger det, at $G = \mathrm{H}$.

Tilfældet $(2, 3, 5)$: Af (6.2.4) følger, at $|G| = 60$. Banernes længder er altså 30, 20, og 12. Betragt de 12 poler i den sidste bane. For hver sådan pol p har isotropigruppen G_p orden 5, så den består af de 5 potenser d^i for $i = 0, \dots, 4$ af drejningen med vinklen $2\pi/5$ omkring p. Det følger, som i det foregående tilfælde, at de 12 poler udgør de 12 hjørner i et regulært ikosaeder. Drejningerne i G er symmetrier af ikosaederet. Da G har samme orden som ikosaedergruppen I, følger det, at $G = \mathrm{I}$.

Hermed er alle tilfældene behandlet, og sætningen vist. □

Ringe og legemer

1. Ringbegrebet.

(1.1) Indledning. De to fundamentale operationer med tallene, addition og multiplikation, er kompositioner. De opfylder en række velkendte regler, nemlig dels regler der vedrører hver enkelt komposition, dels den distributive lov, der involverer begge kompositioner.

Vi har tidligere behandlet grupper, der kan opfattes som den abstrakte generalisation af tallene til systemer med én komposition. Her behandler vi *ringe*, der er generalisationen til systemer med to kompositioner.

(1.2) Definition. Ved en *ring* $(\Lambda, +\,, \,\cdot\,)$ forstås en mængde Λ med to givne kompositioner $\Lambda \times \Lambda \to \Lambda$, en *addition* betegnet $(x, y) \mapsto x + y$ og en *multiplikation* betegnet $(x, y) \mapsto xy$, som opfylder, at med additionen er Λ en kommutativ gruppe, at multiplikationen er associativ og har et neutralt element, og at multiplikationen er *distributiv* mht additionen.

Ringens *nul-element* er det neutrale element for additionen; det betegnes 0_Λ eller blot 0. Som sædvanlig, ved en additivt skrevet gruppe, betegner $-\lambda$ det *modsatte* til λ. Ringens *et-element* er det neutrale element for multiplikationen. Det betegnes 1_Λ eller blot 1.

Betingelserne kan udtrykkes ved ligningerne, for alle $\lambda, \mu, \nu \in \Lambda$,

$$\lambda + \mu = \mu + \lambda, \tag{a0}$$

$$(\lambda + \mu) + \nu = \lambda + (\mu + \nu), \tag{a1}$$

$$\lambda + 0 = \lambda, \tag{a2}$$

$$\lambda + (-\lambda) = 0, \tag{a3}$$

$$(\lambda\mu)\nu = \lambda(\mu\nu), \tag{m1}$$

$$1\lambda = \lambda 1 = \lambda, \tag{m2}$$

$$\lambda(\mu + \nu) = \lambda\mu + \lambda\nu, \quad (\lambda + \mu)\nu = \lambda\nu + \mu\nu. \tag{am}$$

Bemærk, at multiplikationen i ringen, i modsætning til additionen, ikke forudsættes at være kommutativ, og at der indgår to ligninger i den distributive lov (am). En *kommutativ ring* er en ring, hvor multiplikationen er kommutativ.

I en ring Λ gælder for alle elementer λ, μ ligningerne,

$$0\lambda = \lambda 0 = 0, \quad (-\lambda)\mu = \lambda(-\mu) = -\lambda\mu, \quad \text{specielt: } (-1)\mu = \mu(-1) = -\mu. \tag{1.2.1}$$

Da Λ med addition er en kommutativ gruppe, følger det nemlig af udregningen,

$$0\lambda + 0\lambda = (0 + 0)\lambda = 0\lambda,$$

at $0\lambda = 0$, og tilsvarende indses $\lambda 0 = 0$. Videre er

$$\lambda\mu + (-\lambda)\mu = (\lambda - \lambda)\mu = 0\mu = 0,$$

og heraf følger $(-\lambda)\mu = -\lambda\mu$; tilsvarende indses $\lambda(-\mu) = -\lambda\mu$.

(1.3) Invertible elementer. Et element λ i en ring Λ kaldes *invertibelt*, hvis λ er invertibelt mht multiplikationen. Med andre ord er λ invertibelt, hvis der findes et element $\lambda' \in \Lambda$ således, at $\lambda'\lambda = \lambda\lambda' = 1$. Elementet λ' er i så fald entydigt bestemt; det kaldes det *inverse element* til λ, og betegnes λ^{-1}. Et invertibelt element i Λ kaldes også en *enhed*. Multiplikationen i Λ er associativ og et-elementet 1 er neutralt element. De invertible elementer i Λ udgør derfor en gruppe med multiplikation som komposition. Denne gruppe betegnes Λ^*. Når λ er invertibel, kan man, for $\alpha \in \Lambda$ skrive α/λ for $\alpha\lambda^{-1}$.

(1.4) Delring. Lad Λ være en ring. Når en delmængde af Λ er stabil under både addition og multiplikation, så defineres ved restriktion en addition og en multiplikation i delmængden.

Ved en *delring* af Λ forstås en delmængde $\Delta \subseteq \Lambda$, som er stabil under addition og multiplikation, og som med sin addition og multiplikation selv er en ring med samme et-element som Λ. Det følger specielt, at en delring Δ er en undergruppe af Λ mht additionen.

For at en delmængde Δ af Λ er en delring, er det nok, at følgende betingelse er opfyldt:

(†) Delmængden Δ er stabil under addition og multiplikation og $-1_\Lambda \in \Delta$.

Antag nemlig, at betingelsen er opfyldt. Da Δ er stabil under multiplikation og $-1_\Lambda \in \Delta$, følger det, at $1_\Lambda = -(-1_\Lambda) = (-1_\Lambda)(-1_\Lambda)$ ligger i Δ. Da Δ er stabil under addition, følger det videre, at $0_\Lambda = -1_\Lambda + 1_\Lambda \in \Delta$. Hvis $\lambda \in \Delta$ får vi, at $-\lambda = (-1_\Lambda)\lambda \in \Delta$. Vi har således set, at $0_\Lambda, 1_\Lambda \in \Delta$ og at $-\lambda \in \Delta$, når $\lambda \in \Delta$. Herefter er det klart, at betingelserne i (1.2) er opfyldt for delmængden Δ.

(1.5) Nul-ringen. En mængde med kun ét element har kun én komposition, og med denne komposition er mængden den trivielle gruppe. Med den additive skrivemåde betegnes det eneste element med 0, og kompositionen er $0 + 0 = 0$. Med den samme komposition som multiplikation er $\{0\}$ endda en ring. Den kaldes *nul-ringen*.

I nul-ringen er nul-elementet og et-elementet det samme element. I enhver ring Λ, som ikke er nul-ringen, er $1_\Lambda \neq 0_\Lambda$. Antages nemlig for en ring Λ, at $1_\Lambda = 0_\Lambda$, får vi for hvert element λ i Λ, at $\lambda = \lambda 1_\Lambda = \lambda 0_\Lambda = 0_\Lambda$; følgelig består Λ alene af nul-elementet.

Nul-ringen spiller i mange situationer en drilsk rolle og som vi skal se, må vi flere steder undtage nul-ringen.

(1.6) Talringe. De reelle tal med sædvanlig addition og multiplikation er et velkendt eksempel på en ring $(\mathbb{R}, +, \cdot)$, som vi naturligvis blot betegner $\mathbb{R}$. Tilsvarende udgør de komplekse tal en ring $\mathbb{C}$, og $\mathbb{R}$ er en delring af $\mathbb{C}$. Delringe af $\mathbb{C}$ kaldes *talringe*. Øjensynlig udgør de rationale tal en talring $\mathbb{Q}$, og de hele tal udgør en talring $\mathbb{Z}$. Talringe er øjensynlig kommutative.

De invertible elementer i ringen $\mathbb{R}$ er netop tallene forskellige fra 0, så den multiplikative gruppe $\mathbb{R}^* = \mathbb{R}\setminus\{0\}$ er netop gruppen af invertible elementer i ringen $\mathbb{R}$. Tilsvarende har vi $\mathbb{C}^* = \mathbb{C}\setminus\{0\}$ og $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$. I ringen $\mathbb{Z}$ er det 1 og -1, der er de invertible elementer. Vi har altså $\mathbb{Z}^* = \{\pm 1\}$.

(1.7) Restklasseringene. Lad n være et fast naturligt tal. Restklasserne modulo n, med sædvanlig addition og multiplikation af restklasser, udgør en ring $\mathbb{Z}/n$. Gruppen $(\mathbb{Z}/n)^*$ af invertible restklasser er netop den multiplikative gruppe af primiske restklasser modulo n. Restklasseringene er øjensynlig kommutative ringe.

(1.8) Funktionsringe. Lad X være en mængde. Som bekendt defineres sum og produkt af reelle funktioner $f: X \to \mathbb{R}$ og $g: X \to \mathbb{R}$ *argumentvis:* sumfunktionen $f + g$ er bestemt ved $(f + g)(x) = f(x) + g(x)$ og produktfunktionen fg ved $(fg)(x) = f(x)g(x)$. Med disse to kompositioner udgør de reelle funktioner på X en ring $\mathcal{F}(X, \mathbb{R})$ (eller $\mathcal{F}_{\mathbb{R}}(X)$ eller blot $\mathcal{F}(X)$). Nul-elementet er den konstante funktion 0 og et-elementet er den konstante funktion 1. Tilsvarende udgør de komplekse funktioner på X en ring $\mathcal{F}(X, \mathbb{C})$.

Mange vigtige delringe af funktioner optræder i analysen. Antag fx, at X er et interval I. Da udgør de kontinuerte reelle funktioner en delring $\mathcal{C}(I)$ af $\mathcal{F}_{\mathbb{R}}(I)$ og de vilkårligt ofte differentiable funktioner udgør en delring $\mathcal{C}^\infty(I)$ af $\mathcal{C}(I)$. Hvis Ω er en åben delmængde af den komplekse plan, udgør de holomorfe funktioner på Ω en delring $\mathcal{H}(\Omega)$ af $\mathcal{F}_{\mathbb{C}}(\Omega)$.

Også *polynomiumsfunktionerne*, dvs funktioner af formen

$$x \mapsto a_0 + a_1 x + \cdots + a_n x^n,$$

bestemmer delringe, $\mathcal{P}ol(I)$ af $\mathcal{C}^\infty(I)$ og $\mathcal{P}ol(\Omega)$ af $\mathcal{H}(\Omega)$.

Det skal understreges, at mængden X i definitionen kan være vilkårlig, og funktionsringene kan bestå af elementer, som vi normalt ikke tænker på som funktioner. For $X = \{1, 2, \dots, n\}$ svarer funktionerne $f: X \to \mathbb{R}$ til n-sæt $(f_1, \dots, f_n)$ af reelle tal, og funktionsringen $\mathcal{F}_{\mathbb{R}}(X)$ er talrummet $\mathbb{R}^n$ med koordinatvis addition og multiplikation. For $X = \mathbb{N}$ svarer funktionerne $f: \mathbb{N} \to \mathbb{R}$ til følger $(f_1, f_2, \dots)$ og funktionsringen $\mathcal{F}(\mathbb{N}, \mathbb{R})$ er rummet $\mathbb{R}^{\mathbb{N}}$ af alle reelle talfølger, med sædvanlig addition og multiplikation af talfølger.

Det er også klart, at vi i definitionen ikke behøver at indskrænke os til at betragte funktioner med reelle eller komplekse værdier. Vi kan betragte afbildninger $f: X \to \Lambda$ med værdier i en vilkårlig given ring Λ. Med argumentvis addition og multiplikation udgør disse afbildninger en ring $\mathcal{F}_\Lambda(X) = \mathcal{F}(X, \Lambda)$. Den er kommutativ, når Λ er kommutativ.

(1.9) Matrixringe. De reelle $r \times r$-matricer med sædvanlig addition og multiplikation udgør en ring $\mathrm{Mat}_r(\mathbb{R})$. De øvre trekantsmatricer, dvs matricerne der har 0 under diagonalen, udgør en delring $\mathrm{Triang}_r(\mathbb{R})$ af $\mathrm{Mat}_r(\mathbb{R})$, og diagonalmatricerne udgør en delring $\mathrm{Diag}_r(\mathbb{R})$ af $\mathrm{Triang}_r(\mathbb{R})$. De invertible elementer i ringen $\mathrm{Mat}_r(\mathbb{R})$ er netop matricerne, der er invertible i sædvanlig forstand, dvs matricerne med determinant forskellig fra nul. De udgør som bekendt den generelle lineære gruppe, $\mathrm{GL}_r(\mathbb{R}) = \mathrm{Mat}_r(\mathbb{R})^*$.

Det er klart, at vi i definitionen ikke behøver at indskrænke os til kun at betragte matricer med reelle koefficienter. Vi kan betragte matricer med koefficienter i en vilkårlig given ring Λ. De udgør en ring $\mathrm{Mat}_r(\Lambda)$. Gruppen af invertible elementer i $\mathrm{Mat}_r(\Lambda)$ betegnes $\mathrm{GL}_r(\Lambda)$. Velkendte eksempler er ringene $\mathrm{Mat}_r(\mathbb{C})$ og $\mathrm{Mat}_r(\mathbb{Z})$ af matricer med henholdsvis komplekse og hele koefficienter. Ringen $\mathrm{Mat}_r(\mathbb{Z}/n)$ består af matricer, hvis koefficienter er restklasser modulo n. Matrixringen $\mathrm{Mat}_r(\mathbb{Z}/n)$ er en endelig ring med n^{r^2} elementer.

(1.10) Karakteristik og primring. Lad Λ være en ring, og lad os her med 0_Λ og 1_Λ betegne nul- og et-elementet. For et element λ i Λ betegner vi, som sædvanlig i en additiv gruppe, med $n\lambda$ den n'te (additive) potens af λ, altså $n\lambda = \lambda + \cdots + \lambda$ med n led, når $n > 0$, $0\lambda = 0_\Lambda$, og $(-n)\lambda = n(-\lambda)$ for $n > 0$. For den første potens har vi $1\lambda = \lambda = 1_\Lambda\lambda$. Potensreglerne er ligningerne,

$$(n+m)\lambda = n\lambda + m\lambda, \tag{1}$$

$$(nm)\lambda = n(m\lambda), \tag{2}$$

$$n(\lambda + \mu) = n\lambda + n\mu. \tag{3}$$

Vi kan specielt betragte (additive) potenser $n1_\Lambda$ af et-elementet. Herom gælder, for $n \in \mathbb{Z}$ og $\lambda \in \Lambda$, at

$$\lambda(n1_\Lambda) = (n1_\Lambda)\lambda = n\lambda. \tag{1.10.1}$$

Betragt for eksempel den anden ligning. For $n > 0$ følger den af udregningen,

$$(n1_\Lambda)\lambda = (\overbrace{1_\Lambda + \cdots + 1_\Lambda}^{n})\lambda = \overbrace{\lambda + \cdots + \lambda}^{n} = n\lambda,$$

hvor vi i den midterste ligning brugte den distributive lov og at 1_Λ er neutralt element for multiplikationen i Λ. For $n = 0$ følger ligningen af udregningen,

$$(01_\Lambda)\lambda = 0_\Lambda\lambda = 0_\Lambda = 0\lambda,$$

og for negativ „eksponent" følger ligningen af udregningen, for $n > 0$,

$$((-n)1_\Lambda)\lambda = (-(n1_\Lambda))\lambda = -((n1_\Lambda)\lambda) = -(n\lambda) = (-n)\lambda.$$

Ligningen $\lambda(n1_\Lambda) = n\lambda$ indses tilsvarende.

Hvis et-elementet 1_Λ med hensyn til additionen i Λ har endelig orden p, siges ringen Λ at have *karakteristik* p. Hvis 1_Λ har uendelig orden, siges Λ at have *karakteristik* 0. Den cykliske (additive) undergruppe frembragt af 1_Λ er delmængden,

$$\{n1_\Lambda \mid n \in \mathbb{Z}\}. \tag{1.10.2}$$

Denne delmængde er en delring af Λ. Det følger nemlig af den første potensregel, at delmængden er stabil under addition. Af (1.10.1) og den anden potensregel følger, at $(n1_\Lambda)(m1_\Lambda) = n(m1_\Lambda) = (nm)1_\Lambda$, og heraf fremgår, at delmængden er stabil under multiplikation. Endelig ligger $-1_\Lambda = (-1)1_\Lambda$ i delmængden. Følgelig er delmængden en delring. Den kaldes *primringen* i Λ. Det følger af udregningen $(n1_\Lambda)(m1_\Lambda) = (nm)1_\Lambda$, at primringen er en kommutativ delring af Λ. Når primringen er endelig, er karakteristikken dens elementantal, og når den er uendelig, er karakteristikken 0.

Lad os understrege, at Λ har karakteristik 0, hvis og kun hvis summerne,

$$\overbrace{1_\Lambda + \cdots + 1_\Lambda}^{n}, \tag{1.10.3}$$

for $n > 0$, alle er forskellige fra 0_Λ. Hvis ringen har karakteristik større end 0, er karakteristikken det mindste positive tal n således, at summen (1.10.3) er nul-elementet 0_Λ.

Bemærk, at karakteristik 1 indtræffer, hvis og kun hvis $1_\Lambda = 0_\Lambda$, altså hvis og kun hvis Λ er nul-ringen.

(1.11) Integritetsområde og skævlegeme. I ringen Λ siges *nul-reglen* at gælde, hvis

$$\lambda\mu = 0 \implies \lambda = 0 \text{ eller } \mu = 0, \tag{1.11.1}$$

eller, ækvivalent,

$$\lambda \neq 0 \text{ og } \mu \neq 0 \implies \lambda\mu \neq 0. \tag{1.11.2}$$

Ringen Λ kaldes et *integritetsområde*, hvis nul-reglen gælder og Λ ikke er nul-ringen.

Ringen Λ kaldes et *skævlegeme*, hvis alle elementer forskellige fra nul i Λ er invertible og Λ ikke er nul-ringen. Et *legeme* er et kommutativt skævlegeme.

(1.12) Observation. (1) Ethvert skævlegeme Λ er et integritetsområde. Antag nemlig, at vi for elementer λ, μ i et skævlegeme Λ har $\lambda\mu = 0$. Det skal vises, at en af faktorerne er nul. Antag for eksempel, at $\mu \neq 0$. Da er μ invertibel, og ved multiplikation med μ^{-1} fås

$$0 = 0\mu^{-1} = \lambda\mu\mu^{-1} = \lambda 1 = \lambda.$$

Altså er $\lambda = 0$.

(2) For et integritetsområde (og specielt for et skævlegeme) Λ er karakteristikken enten 0 eller et primtal. Da Λ ikke er nul-ringen, er det nemlig udelukket, at karakteristikken kan være 1. Hvis karakteristikken, n, ikke er 0 eller et primtal, må den derfor være et sammensat tal, $n = qd$, hvor $1 < q, d < n$. Da n er ordenen af 1_Λ og $q < n$, er $q1_\Lambda \neq 0_\Lambda$. Af samme grund er $d1_\Lambda \neq 0_\Lambda$. Men så er ligningerne,

$$(q1_\Lambda)(d1_\Lambda) = (qd)1_\Lambda = n1_\Lambda = 0_\Lambda,$$

i modstrid med, at nul-reglen gælder i Λ.

(3) I et integritetsområde gælder *forkortningsreglen:* Af $\lambda\mu = \lambda\nu$ følger, når $\lambda \neq 0$, at $\mu = \nu$. Dette ses ved at anvende (1.11.1) med $\mu := \mu - \nu$.

(1.13) Eksempel. (0) Nul-ringen har som nævnt karakteristik 1, og den er ikke et integritetsområde og ikke et legeme.

(1) Talringe har tallet 1 som et-element, og vi har $n1 = n$ for $n \in \mathbb{Z}$. Enhver talring har altså karakteristik 0, og primring $\mathbb{Z}$. Alle talringe er integritetsområder, og ringene $\mathbb{Q}$, $\mathbb{R}$, og $\mathbb{C}$ er legemer.

(2) En funktionsring R, som er en delring af ringen $\mathcal{F}(X, \mathbb{C})$ af komplekse funktioner på X, har den konstante funktion 1 som et-element. Funktionen $n1_R$, for $n \in \mathbb{Z}$, er den konstante funktion n. En sådan funktionsring har altså karakteristik 0 (med mindre X er den tomme mængde), og primringen består af de konstante funktioner med heltalsværdier. En funktionsring er normalt ikke et integritetsområde: hvis funktionen f er nul på delmængden Y af X og g er nul på delmængden Z og $Y \cup Z = X$, så er produktfunktionen fg nul-funktionen.

(3) Et-elementet i matrixringen $\mathrm{Mat}_r(\mathbb{R})$ er enhedsmatricen 1_r, og $n1_r$ er skalarmatricen med tallet n overalt i diagonalen. Primringen består altså af skalarmatricer med et helt tal i diagonalen. Matrixringen har således karakteristik 0. Når $r \geqslant 2$ er matrixringen ikke et integritetsområde.

(4) Et-elementet i restklasseringen $\mathbb{Z}/d$, for $d \geqslant 1$, er restklassen $[1]$, og $n[1] = [n]$. Primringen er altså hele restklasseringen, og karakteristikken er d.

(1.14) Sætning. *Lad Λ være en ring med p elementer, hvor p er et primtal. Da er Λ et legeme, og bortset fra valg af betegnelser er Λ lig med restklasseringen $\mathbb{Z}/p$.*

Bevis. Øjensynlig er Λ ikke nul-ringen. For at vise, at Λ er et legeme, skal det derfor vises, at Λ er kommutativ og at hvert element $\lambda \neq 0_\Lambda$ har en invers. Betragt, for $\lambda \neq 0_\Lambda$, den additive cykliske undergruppe frembragt af λ, bestående af alle elementer $k\lambda$ for $k \in \mathbb{Z}$. Da ordenen $|\Lambda| = p$ er et primtal, må undergruppen være hele Λ. Specielt ligger 1_Λ i undergruppen. Altså er $1_\Lambda = k\lambda$ med $k \in \mathbb{Z}$. Af ligningen $1_\Lambda = k\lambda$ og (1.10.1) får vi derfor ligningerne,

$$1_\Lambda = (k1_\Lambda)\lambda = \lambda(k1_\Lambda).$$

Af ligningerne fremgår, at λ er invertibel. Yderligere fremgår det, at den inverse til λ ligger i primringen. Den inverse til den inverse er λ selv. Altså ligger hvert element $\lambda \neq 0_\Lambda$ i primringen. Det følger, at primringen i Λ er hele Λ.

Da primringen altid er kommutativ, er Λ kommutativ, og altså et legeme. Som kommutativ gruppe er Λ den cykliske undergruppe frembragt af 1_Λ som har orden p, og derfor er Λ isomorf med restklassegruppen $\mathbb{Z}/p$, idet elementet $n1_\Lambda$ svarer til restklassen $[n]$ modulo p. Det er klart, at under denne isomorfi svarer produkt $(n1_\Lambda)(m1_\Lambda) = (nm)1_\Lambda$ i Λ til produkt $[n][m] = [nm]$ af restklasser. Hermed er den sidste påstand i sætningen eftervist. $\square$

(1.15) Notation. Lad p være et primtal. Det følger af Sætning (1.14), at restklasseringen $\mathbb{Z}/p$ er et legeme. Dette følger naturligvis også af tidligere resultater om restklasseringene: I almindelighed, for et naturligt tal $n \geqslant 2$, er de invertible restklasser i $\mathbb{Z}/n$ de primiske restklasser. Det er altså netop, når n er et primtal, at de invertible restklasser er samtlige restklasser $[1], \dots, [n-1]$ forskellige fra $[0]$, dvs at $\mathbb{Z}/n$ er et legeme.

Legemet $\mathbb{Z}/p$ spiller så stor en rolle i anvendelser af algebra, at det har fået en særlig notation: det betegnes $\mathbb{F}_p$. For hver primtalspotens q findes faktisk et endeligt legeme med q elementer, og det betegnes ofte $\mathbb{F}_q$. Det er altså *kun*, når q er et primtal, at $\mathbb{F}_q$ betegner restklasseringen $\mathbb{Z}/q$.

(1.16) Definition. Et element λ i en ring Λ kaldes *involutorisk*, hvis $\lambda^2 = 1_\Lambda$, det kaldes *idempotent*, hvis $\lambda^2 = \lambda$, og det kaldes *nilpotent*, hvis $\lambda^N = 0_\Lambda$ for en passende stor eksponent N. De tre betingelser kan skrives,

$$(\lambda - 1)(\lambda + 1) = 0, \quad \lambda(\lambda - 1) = 0, \quad \overbrace{\lambda \cdots \lambda}^{N} = 0.$$

Heraf ses, at hvis nul-reglen gælder i Λ, så er ± 1 de eneste involutoriske elementer, 0 og 1 er de eneste idempotente elementer, og 0 er det eneste nilpotente element.

(1.17) Opgaver.

1. Er delmængden af lige tal en delring af $\mathbb{Z}$?

2. Vis, at polynomiumsfunktionerne $g\colon \mathbb{R} \to \mathbb{R}$, som opfylder $g(0) \in \mathbb{Z}$, udgør en delring af $\mathcal{Pol}(\mathbb{R})$.

3. Lad Λ_1 og Λ_2 være ringe. Gør rede for hvorledes produktmængden $\Lambda := \Lambda_1 \times \Lambda_2$ naturligt organiseres som en ring (*produktringen*). Kan Λ være et integritetsområde? Hvordan bestemmes karakteristikken af Λ?

4. Lad p være et primtal. Vis, at mængden af rationale tal af formen a/s, hvor $a, s \in \mathbb{Z}$ og p ikke går op i s, udgør en delring af $\mathbb{Q}$. Delringen betegnes $\mathbb{Z}_{(p)}$. Ligger brøken $2/14$ i $\mathbb{Z}_{(2)}$?

5. Lad f være et naturligt tal. Vis, at mængden af rationale tal af formen a/f^n, hvor $a \in \mathbb{Z}$ og $n = 0, 1, \dots$, udgør en delring af $\mathbb{Q}$. Delringen betegnes $\mathbb{Z}[1/f]$. Ligger brøken $2/14$ i $\mathbb{Z}[1/7]$? Bestem, for et primtal p, fællesmængden $\mathbb{Z}_{(p)} \cap \mathbb{Z}[1/p]$.

6. Vis, at funktionsringen $\mathcal{F}(X)$ af reelle funktioner på X ikke er et integritetsområde, når X indeholder mere end et element. Vis, at ringen $\mathcal{C}^\infty(I)$ af $\mathcal{C}^\infty$-funktioner på et interval I ikke er et integritetsområde. Vis, at delringen $\mathcal{P}ol(I)$ af polynomiumsfunktioner er et integritetsområde.

7. For hvilke åbne delmængder $\Omega \subseteq \mathbb{C}$ er ringen $\mathcal{H}(\Omega)$ af holomorfe funktioner på Ω et integritetsområde?

8. Vis, at elementerne i funktionsringen $\mathcal{F}(X, \mathbb{F}_2)$ svarer bijektivt til delmængderne af X. Sum og produkt af funktioner svarer altså til to kompositioner i mængden $\mathcal{P}(X)$ af delmængder af X. Beskriv de to kompositioner.

9. Vis, at en matrixring $\mathrm{Mat}_r(\Lambda)$ for $r \geqslant 2$ ikke kan være et integritetsområde.

10. Vis, at hvis en ring Λ har primtalskarakteristik p, så er $(1+\lambda)^p = 1 + \lambda^p$ for alle $\lambda \in \Lambda$.

11. For hvilke værdier af karakteristikken af Λ gælder $1_\Lambda \neq -1_\Lambda$.

12. Vis, at en delring af et integritetsområde selv er et integritetsområde. Er en delring af et legeme selv et legeme?

13. Vis, at et endeligt integritetsområde er et skævlegeme. [Det er i øvrigt en sætning af Wedderburn, at et endeligt skævlegeme er kommutativt.]

14. Vis, at hvis der for alle λ i ringen Λ gælder $\lambda^2 = \lambda$, så er Λ kommutativ.

15. *Vis, at hvis der for alle λ i ringen Λ gælder $\lambda^3 = \lambda$, så er Λ kommutativ.

16. Hvilke elementer i $\mathbb{Z}/8$ er idempotente? involutoriske? nilpotente?

17. Vis, at der i ringen $\mathrm{Mat}_2(\mathbb{R})$ findes (ikke-trivielle) matricer, der er involutoriske, og idempotente, og nilpotente.

18. Hvor mange elementer indeholder ringen $\mathrm{Mat}_2(\mathbb{F}_2)$? Beskriv gruppen $\mathrm{Mat}_2(\mathbb{F}_2)^*$.

19. *Lad R være en kommutativ ring. Vis, at en matrix $A \in \mathrm{Mat}_r(R)$ er invertibel, hvis og kun hvis determinanten $\det(A)$ er et invertibelt element i R.

Antag, at L er et legeme. Tro på, at L^r, ganske som for talrummene (dvs for $L = \mathbb{R}$ og $L = \mathbb{C}$), er et *vektorrum* over L, af dimension r, og at de lineære afbildninger $L^r \to L^r$ er afbildningerne af formen $x \mapsto Ax$ med en matrix $A \in \mathrm{Mat}_r(L)$. Afbildningen er invertibel, hvis og kun hvis søjlerne i matricen A er lineært uafhængige. Hvis legemet L er endeligt, med q elementer, kan vi herved bestemme ordenen af gruppen $\mathrm{GL}_r(L)$ af invertible matricer. Der er q^r mulige søjler. For en matrix i $\mathrm{GL}_r(L)$ må første søjle ikke være nul, hvilket giver $q^r - 1$ muligheder for første søjle. Anden søjle må ikke ligge i det 1-dimensionale underrum frembragt af første søjle, hvilket giver $q^r - q$ muligheder for anden søjle, osv. Vis formlen,

$$|\,\mathrm{GL}_r(L)| = (q^r - 1)(q^r - q) \cdots (q^r - q^{r-1}).$$

20. Kvaternion-enhederne $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ tilhører ringen $\mathrm{Mat}_2(\mathbb{C})$. Vis, at matricerne af formen $a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, for reelle tal (a, b, c, d), udgør en delring $\mathbb{H}$ af $\mathrm{Mat}_2(\mathbb{C})$. Vis, at $\mathbb{H}$ er et skævlegeme.

21. I hvilken situation indgår følgende opskrift: „ombyt diagonalelementerne og skift fortegn udenfor"? Lær opskriften udenad, og prøv den! [Vink: Det drejer sig om invertering af (2×2)-matricer. Opskriften fører fra

$$\alpha = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \quad \text{til} \quad \alpha^{\mathrm{J}} := \begin{bmatrix} d & -c \\ -b & a \end{bmatrix};$$

Vis, at $\alpha\alpha^{\mathrm{J}} = \alpha^{\mathrm{J}}\alpha = (\det\alpha)\, 1_2$, og udled en formel for α^{-1}.]

Inverter følgende matricer i $\mathrm{GL}_2(\mathbb{Z})$:

$$\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix}.$$

22. *Vis, at ingen ring Λ kan have præcis 5 enheder.

23. I mængden $\mathbb{R}$ defineres *tropisk addition* $\oplus$ og *tropisk multiplikation* $\odot$ ved

$$x \oplus y := \min\{x, y\}, \qquad x \odot y := x + y.$$

Hvilke af betingelserne for en ring er opfyldt for $(\mathbb{R}, \oplus, \odot)$? Og hvilke er opfyldt, hvis man med oplagte kompositioner tilføjer $+\infty$ til $\mathbb{R}$?

24. Vis, at $\mathrm{Mat}_p(\Lambda) \times \mathrm{Mat}_q(\Lambda)$ naturligt er en delring af $\mathrm{Mat}_{p+q}(\Lambda)$.

2. Ideal og kvotientring.

(2.1) Indledning. En ring er specielt en kommutativ gruppe mht addition, så for hver given undergruppe i ringens additive gruppe har vi en naturlig addition i den tilsvarende mængde af sideklasser. Men i almindelighed har vi ingen naturlig multiplikation af sideklasser. *Idealer*, som vi indfører nedenfor, kan opfattes som de undergrupper i en ring, for hvilke kvotientgruppen naturligt også kan organiseres med en multiplikation.

I det følgende vil vi udelukkende beskæftige os med kommutative ringe. Vi lader R betegne en fast kommutativ ring.

(2.2) Ideal. En delmængde $\mathfrak{a}$ af R kaldes et *ideal*, hvis $\mathfrak{a}$ er en undergruppe mht additionen i R og der for alle $a \in \mathfrak{a}$ og $r \in R$ gælder, at $ra \in \mathfrak{a}$. Det er nok at kræve, at følgende betingelse er opfyldt:

(†) Delmængden $\mathfrak{a}$ er stabil under addition, den indeholder nul-elementet 0, og for alle elementer $a \in \mathfrak{a}$ og $r \in R$ er $ra \in \mathfrak{a}$.

Det følger nemlig af den sidste del af betingelsen, anvendt med $r := -1$, at for $a \in \mathfrak{a}$ er $-a = (-1)a \in \mathfrak{a}$, og så er det klart, at betingelsen medfører, at $\mathfrak{a}$ er en undergruppe.

Bemærk, at den sidste del af betingelsen (†) er (meget) stærkere end at delmængden er stabil under multiplikation.

Det er klart, at delmængden $\{0\}$ er et ideal, og at R, opfattet som delmængde af sig selv, er et ideal i R. Idealerne $\{0\}$ og R kaldes de *trivielle idealer*. Et ideal, der er en ægte delmængde af R, kaldes et *ægte ideal*.

I nul-ringen er der kun én ikke-tom delmængde, og den er et ideal. I nul-ringen er der kun ét trivielt ideal, i alle andre ringe er de to trivielle idealer forskellige. I nul-ringen er der ingen ægte idealer, i alle andre ringe er $\{0\}$ et ægte ideal.

(2.3) Sætning. *Idealerne i ringen $\mathbb{Z}$ er netop delmængderne af formen $\mathbb{Z}n$ for $n \geqslant 0$.*

Bevis. Et ideal i en ring er specielt en undergruppe i ringens additive gruppe. I den additive gruppe $\mathbb{Z}$ er undergrupperne de cykliske undergrupper $\mathbb{Z}n$ for $n \geqslant 0$; blandt disse undergrupper skal eventuelle idealer i $\mathbb{Z}$ altså søges. Et element i $\mathbb{Z}n$ har formen qn med $q \in \mathbb{Z}$, og efter multiplikation med $r \in \mathbb{Z}$ får vi $r(qn) = (rq)n \in \mathbb{Z}n$. Heraf fremgår, at undergruppen $\mathbb{Z}n$ er et ideal. Alle undergrupperne $\mathbb{Z}n$ er altså idealer. ▯

(2.4) Eksempel. (1) I et legeme L findes der kun trivielle idealer. Antag nemlig, at $\mathfrak{a}$ er et ideal i L og at $\mathfrak{a} \neq \{0\}$; det skal vises, at $\mathfrak{a} = L$. Da $\mathfrak{a} \neq \{0\}$, findes et element $a \neq 0$ i $\mathfrak{a}$. Produktet ra ligger i $\mathfrak{a}$ for hvert element $r \in L$, og specielt for $r := a^{-1}$. Følgelig er $1 = a^{-1}a \in \mathfrak{a}$. Heraf følger videre, at $r = r1 \in \mathfrak{a}$ for alle $r \in L$. Altså er $\mathfrak{a} = L$.

Talringene $\mathbb{Q}$, $\mathbb{R}$, og $\mathbb{C}$ er legemer. I disse ringe findes altså kun de trivielle idealer.

(2) Idealer i en funktionsring, altså i en delring af $\mathcal{F}(X)$, fremkommer ofte ved at betragte funktioner, som er nul på visse delmængder af X.

Betragt for eksempel ringen $\mathcal{C}(I)$ af kontinuerte reelle funktioner på et interval I. Hvis a er et tal i I, kan vi betragte delmængden $\mathcal{I}_a$ af kontinuerte funktioner $f : I \to \mathbb{R}$, som opfylder, at $f(a) = 0$. Hvis $f(a) = g(a) = 0$, så er $(f + g)(a) = 0$, idet sumfunktionen

$f + g$ er defineret ved $(f + g)(t) = f(t) + g(t)$. Tilsvarende ses, at hvis $f(a) = 0$, og g er en vilkårlig funktion i $\mathcal{C}(I)$, så er $(gf)(a) = 0$. Altså er $\mathcal{I}_a$ et ideal i $\mathcal{C}(I)$.

Tilsvarende ses, at i ringen $\mathbb{R}^{\mathbb{N}}$ af alle reelle talfølger udgør følgerne, der er 0 fra et vist trin (dvs følger $(a_1, a_2, \dots)$ for hvilke der findes et N så $a_n = 0$ for $n \geqslant N$), et ideal.

(2.5) Hovedidealer. For et givet element a i ringen R kan vi betragte delmængden,

$$Ra := \{ra \mid r \in R\}.$$

Delmængden er et ideal. For to elementer i delmængden, r_1a og r_2a, får vi nemlig, at $r_1a + r_2a = (r_1 + r_2)a \in Ra$, og er ra i delmængden og s et vilkårligt element i R, får vi, at $s(ra) = (sr)a \in Ra$. Endelig er $0 = 0a \in Ra$. Delmængden Ra er derfor et ideal. Bemærk, at det givne element a ligger i idealet Ra, idet vi har $a = 1a$. Yderligere gælder, at Ra er det mindste ideal, der indeholder a. For et ideal $\mathfrak{a}$, som indeholder a, må vi nemlig have $ra \in \mathfrak{a}$ for alle $r \in R$, og altså er $\mathfrak{a} \supseteq Ra$.

Idealet Ra kaldes *hovedidealet frembragt* af elementet a, og det betegnes også (a). Et ideal i R, der har formen (a) med et element $a \in R$, kaldes et *hovedideal*.

Hovedidealet frembragt af nul-elementet 0 består af alle elementer $r0 = 0$, altså alene af 0; vi har altså $(0) = \{0\}$. Hovedidealet frembragt af et-elementet 1 består af alle elementer $r1 = r$, altså af alle elementer i R; vi har altså $(1) = R$. De to trivielle idealer i R er således hovedidealerne (0) og (1).

(2.6) Eksempel. I et legeme er de trivielle idealer (0) og (1) de eneste idealer. Det er indholdet af Sætning (2.3), at i ringen $\mathbb{Z}$ er alle idealer hovedidealer.

For at give et eksempel på et ideal, der ikke er et hovedideal, betragtes ringen $R := \mathbb{R}^{\mathbb{N}}$ af alle reelle talfølger $(f_1, f_2, \dots)$. Det påstås, at idealet $\mathcal{I}$ bestående af de følger, der er 0 fra et vist trin, ikke kan være et hovedideal. Betragt nemlig, for en følge $a = (a_1, a_2, \dots)$ i $\mathcal{I}$, hovedidealet Ra. Da $a \in \mathcal{I}$, er følgen a nul fra et vist trin, dvs der findes et naturligt tal N således, at $a_n = 0$ for $n \geqslant N$. En vilkårlig følge g i Ra har formen $g = (f_1a_1, f_2a_2, \dots)$; altså er $g_n = f_na_n = 0$ for $n \geqslant N$. Betragter vi specielt følgen h, hvor $h_N = 1$ og $h_n = 0$ for $n \neq N$, fremgår det, at $h \in \mathcal{I}$ og $h \notin Ra$. Lighedstegnet $\mathcal{I} = Ra$ er altså udelukket for hvert element $a \in \mathcal{I}$. Altså er $\mathcal{I}$ ikke et hovedideal.

(2.7) Kvotientring. Lad $\mathfrak{a}$ være et ideal i ringen R. Mht addition er R en kommutativ gruppe, og $\mathfrak{a}$ er en undergruppe. Derfor kan vi betragte kvotientgruppen $R/\mathfrak{a}$. Den består som bekendt af alle sideklasser $[r] = r + \mathfrak{a}$ for $r \in R$, og addition af sideklasser er bestemt ved ligningen,

$$[r] + [s] = [r + s]. \tag{2.7.1}$$

Med denne komposition af sideklasser er $R/\mathfrak{a}$ en kommutativ gruppe. Vi kan yderligere indføre et veldefineret produkt af sideklasser, bestemt ved ligningen,

$$[r][s] = [rs]. \tag{2.7.2}$$

At produktet er veldefineret betyder, at højresiden ikke afhænger af de repræsentanter r og s, der er valgt i sideklasserne på venstresiden. Antag hertil, at $[r'] = [r]$ og $[s'] = [s]$; det skal vises, at $[r's'] = [rs]$. Da $[r'] = [r]$, er $r' - r \in \mathfrak{a}$. Tilsvarende er $s' - s \in \mathfrak{a}$. Idet vi benytter idealegenskaberne, følger det, at

$$r's' - rs = r'(s' - s) + s(r' - r) \in \mathfrak{a}.$$

Altså er $[r's'] = [rs]$, som ønsket. Hermed er eftervist, at der er en veldefineret multiplikation i mængden af sideklasser, bestemt ved ligningen (2.7.2).

Mængden $R/\mathfrak{a}$ af sideklasser modulo idealet $\mathfrak{a}$, med addition og multiplikation bestemt ved (2.7.1) *og* (2.7.2)*, er en kommutativ ring med nul-elementet* [0] *og et-elementet* [1].

Hertil bemærker vi, at vi allerede ved, at med additionen udgør sideklasserne en kommutativ gruppe med sideklassen [0] som nul-element. Det skal altså yderligere vises, at multiplikation af sideklasser er kommutativ og associativ, at sideklassen [1] er neutralt element, og at multiplikation af sideklasser er distributiv mht addition.

Vi viser den distributive lov. Betragt altså tre sideklasser $[r]$, $[s]$ og $[t]$. Vi skal eftervise ligningen i $R/\mathfrak{a}$,

$$[r]\big([s] + [t]\big) = [r][s] + [r][t].$$

Venstresiden er, ifølge (2.7.1) og (2.7.2), sideklassen $[r][s + t] = [r(s + t)]$. Tilsvarende er højresiden sideklassen $[rs + rt]$. Da den distributive lov gælder i R, er $r(s + t) = rs + rt$. Altså gælder den distributive lov i $R/\mathfrak{a}$.

De øvrige betingelser vises tilsvarende.

Ringen $R/\mathfrak{a}$ af sideklasser modulo $\mathfrak{a}$ kaldes *kvotientringen*.

(2.8) Eksempel. Idealerne i $\mathbb{Z}$ er hovedidealerne $(n) = \mathbb{Z}n$ for $n \geqslant 0$. For $n \geqslant 1$ er kvotientringen $\mathbb{Z}/(n)$ øjensynlig restklasseringen $\mathbb{Z}/n$. Vi har $(0) = \{0\}$, så sideklasser modulo (0) er et-punkts-delmængderne af $\mathbb{Z}$. Kvotientringen $\mathbb{Z}/(0)$ kan altså identificeres med $\mathbb{Z}$. Bemærk, at ringen $\mathbb{Z}/(n)$ i alle tilfælde har karakteristik n.

(2.9) Primideal og maksimalideal. Et ideal $\mathfrak{p}$ i R kaldes et *primideal*, hvis $\mathfrak{p}$ er et ægte ideal og der for alle a, b i R gælder betingelsen,

$$ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ eller } b \in \mathfrak{p}. \tag{2.9.1}$$

Et ideal $\mathfrak{m}$ i R kaldes et *maksimalideal*, hvis $\mathfrak{m}$ er maksimalt blandt de ægte idealer. Det kræves altså, at $\mathfrak{m}$ er et ægte ideal og at $\mathfrak{m}$ er maksimalt, med hensyn til inklusion af delmængder, blandt de ægte idealer. Det sidste betyder, at intet ægte ideal er strengt større end $\mathfrak{m}$, og det kan udtrykkes ved betingelsen, for alle idealer $\mathfrak{a}$ i R,

$$\mathfrak{m} \subseteq \mathfrak{a} \subset R \implies \mathfrak{a} = \mathfrak{m}, \tag{2.9.2}$$

eller, ækvivalent,

$$\mathfrak{m} \subset \mathfrak{a} \subseteq R \implies \mathfrak{a} = R. \tag{2.9.3}$$

Bemærk, at betingelserne er opfyldt for det trivielle ideal R, men at begge definitioner kræver, at idealet skal være ægte. Det trivielle ideal R er altså hverken et primideal eller et maksimalideal.

(2.10) Observation. Det trivielle ideal (0) i R kan være et primideal og det kan være et maksimalideal. Vi bemærker først, at (0) er et ægte ideal, hvis og kun hvis R består af mere end nul-elementet, altså hvis og kun hvis R ikke er nul-ringen. Antag derfor, at R ikke er nul-ringen. Idealet (0) består alene af 0, så $a \in (0)$ betyder, at $a = 0$. Betingelsen (2.9.1), for $\mathfrak{p} := (0)$, er derfor nul-reglen,

$$ab = 0 \implies a = 0 \text{ eller } b = 0.$$

Idealet (0) er derfor et primideal i R, hvis og kun hvis R er et integritetsområde.

Vi påstår videre, at (0) er et maksimalideal, hvis og kun hvis R er et legeme. Antag nemlig først, at R er et legeme. Vi efterviser betingelsen (2.9.3), og antager for idealet $\mathfrak{a}$, at $(0) \subset \mathfrak{a}$. Det følger, at der i $\mathfrak{a}$ findes et element $a \neq 0$. Da R er et legeme, er a invertibelt. Følgelig er $1 = a^{-1}a \in \mathfrak{a}$. Heraf følger videre, for hvert element $r \in R$, at $r = r1 \in \mathfrak{a}$. Altså er $\mathfrak{a} = R$.

Antag omvendt, at (0) er et maksimalideal. Det skal vises, at hvert element $a \neq 0$ i R er invertibelt. Betragt hertil hovedidealet (a). Det indeholder a, og specielt er $(0) \subset (a)$. Da (0) er et maksimalideal, følger det, at $(a) = R$. Specielt ligger 1 i (a). Følgelig findes et element $r \in R$ således, at $1 = ra$. Ligningen $1 = ra$ udsiger, at a er invertibel, med r som det inverse element.

(2.11) Sætning. *Primidealerne i ringen $\mathbb{Z}$ er hovedidealerne (p), hvor $p = 0$ eller p er et primtal. Maksimalidealerne i $\mathbb{Z}$ er hovedidealerne (p), hvor p er et primtal.*

Bevis. Idealerne i $\mathbb{Z}$ er, ifølge (2.3), hovedidealerne (p), for $p \geqslant 0$. Øjensynlig er (p) et ægte ideal, hvis og kun hvis $p \neq 1$. Idealet (0) er et primideal, fordi $\mathbb{Z}$ er et integritetsområde, og det er ikke et maksimalideal, fx fordi $(0) \subset (2) \subset \mathbb{Z}$.

Vi betragter derfor et ideal (p), hvor $p \geqslant 2$. Vi har $a \in (p)$, hvis og kun hvis $p|a$. Betingelsen (2.9.1), for $\mathfrak{p} := (p)$, er altså følgende:

$$p|ab \implies p|a \text{ eller } p|b.$$

Det er velkendt, at denne betingelse er opfyldt, når p er et primtal. Omvendt, hvis p er sammensat, så er $p = ab$, hvor $1 < a, b < p$, og så er p divisor i ab uden at p er divisor i nogen af faktorerne. Vi har således vist, for $p \geqslant 2$, at (p) er et primideal, hvis og kun hvis p er et primtal. Hermed er sætningens første påstand bevist.

Betragt betingelsen (2.9.2) for $\mathfrak{m} := (p)$. Idealerne i $\mathbb{Z}$ er hovedidealer, så vi kan antage i (2.9.2), at $\mathfrak{a} = (d)$, hvor $d \geqslant 0$. Betingelsen er altså følgende, for alle $d \geqslant 0$,

$$(p) \subseteq (d) \subset \mathbb{Z} \implies (d) = (p).$$

Vi har $(p) \subseteq (d)$, hvis og kun hvis $d\,|\,p$; da d og p ikke er negative, har vi $(d) = (p)$, hvis og kun hvis $d = p$. Endelig er $(d) \subset \mathbb{Z}$, hvis og kun hvis $d \neq 1$. Betingelsen er derfor ækvivalent med følgende, for alle $d \geqslant 0$,

$$d\,|\,p \text{ og } d \neq 1 \implies d = p.$$

Betingelsen udtrykker, at den eneste (positive) divisor forskellig fra 1 i p er p, altså at p er et primtal.

Vi har således vist, at (p) er et maksimalideal, hvis og kun hvis p er et primtal. Hermed er sætningens anden påstand bevist. □

(2.12) Sætning. *Et ideal $\mathfrak{p}$ i R er et primideal, hvis og kun hvis kvotientringen $R/\mathfrak{p}$ er et integritetsområde. Et ideal $\mathfrak{m}$ i R er et maksimalideal, hvis og kun hvis kvotientringen $R/\mathfrak{m}$ er et legeme.*

Bevis. Det kræves for primidealer og maksimalidealer, at de skal være ægte, og det kræves for integritetsområder og legemer, at de ikke må være nul-ringen. Et ideal er ægte, hvis og kun hvis den tilhørende kvotientring ikke er nul-ringen. Vi kan derfor i resten af beviset antage, at $\mathfrak{p}$ og $\mathfrak{m}$ er ægte idealer. Det er påstanden, at betingelsen (2.9.1) gælder for $\mathfrak{p}$, hvis og kun hvis nul-reglen gælder i $R/\mathfrak{p}$, og at (2.9.3) gælder for $\mathfrak{m}$, hvis og kun hvis alle elementer forskellige fra nul-elementet i $R/\mathfrak{m}$ er invertible.

Antag først, at $\mathfrak{p}$ er et primideal. Betragt to sideklasser A, B i $R/\mathfrak{p}$ således, at AB er nul-elementet [0]. Vi kan antage, at $A \neq [0]$, og skal så vise, at $B = [0]$. Vælg elementer $a, b \in R$ således, at $A = [a]$ og $B = [b]$. Produktet AB er så sideklassen $[ab]$. Ifølge antagelsen er $[ab] = [0]$, dvs $ab \in \mathfrak{p}$, og $[a] \neq [0]$, dvs $a \notin \mathfrak{p}$. Af (2.9.1) følger derfor, at $b \in \mathfrak{p}$. Følgelig er $B = [b] = [0]$.

Antag omvendt, at nul-reglen gælder i $R/\mathfrak{p}$. For at vise (2.9.1) antages, at $ab \in \mathfrak{p}$ og at $a \notin \mathfrak{p}$. Det skal vises, at $b \in \mathfrak{p}$. Af antagelsen følger, at $[a][b] = [ab] = [0]$ og at $[a] \neq [0]$. Nul-reglen medfører derfor, at $[b] = [0]$, dvs $b \in \mathfrak{p}$.

Antag dernæst, at $\mathfrak{m}$ er et maksimalideal. Det skal vises, at hver sideklasse A forskellig fra nul-klassen [0] i $R/\mathfrak{m}$ er invertibel. Vælg hertil et element $a \in R$ således, at $A = [a]$. Da $A \neq [0]$, er $a \notin \mathfrak{m}$. Betragt summen,

$$\mathfrak{m} + (a) = \{x + sa \mid x \in \mathfrak{m} \text{ og } s \in R\}.$$

Summen er en undergruppe, og hvis $x \in \mathfrak{m}$ og $s \in R$, får vi for hvert element $r \in R$, at $r(x + sa) = rx + rsa \in \mathfrak{m} + (a)$. Altså er summen et ideal i R. Vi har $\mathfrak{m} \subseteq \mathfrak{m} + (a)$, thi når $x \in \mathfrak{m}$, er $x = x + 0a \in \mathfrak{m} + (a)$. Yderligere er $a = 0 + 1a \in \mathfrak{m} + (a)$, og $a \notin \mathfrak{m}$. Altså er $\mathfrak{m} \subset \mathfrak{m} + (a)$. Af (2.9.3) følger derfor, at $\mathfrak{m} + (a) = R$. Specielt ligger et-elementet 1 i $\mathfrak{m} + (a)$, så vi har en fremstilling $1 = x + sa$ med $x \in \mathfrak{m}$ og $s \in R$. Af fremstillingen følger, at $1 - sa = x \in \mathfrak{m}$. Altså er $[1] = [sa] = [s][a] = [s]A$. Vi har således vist, at A er invertibel, med sideklassen $[s]$ som den inverse.

Antag omvendt, at $R/\mathfrak{m}$ er et legeme. Vi efterviser betingelsen (2.9.3). Lad hertil $\mathfrak{a}$ være et ideal med $\mathfrak{m} \subset \mathfrak{a}$. Da inklusionen er skarp, findes et element $a \in \mathfrak{a}$ med $a \notin \mathfrak{m}$. Da $a \notin \mathfrak{m}$, er $[a] \neq [0]$. Følgelig findes en sideklasse $[s]$ i $R/\mathfrak{m}$, som er invers til $[a]$. Vi har da ligningen $[sa] = [s][a] = [1]$. Altså er $1 - sa \in \mathfrak{m}$. Da $\mathfrak{m}$ var en delmængde af $\mathfrak{a}$, følger det, at $1 - sa \in \mathfrak{a}$. Heraf ses, at $1 = (1 - sa) + sa \in \mathfrak{a}$. For hvert element $r \in R$ følger det nu, at $r = r1 \in \mathfrak{a}$. Altså er $\mathfrak{a} = R$, som ønsket.

Hermed er sætningens fire implikationer bevist. □

(2.13) Korollar. *Et maksimalideal er et primideal.*

Bevis. Påstanden følger af karakteriseringen i Sætningen, idet et legeme er et integritetsområde. □

(2.14) Eksempel. Lad p være et primtal. Af (2.11) følger, at hovedidealet (p) i $\mathbb{Z}$ er et maksimalideal. I (2.12) genfinder vi derfor resultatet fra (1.14), at kvotientringen $\mathbb{Z}/p$ er et legeme. Desuden følger det, at når $n > 1$ er sammensat, så er restklasseringen $\mathbb{Z}/n$ ikke et integritetsområde.

(2.15) Opgaver.

1. Vis, at et ideal $\mathfrak{a}$ i R er et ægte ideal, hvis og kun hvis $1 \notin \mathfrak{a}$.

2. Vis for $n, m \in \mathbb{Z}$, at $(n) = (m)$, hvis og kun hvis $n = \pm m$.

3. Betragt ringen $\mathcal{F}(X)$ af alle reelle funktioner på mængden X. Lad a være et element i X, og lad $\mathcal{I}_a$ være idealet af funktioner $f \in \mathcal{F}(X)$ med $f(a) = 0$. Vis, at $\mathcal{I}_a$ er et maksimalideal. Vis, at $\mathcal{I}_a$ er et hovedideal.

4. Vis, at når X er en endelig mængde, så har hvert maksimalideal i ringen $\mathcal{F}(X)$ formen $\mathcal{I}_a$ med et element $a \in X$.

5. Betragt ringen $\mathcal{C}(I)$ af kontinuerte funktioner på intervallet I. Lad a være et tal i I, og lad $\mathcal{I}_a$ være idealet af funktioner $f \in \mathcal{C}(I)$ med $f(a) = 0$. Vis, at $\mathcal{I}_a$ er et maksimalideal.

6. *Vis, for et interval I og $a \in I$, at idealet $\mathcal{I}_a$ i ringen $\mathcal{C}(I)$ ikke er et hovedideal.

7. *Antag, at I er et begrænset og afsluttet interval. Vis, at ethvert maksimalideal i $\mathcal{C}(I)$ er af formen $\mathcal{I}_a$ for et tal $a \in I$.

8. Vis, at hvis $\mathfrak{a}_1, \dots, \mathfrak{a}_k$ er idealer, så er både fællesmængden $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_k$ og summen $\mathfrak{a}_1 + \cdots + \mathfrak{a}_k$ igen et ideal. Vis ved et eksempel, at foreningsmængden $\mathfrak{a}_1 \cup \cdots \cup \mathfrak{a}_k$ ikke nødvendigvis er et ideal.

9. Vis, at summen af hovedidealer $Ra_1, \dots, Ra_k$ i R består af alle elementer af formen $r_1a_1 + \cdots + r_ka_k$ for $r_i \in R$. Dette ideal betegnes også $(a_1, \dots, a_k)$. Vis, for ringen $\mathbb{Z}$, at idealet $(a_1, \dots, a_k)$ er et hovedideal (d), hvor $d \geqslant 0$, og at d, når $a_i \neq 0$ for mindst et i, er den største fælles divisor for tallene $a_1, \dots, a_k$. (Heraf skrivemåden $d = (a_1, \dots, a_k)$ for den største fælles divisor.)

10. Vis, at et ideal $\mathfrak{a}$ i en delring R af en ring S ikke nødvendigvis er et ideal i S.

11. Lad R være en kommutativ ring, og lad $\mathfrak{a}$ være et ægte ideal. Antag, at $R \setminus \mathfrak{a} \subseteq R^*$ (altså at hvert $r \in R$ med $r \notin \mathfrak{a}$ er invertibelt i R). Vis, at $R/\mathfrak{a}$ er et legeme og at $\mathfrak{a}$ er et maksimalideal. Vis, at $\mathfrak{a}$ er det eneste maksimalideal i R.

12. En delmængde af en ring R, stabil under addition og multiplikation, kan være en ring, men den er kun en delring, hvis den har samme et-element som R. Vis, at følgende betingelser for et ideal $\mathfrak{a} \subseteq R$ er ækvivalente:

(i) $\mathfrak{a}$ er en ring.
(ii) $\mathfrak{a} = (e)$ er hovedidealet frembragt af et element e, der er idempotent ($e^2 = e$).
(iii) Der findes et ideal $\mathfrak{b} \subseteq R$ således, at gruppehomorfien $\mathfrak{a} \times \mathfrak{b} \to R$ er bijektiv.
(iv) Det findes en ringhomomorfi $R \to R'$ således, at restriktionen $\mathfrak{a} \to R'$ er bijektiv.

3. Homomorfi og isomorfi.

(3.1) Indledning. Lad R og R' være kommutative ringe. En afbildning $\varphi\colon R \to R'$ kaldes en *ringhomomorfi* eller blot en *homomorfi*, hvis der for alle $x, y \in R$ gælder, at

$$\varphi(x+y) = \varphi(x) + \varphi(y), \quad \varphi(xy) = \varphi(x)\varphi(y), \tag{3.1.1}$$

og hvis $\varphi(1_R) = 1_{R'}$. En bijektiv ringhomomorfi kaldes også en *(ring-)isomorfi*.

De to ligninger i (3.1.1) udtrykker, at afbildningen er henholdsvis *additiv* og *multiplikativ*. Additiviteten udsiger, at en ringhomomorfi specielt er en homomorfi mellem de to ringes additive grupper. En gruppehomomorfi afbilder neutralt element på neutralt element, så ved en ringhomomorfi afbildes nul-element på nul-element. Derimod følger det ikke af multiplikativiteten, at et-element afbildes på et-element; dét er altså et ekstra krav, der stilles til ringhomomorfier. I dette kapitel kigger vi nærmere på homomorfier og isomorfier mellem ringe, og vi viser de fundamentale isomorfisætninger. Resultaterne er helt analoge til de tilsvarende resultater for gruppehomomorfier. Som i det foregående kapitel betragter vi udelukkende kommutative ringe.

(3.2) Observation. For en ringhomomorfi $\varphi\colon R \to R'$ og et invertibelt element $r \in R$ gælder, at $\varphi(r)$ er invertibel i R' med det inverse bestemt ved ligningen,

$$\varphi(r)^{-1} = \varphi(r^{-1}).$$

Vi finder nemlig $\varphi(r^{-1})\varphi(r) = \varphi(r^{-1}r) = \varphi(1) = 1$, og heraf fremgår påstanden. Det følger specielt, at en ringhomomorfi $\varphi\colon R \to R'$ ved restriktion bestemmer en gruppehomomorfi $R^* \to (R')^*$ mellem grupperne af invertible elementer.

(3.3) Kerne og billede. Lad $\varphi\colon R \to R'$ være en ringhomomorfi. Det ses let, at for hver delring $S \subseteq R$ er billedmængden $\varphi(S)$ en delring af R'. Specielt er billedmængden $\varphi(R)$ en delring af R'. Den kaldes også *billedringen* eller *billedet* for homomorfien φ. Tilsvarende ses, for hver delring S' af R', at originalmængden $\varphi^{-1}(S')$ er en delring af R.

Det ses let, at for hvert ideal $\mathfrak{a}'$ i R' er originalmængden $\varphi^{-1}(\mathfrak{a}')$ et ideal i R. Specielt er originalmængden $\varphi^{-1}(0)$ et ideal i R. Originalmængden $\varphi^{-1}(0)$ kaldes *kernen* for homomorfien φ. Øjensynlig er $\varphi^{-1}(0)$ kernen, når φ opfattes som homomorfi af kommutative grupper. Det følger, at en ringhomomorfi φ er injektiv, hvis og kun hvis $\varphi^{-1}(0) = (0)$.

Tilsvarende ses, at for hvert ideal $\mathfrak{a}$ i R er billedmængden $\varphi(\mathfrak{a})$ et ideal i billedringen $\varphi(R)$.

(3.4) Eksempel. (0) For to givne ringe R og R' vil den trivielle homomorfi af grupper, der afbilder alle elementer i R på nul-elementet i R', i almindelighed *ikke* være en ringhomomorfi; en ringhomomorfi skal jo afbilde et-element på et-element, og det er kun opfyldt for afbildningen $r \mapsto 0$, hvis $1 = 0$ i R', altså hvis R' er nul-ringen.

Det følger tilsvarende, at der ikke findes ringhomomorfier fra nul-ringen til en ring, der ikke er nul-ringen.

(1) Hvis $S \subseteq R$ er en delring, så er inklusionsafbildningen, $x \mapsto x$ for $x \in S$, en injektiv homomorfi $S \to R$. Dens kerne er det trivielle ideal (0) i S.

(2) Lad $\mathfrak{a} \subseteq R$ være et ideal. Den kanoniske afbildning $R \to R/\mathfrak{a}$ er afbildningen $r \mapsto [r]$. Den er en homomorfi af kommutative grupper, og det følger af (2.7), at afbildningen er en ringhomomorfi. Den kaldes også den *kanoniske homomorfi*. Øjensynlig er den surjektiv. Dens kerne er det givne ideal $\mathfrak{a}$.

(3) For hver ring R er afbildningen $k \mapsto k1_R$ en ringhomomorfi $\mathbb{Z} \to R$. Billedringen er øjensynlig primringen i R. Homomorfiens kerne er et hovedideal (n) i $\mathbb{Z}$, hvor vi kan antage $n \geqslant 0$. Hvis $n = 0$, er homomorfien injektiv. Hvis $n > 0$, er n ordenen af et-elementet i den additive gruppe. I begge tilfælde er n altså karakteristikken af R.

(3.5) Homomorfisætningen. *Lad der være givet en surjektiv ringhomomorfi $\kappa\colon R \to \overline{R}$ med kernen $\mathfrak{a}$. Lad videre $\varphi\colon R \to R'$ være en vilkårlig ringhomomorfi. Antag, at φ forsvinder på $\mathfrak{a}$, altså at $\varphi(\mathfrak{a}) = \{0\}$. Da findes en og kun én ringhomomorfi $\overline{\varphi}\colon \overline{R} \to R'$ således, at der for alle $r \in R$ gælder ligningen,*

$$\overline{\varphi}(\kappa(r)) = \varphi(r). \tag{3.5.1}$$

Bevis. Fra Homomorfisætningen for grupper ved vi allerede, at der findes en og kun én homomorfi af additive grupper $\overline{\varphi}\colon \overline{R} \to R'$ således, at (3.5.1) er opfyldt. Det skal altså vises, at denne afbildning $\overline{\varphi}\colon \overline{R} \to R'$ også er multiplikativ og afbilder et-element på et-element. Da κ er surjektiv, har to vilkårlige elementer i $\overline{R}$ formen $\kappa(r)$ og $\kappa(s)$ for $r, s \in R$. For produktet har vi $\kappa(r)\kappa(s) = \kappa(rs)$. Produktet afbildes derfor ved $\overline{\varphi}$ på $\varphi(rs) = \varphi(r)\varphi(s)$, altså på produktet af billederne. Videre er $\kappa(1_R)$ et-elementet i $\overline{R}$, og dette element afbildes ved $\overline{\varphi}$ på $\varphi(1_R) = 1_{R'}$, altså på et-elementet i R'.

Hermed er Homomorfisætningen bevist. ∎

(3.6) Observation. Standardanvendelsen af Homomorfisætningen er på den kanoniske homomorfi $\kappa\colon R \to R/\mathfrak{a}$, hvor $\mathfrak{a}$ er et givet ideal i R. Hvis homomorfien $\varphi\colon R \to R'$ forsvinder på $\mathfrak{a}$, så findes ifølge Homomorfisætningen præcis én homomorfi $\overline{\varphi}\colon R/\mathfrak{a} \to R'$ således, at

$$\overline{\varphi}([r]) = \varphi(r), \tag{3.6.1}$$

hvor $[r] = r + \mathfrak{a}$. Homomorfien $\overline{\varphi}\colon R/\mathfrak{a} \to R'$ siges at være *induceret* af φ.

(3.7) Isomorfisætningen. *Lad $\varphi\colon R \to R'$ være en ringhomomorfi. Den inducerede homomorfi, $[r] \mapsto \varphi(r)$, er da en ringisomorfi,*

$$R/\varphi^{-1}(0) \xrightarrow{\sim} \varphi(R), \tag{3.7.1}$$

af kvotientringen af R modulo kernen på billedringen $\varphi(R)$.

Bevis. Fra Isomorfisætningen for grupper ved vi allerede, at (3.7.1) er en veldefineret additiv gruppeisomorfi, og af Homomorfisætningen (3.5) følger, at afbildningen er en ringhomomorfi. Den er følgelig en ringisomorfi. ∎

(3.8) Eksempel. For en given ring R har homomorfien $\mathbb{Z} \to R$, bestemt ved $k \mapsto k1_R$, kernen $n\mathbb{Z}$, hvor n er ringens karakteristik. Billedringen er primringen i R. Af Isomorfisætningen fås derfor en isomorfi af $\mathbb{Z}/n$ på primringen i R.

(3.9) Bemærkning. Homomorfi- og Isomorfisætningen for ringe er helt analoge til de tilsvarende sætninger for grupper. Og det følger af beviserne, at de kan udledes af de tilsvarende sætninger stort set ved at bemærke, at visse additive gruppehomomorfier også er multiplikative. Det forholder sig tilsvarende med Noether's isomorfisætninger. Den første, for ringe, anvendes ikke ret meget. Den udsiger følgende:

Lad S være en delring af R, og lad $\mathfrak{a}$ være et ideal i R. Da er summen $S + \mathfrak{a}$, bestående af alle elementer $s + a$ for $s \in S$ og $a \in \mathfrak{a}$, en delring af R og $\mathfrak{a}$ er et ideal i $S + \mathfrak{a}$. Yderligere er $S \cap \mathfrak{a}$ et ideal i S, og der findes en naturlig ringisomorfi,

$$S/(S \cap \mathfrak{a}) \xrightarrow{\sim} (S + \mathfrak{a})/\mathfrak{a}. \tag{3.9.1}$$

Beviset for Noether's første Isomorfisætning er en udmærket øvelse.

(3.10) Noether's anden Isomorfisætning. *Lad $\varphi\colon R \to R'$ være en ringhomomorfi, og lad $\mathfrak{a}_0$ være kernen for φ. Da gælder:*

Ved $\mathfrak{a} \mapsto \varphi(\mathfrak{a})$ defineres en bijektiv afbildning fra mængden af de idealer $\mathfrak{a}$ i R, der omfatter $\mathfrak{a}_0$, på mængden af alle idealer i billedringen $\varphi(R)$. Den inverse afbildning er bestemt ved $\mathfrak{a}' \mapsto \varphi^{-1}(\mathfrak{a}')$, for idealer $\mathfrak{a}'$ i $\varphi(R)$.

For hvert ideal $\mathfrak{a}$ i R med $\mathfrak{a} \supseteq \mathfrak{a}_0$ findes en kanonisk ringisomorfi,

$$R/\mathfrak{a} \xrightarrow{\sim} \varphi(R)/\varphi(\mathfrak{a}). \tag{3.10.1}$$

Bevis. Det skal vises, at under den bijektive forbindelse mellem undergrupper, kendt fra det tilsvarende resultat for grupper, svarer ideal til ideal. Det skal desuden vises, at afbildningen (3.10.1), der vides at være en isomorfi af kommutative grupper, også er en ringhomomorfi. Det er let at eftervise begge påstande. ▯

(3.11) Observation. Noether's anden Isomorfisætning anvendes oftest på den kanoniske (surjektive) homomorfi $R \to R/\mathfrak{a}_0$, hvor $\mathfrak{a}_0$ er et givet ideal i R. For et ideal $\mathfrak{a}$ i R, med $\mathfrak{a} \supseteq \mathfrak{a}_0$, består billedet af sideklasserne $a + \mathfrak{a}_0$, for $a \in \mathfrak{a}$. Billedet kan altså identificeres med den additive kvotientgruppe $\mathfrak{a}/\mathfrak{a}_0$, og denne kvotientgruppe er altså et ideal i $R/\mathfrak{a}_0$. Det er således påstanden i Sætningen, at samtlige idealer i $R/\mathfrak{a}_0$ har formen $\mathfrak{a}/\mathfrak{a}_0$, med et entydigt bestemt ideal $\mathfrak{a} \supseteq \mathfrak{a}_0$. Isomorfien (3.10.1) er her en isomorfi,

$$R/\mathfrak{a} \xrightarrow{\sim} \frac{R/\mathfrak{a}_0}{\mathfrak{a}/\mathfrak{a}_0}.$$

(3.12) Opgaver.

1. Lad $\varphi\colon R \to R'$ være en ringhomomorfi. Lad S og S' være delringe af henholdsvis R og R', og lad $\mathfrak{a}$ og $\mathfrak{a}'$ være idealer i henholdsvis R og R'. Vis, at $\varphi(S)$ er en delring af R' og at $\varphi^{-1}(S')$ er en delring af R. Vis, at $\varphi^{-1}(\mathfrak{a}')$ er et ideal i R, og at $\varphi(\mathfrak{a})$ er et ideal i $\varphi(R)$. Er $\varphi(\mathfrak{a})$ et ideal i R'?

2. Vis for hver ring R, at afbildningen $k \mapsto k1_R$ er en ringhomomorfi $\mathbb{Z} \to R$.

3. Vis, når $d\,|\,n$, at afbildningen $[x]_n \mapsto [x]_d$ er en ringhomomorfi $\mathbb{Z}/n \to \mathbb{Z}/d$.

4. Lad R være en ring af primtalskarakteristik p. Vis, at R indeholder restklasselegemet $\mathbb{F}_p$ som delring.

5. Antag, at R har primtalskarakteristik p. Vis, at afbildningen $x \mapsto x^p$ er en ringhomomorfi $R \to R$. Angiv egenskaber ved R, som sikrer, at homomorfien er injektiv.

6. Lad $\mathcal{F} = \mathcal{F}(X, R)$ være ringen af funktioner $X \to R$, og lad $a \in X$. Vis, at $f \mapsto f(a)$ er en ringhomomorfi $\mathcal{F} \to R$. Beskriv kerne og billedring.

7. Vis Noether's isomorfisætninger for ringe.

4. Brøklegeme.

(4.1) Indledning. Vi har defineret legemet $\mathbb{Q}$ af rationale tal som delringen af $\mathbb{R}$ bestående af alle *brøker* $a/s := as^{-1}$, hvor $a, s \in \mathbb{Z}$ og $s \neq 0$. Når vi regner med brøker, er det naturligvis nok at vide, at brøkerne udgør et legeme, der indeholder de hele tal, og at hver brøk kan skrives som et produkt as^{-1}, hvor $a, s \in \mathbb{Z}$ og $s \neq 0$ og s^{-1} er det inverse (i legemet $\mathbb{Q}$) af s. Heraf udleder man reglerne for at *forlænge* og *forkorte* brøker,

$$\frac{au}{su} = \frac{a}{s}, \tag{4.1.1}$$

og beskrivelserne af addition og multiplikation,

$$\frac{a}{s} + \frac{b}{t} = \frac{ta + sb}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}. \tag{4.1.2}$$

Af disse beskrivelser følger gyldigheden af de sædvanlige regneregler for brøker.

Det er klart, at hvis vi i stedet for ringen $\mathbb{Z}$ af hele tal betragter en given kommutativ ring R, og antager, at R er delring af et legeme L, så kan vi tilsvarende bestemme et *brøklegeme* bestående af alle brøker as^{-1} i L, hvor $a, s \in R$ og $s \neq 0$, med tilsvarende regneregler.

En ring R, som er delring af et legeme, er nødvendigvis et integritetsområde. Vi viser i dette kapitel, at for et givet kommutativt integritetsområde R, som a priori ikke antages at være delring af et legeme, kan vi konstruere et brøklegeme for R, og specielt et legeme, som indeholder R. Denne konstruktion, anvendt på ringen $\mathbb{Z}$ af hele tal, fører til legemet $\mathbb{Q}$ af rationale tal, og konstruktionen viser altså specielt, at det ikke er nødvendigt at forudsætte eksistensen af reelle tal for at definere de rationale tal. Mere interessant er det naturligvis, at konstruktionen fører til brøklegemer for integritetsområder, som ikke på forhånd er delringe af legemer.

(4.2) Konstruktion. Lad R være et givet kommutativt integritetsområde. I konstruktionen skeler vi til egenskaberne ved brøker fremhævet ovenfor. Hvert par (a, s) med $s \neq 0$ skal bestemme en brøk, men flere forskellige par vil bestemme den samme brøk. Brøkerne må derfor svare til ækvivalensklasser af par med en passende ækvivalensrelation.

Lad P være mængden af alle par (a, s), hvor $a, s \in R$ og $s \neq 0$. Da R er et integritetsområde, er $us \neq 0$, når $u, s \neq 0$. Hvis (a, s) er et par i P og $u \neq 0$, så er $u(a, s) := (ua, us)$ altså igen et par i P. Parret (ua, us) siges at fremgå af parret (a, s) ved at *forlænge* med u. For to par (a, s) og (a', s') i P skriver vi

$$(a, s) \sim (a', s'),$$

hvis de to par kan forlænges til det samme par, altså hvis der findes elementer $u, u' \neq 0$ i R således, at $u(a, s) = u'(a', s')$. Den herved definerede relation i mængden P af par er øjensynlig symmetrisk. Den er refleksiv, fordi parrene (a, s) og (a, s) kan forlænges med et-elementet 1 til parret $1(a, s) = (a, s)$. Endelig er relationen transitiv: Antag, at $(a, s) \sim (a', s')$ og at $(a', s') \sim (a'', s'')$. Der findes da elementer $u, u' \neq 0$ således, at

$u(a,s) = u'(a',s')$ og der findes elementer $v', v'' \neq 0$ således, at $v'(a',s') = v''(a'',s'')$. Det følger, at

$$v'u(a,s) = v'u'(a',s') = u'v'(a',s') = u'v''(a'',s'');$$

altså er $(a,s) \sim (a'',s'')$. Relationen er således en ækvivalensrelation i mængden P. Vi definerer en *brøk* som en ækvivalensklasse af par. Ækvivalensklassen, der indeholder et givet par $(a,s) \in P$ kaldes *brøken bestemt ved* (a,s), og den betegnes a/s eller $\frac{a}{s}$. Parret (a,s) kaldes et *repræsentantpar* for brøken a/s, og a og s kaldes, henholdsvis, *tæller* og *nævner* for parret. Bemærk, at det er repræsentantparret, og ikke selve brøken, der har en tæller og en nævner.

Ækvivalente par (a,s) og (a',s') ligger i samme ækvivalensklasse, og definerer altså den samme brøk. Specielt følger det, at brøken bestemt ved (a,s) ikke ændres, når vi forlænger parret (a,s) til (ua,us). Med andre ord gælder ligningen,

$$\frac{ua}{us} = \frac{a}{s}\,. \tag{4.2.1}$$

Lad K være mængden af brøker, altså mængden af ækvivalensklasser. Lad os vise, at der er en veldefineret addition og en veldefineret multiplikation i K således, at der for alle par (a,s) og (b,t) i P gælder ligningerne,

$$\frac{a}{s} + \frac{b}{t} = \frac{ta+sb}{st}\,, \quad \frac{a}{s}\cdot\frac{b}{t} = \frac{ab}{st}\,. \tag{4.2.2}$$

Som sædvanlig skal det eftervises, at brøkerne på ligningernes højresider ikke ændres, når de givne par (a,s) og (b,t) erstattes med ækvivalente par. Det er øjensynlig nok at vise, at højresiderne ikke ændres, når (a,s) forlænges, dvs når (a,s) erstattes med $u(a,s)$ for $u \neq 0$. Når (a,s) erstattes med $u(a,s)$, fås de nye højresider,

$$\frac{t(ua)+(us)b}{ust}\,, \quad \frac{uab}{ust}\,.$$

Da $t(ua)+(us)b = u(ta+sb)$, følger det af (4.2.1), at de to nye højresider er lig med de gamle.

Bemærk, at addition af to brøker, der er bestemt ved par med samme nævner, er specielt simpel:

$$\frac{a}{s} + \frac{b}{s} = \frac{a+b}{s}\,. \tag{4.2.3}$$

Ifølge (4.2.2) er venstresiden nemlig $(sa+sb)/ss$, og derfor, ifølge (4.2.1), lig med højresiden.

Udregninger, hvori der indgår addition af flere brøker, lettes ofte ved at bemærke, at der for givne endelig mange brøker altid findes repræsentantpar, der har den samme nævner. Er nemlig $(a_1,s_1),\dots,(a_n,s_n)$ repræsentantpar for de givne brøker, kan vi forlænge det i'te par med produktet af de øvrige nævnere. Herefter har alle repræsentantparrene den samme nævner, nemlig $s_1\cdots s_n$.

(4.3) Sætning. *Mængden K af alle brøker a/s for $a, s \in R$ og $s \neq 0$ udgør, med den ovenfor bestemte addition og multiplikation, et legeme. Nul-elementet er brøken $0/1$ og et-elementet er brøken $1/1$. For en brøk a/s er den modsatte brøk bestemt ved $(-a)/s$. For en brøk a/s som ikke er nul-elementet i K er $a \neq 0$, og den inverse brøk er bestemt som $(a/s)^{-1} = s/a$.*

Endelig gælder, at afbildningen $a \mapsto a/1$ er en injektiv ringhomomorfi $R \to K$.

Bevis. Det fremgår umiddelbart af ligningerne (4.2.2), at addition er kommutativ, at multiplikation er kommutativ og associativ, og at brøken $1/1$ er neutralt element for multiplikation.

Den associative lov involverer tre brøker. Som bemærket i (4.2) kan vi antage, at de tre brøker har repræsentantpar med samme nævner, altså at brøkerne har formen a/s, b/s, og c/s. Den associative lov for addition af brøker følger nu umiddelbart af (4.2.3). Tilsvarende, for at vise, at multiplikation er distributiv mht addition, er det nok at betragte tre brøker af formen a/s, b/t og c/t. Ved brug af ligningerne i (4.2) får vi, at

$$\frac{a}{s} \cdot \left(\frac{b}{t} + \frac{c}{t}\right) = \frac{a}{s} \cdot \frac{b+c}{t} = \frac{a(b+c)}{st},$$
$$\frac{a}{s} \cdot \frac{b}{t} + \frac{a}{s} \cdot \frac{c}{t} = \frac{ab}{st} + \frac{ac}{st} = \frac{ab+ac}{st}.$$

Brøkerne på højresiderne er ens, fordi den distributive lov gælder i R. Altså gælder den distributive lov for brøker.

Brøken $0/1$ er neutralt element for addition. Da $s0 = 0$ for alle elementer s, har vi nemlig $0/1 = 0/s$, og for en vilkårlig brøk a/s får vi derfor, at

$$\frac{a}{s} + \frac{0}{1} = \frac{a}{s} + \frac{0}{s} = \frac{a+0}{s} = \frac{a}{s}.$$

Af samme grund finder vi $a/s + (-a)/s = (a-a)/s = 0/s = 0/1$. Brøken $(-a)/s$ er altså den modsatte til a/s.

Lad nu a/s være en brøk, som ikke er nul-elementet $0/1$. Da $0/1 = 0/s$, er $a \neq 0$. Altså er $(s, a) \in P$, og s/a er en brøk. Øjensynlig er $(s/a)(a/s) = (sa)/(sa) = 1/1$. Følgelig er a/s invertibel, med brøken s/a som den inverse.

Hermed er det vist, at mængden K af alle brøker er et legeme.

Betragt endelig afbildningen $a \mapsto a/1$. Det fremgår umiddelbart, at afbildningen er en ringhomomorfi $R \to K$. For at vise, at den er injektiv, er det nok at vise, at kernen kun består af 0. Antag altså, at $a/1$ er nul-elementet $0/1$ i K. Da er parrene $(a, 1)$ og $(0, 1)$ ækvivalente. Altså findes elementer $u, v \neq 0$ i R således, at $u(a, 1) = v(0, 1)$. Vi har altså $(ua, u) = (0, v)$, og specielt $ua = 0$. Da R er et integritetsområde, følger det, at $a = 0$.

Hermed er alle påstandene bevist. □

(4.4) Definition. Legemet K af alle brøker a/s kaldes *brøklegemet* for det givne integritetsområde R. Afbildningen $a \mapsto a/1$ er en injektiv ringhomomorfi $R \to K$, så integritetsområdet R er isomorft med billedringen. Oftest identificerer vi elementerne i R med deres billeder, og vi skriver blot a for brøken $a/1$. Med denne identifikation er R en delring af brøklegemet.

(4.5) Eksempler. (1) Brøklegemet for integritetsområdet $\mathbb{Z}$ er som nævnt legemet $\mathbb{Q}$ af rationale tal.

(2) For en åben, sammenhængende delmængde Ω af $\mathbb{C}$ udgør de holomorfe funktioner på Ω et integritetsområde $\mathcal{H}(\Omega)$. Man kan vise, at brøklegemet er legemet $\mathcal{M}(\Omega)$ af såkaldt *meromorfe* funktioner på Ω.

(3) For et givet legeme L kan man betragte den såkaldte polynomiumsring $L[X]$ i én variabel X. Den er et integritetsområde. Brøklegemet kaldes legemet af *rationale funktioner* i én variabel, og det betegnes $L(X)$.

(4) Mere generelt har ringen $L[X_1, \dots, X_r]$ af polynomier i r variable som brøklegeme legemet $L(X_1, \dots, X_r)$ af rationale funktioner i r variable.

(4.6) Opgaver.

1. Vis, for et integritetsområde R, at $(a, s) \sim (a', s')$, hvis og kun hvis $sa' = s'a$.

2. Vis, at ethvert legeme af karakteristik 0 indeholder de rationale tals legeme $\mathbb{Q}$.

3. Lad L være et legeme, og lad R være en delring. Vis, at brøklegemet for R naturligt kan identificeres med delringen af L bestående af alle produkter as^{-1}, for $a, s \in R$ og $s \neq 0$.

4. Afbildningen $f \mapsto D(f) := f'$ er en *derivation* i polynomiumsringen $L[X]$, dvs der gælder ligningerne $D(f+g) = D(f) + D(g)$ og $D(fg) = fD(g) + D(f)g$. Vis, når L er et legeme, at der er en veldefineret derivation i brøklegemet $L(X)$, bestemt ved ligningen,

$$D\Big(\frac{f}{g}\Big) = \frac{D(f)g - fD(g)}{g^2}\,.$$

5. PID og UFD.

(5.1) Indledning. I det følgende betegner R et fast kommutativt integritetsområde. Vi vil undersøge betingelser, der sikrer, at resultater svarende til Aritmetikkens Fundamentalsætning gælder i R. Denne sætning udsiger som bekendt, at ethvert helt tal, som ikke er 0 eller ± 1, har en fremstilling som ± 1 gange et produkt af primtal, og at fremstillingen er entydig bortset fra ombytning af primfaktorerne. Ved hjælp af dette resultat kan en række problemer vedrørende divisorer mm umiddelbart løses for de hele tal.

Et (stort) naturligt tal, der er skrevet som produkt af to mindre tal er blevet „reduceret“. Primopløsningen af et tal er den ultimative reduktion: tallet er faktoriseret som produkt af tal, der ikke kan reduceres yderligere. Primtal er altså tal, som ikke kan reduceres. Det er en velkendt yderligere egenskab ved primtal, at et primtal, der går op i et produkt, nødvendigvis går op i en af faktorerne.

Begge disse egenskaber kan efterspørges for elementer i et givet integritetsområde. Som vi skal se, er de to egenskaber i almindelighed forskellige. Det er i øvrigt formålet med dette kapitel at udvikle en generel faktoriseringsteori. Anvendelsen er dels på polynomier (som introduceres senere), dels på visse talringe. De sidste anvendelser er nok de mest spændende. Vi berører nogle af dem i næste kapitel.

Vi har forudsat, at R er et (kommutativt) integritetsområde. Specielt er R altså ikke nulringen, så i R er $0 \neq 1$. Desuden følger det, at forkortningsreglen gælder i R, jfr (1.12)(3):

$$r \neq 0 \text{ og } rx = ry \implies x = y.$$

(5.2) Definition. Lad a være et element i R. For et element $d \in R$ siger vi, at d er *divisor* i a, eller at a er et *multiplum* af d, eller at d *går op* i a, og vi skriver $d \,|\, a$, hvis der findes et element $q \in R$ således, at $a = qd$. Bemærk, at nul-elementet 0 er specielt: ethvert element er divisor i 0; nul-elementet 0 er kun divisor i 0.

For en enhed $u \in R^*$ har vi ligningerne $a = (au^{-1})u = u^{-1}(ua)$ og det følger, at u og ua er divisorer i a. Mere generelt, hvis $a = qd$, så er $a = (qu^{-1})(ud)$ og $ua = (uq)d$. Udsagnet $d \,|\, a$ er altså ensbetydende med udsagnet $ud \,|\, a$, og ensbetydende med udsagnet $d \,|\, ua$. I de fleste spørgsmål vedrørende divisorer er to elementer, der afviger fra hinanden ved multiplikation med en enhed fra R, altså „lige gode“. Vi siger, at a og a' er *associerede*, hvis der findes en enhed u således, at $a' = ua$.

Det følger specielt, at enhederne og elementerne associerede med a altid er divisorer i a; de er de *trivielle divisorer* i a.

Et element $q \in R$ kaldes *irreducibelt*, hvis q ikke er 0 eller en enhed og q kun har trivielle divisorer. Den sidste betingelse – at q kun har trivielle divisorer – kan alternativt udtrykkes som følger: de eneste faktoriseringer af q som et produkt $q = ab$ er de trivielle, hvor en af faktorerne a eller b er en enhed (og den anden følgelig er associeret med q).

Et element $p \in R$ kaldes et *primelement*, hvis p ikke er 0 eller en enhed og p opfylder betingelsen, for alle $a, b \in R$,

$$p \,|\, ab \implies p \,|\, a \text{ eller } p \,|\, b. \tag{5.2.1}$$

(5.3) Lemma. *Et primelement er irreducibelt.*

Bevis. Antag, at p er et primelement i R. Betragt en ligning $p = ab$. Det skal vises, at a eller b er en enhed. Ligningen kan skrives $1p = ab$, så specielt er $p \mid ab$. Primelementet p går derfor op i en af faktorerne a eller b. Vi kan antage, at $p \mid b$, altså at $b = rp$ med $r \in R$. Det følger, at $p = ab = arp$. Her kan p bortforkortes, og det følger, at $1 = ar$. Altså er faktoren a en enhed (med r som det inverse element). ▯

(5.4) Lemma. *Egenskaber ved elementer i R modsvarer egenskaber ved de tilhørende hovedidealer:*

(1) u *er en enhed* $\iff$ $(u) = R$.
(2) a' *er associeret med* a $\iff$ $(a') = (a)$.
(3) d *er divisor i* a $\iff$ $a \in (d)$ $\iff$ $(a) \subseteq (d)$.
(4) d *er triviel divisor i* a $\iff$ $(d) = (a)$ eller $(d) = R$.
(5) q *er irreducibelt* $\iff$ $q \neq 0$ og (q) *er maksimalt blandt ægte hovedidealer.*
(6) p *er et primelement* $\iff$ $p \neq 0$ og (p) *er et primideal.*

Bevis. (1) Som bekendt betegner (u) hovedidealet Ru. Hvis u er en enhed, findes $s \in R$ således, at $su = 1$; det følger først, at $1 \in (u)$, og dernæst, at $r = r1 \in (u)$ for alle $r \in R$. Altså er $(u) = R$. Antages omvendt, at $(u) = R$, så er $1 \in (u)$, og følgelig er $1 = su$ med et element $s \in R$; altså er u en enhed (med s som det inverse element).

(2) Hvis a' er associeret med a, er $a' = ua$ med en enhed u. Følgelig er $a' \in (a)$, og heraf følger, at $(a') \subseteq (a)$. Desuden er $a = va'$, med $v := u^{-1}$, og derfor er $(a) \subseteq (a')$. Altså er $(a') = (a)$. Antag omvendt, at $(a') = (a)$. Hvis $a = 0$, følger det umiddelbart, at også $a' = 0$; specielt er a og a' associerede. Antag derfor, at $a \neq 0$. Vi har $a' = ua$ og $a = va'$, med elementer $u, v \in R$. Vi udleder, at $a = va' = vua$. Da $a \neq 0$, kan faktoren a bortforkortes, og det følger, at $1 = vu$. Altså er u en enhed; da $a' = ua$, er a' associeret med a.

(3) Denne påstand er triviel.

(4) Påstanden følger umiddelbart af (1) og (2).

(5) Et irreducibelt element må ikke være 0. I beviset kan vi derfor antage, at $q \neq 0$. Tilsvarende kan vi antage, at q ikke er en enhed, idet dette, ifølge (1), er ækvivalent med at (q) er et ægte ideal. Ifølge (3) og (4) svarer divisorerne d i q til de elementer $d \in R$, for hvilke

$$(q) \subseteq (d) \subseteq R, \tag{*}$$

og d er en triviel divisor i q, hvis og kun hvis en af de to inklusioner i (*) er en lighed. At q kun har trivielle divisorer betyder med andre ord, at de to inklusioner i (*) ikke begge kan være skarpe, altså at intet ægte hovedideal (d) kan være strengt større end (q). Hermed er (5) bevist.

(6) Et primelement må ikke være 0. I beviset kan vi derfor antage, at $p \neq 0$. Tilsvarende kan vi antage, at p ikke er en enhed, idet dette, ifølge (1), er ækvivalent med at (p) er et ægte ideal. Betingelsen (5.2.1) for at p er et primelement er øjensynlig ækvivalent med betingelsen (2.9.1) for at (p) er er primideal. Altså gælder påstanden i (6). ▯

(5.5) Hovedidealområde. Integritetsområdet R kaldes et *hovedidealområde*, hvis alle idealer i R er hovedidealer. Et hovedidealområde hedder på engelsk et 'Principal Ideal Domain', og vi vil kort skrive *PID* for hovedidealområde.

Det fremgår af Sætning (2.3), at ringen $\mathbb{Z}$ er et PID. Det er et fundamentalt resultat om polynomier, at polynomiumsringen $L[X]$ med koefficienter i et legeme L er et PID.

Bemærk, at definitionen af et PID i en vis forstand er parallel med ε-δ-definitioner fra analysen: for at bevise, at et givet integritetsområde R er et PID, skal det vises, at der for alle idealer $\mathfrak{a}$ i R eksisterer et element d i R således, at $\mathfrak{a} = (d)$.

(5.6) Note. Beviserne for at $\mathbb{Z}$ er et PID og for at polynomiumsringen $L[X]$ for et legeme L er et PID bygger på sætningerne om division med rest. De to beviser har fælles træk, der kan udmøntes i et generelt resultat:

Numerisk betingelse for PID. *Antag for integritetsområdet R, at der er givet en funktion $\nu : R \to \mathbb{Z}$, som er nedad begrænset og opfylder, at for hvert $d \neq 0$ og for hvert a findes et element q således, at $\nu(a - qd) < \nu(d)$. Da er R et hovedidealområde.*

Bevis. Lad $\mathfrak{a}$ være et ideal i R. Det skal vises, at $\mathfrak{a}$ er et hovedideal, altså at der eksisterer et element $d \in \mathfrak{a}$ således, at $\mathfrak{a} = (d)$. Eksistensen er klar, hvis $\mathfrak{a} = (0)$, så vi kan antage, at $\mathfrak{a} \neq (0)$. Der findes altså elementer $r \neq 0$ i $\mathfrak{a}$. Da funktionen $\nu\colon R \to \mathbb{Z}$ er nedad begrænset, kan vi betragte det mindste af tallene,

$$\nu(r), \quad \text{hvor } r \in \mathfrak{a},\ r \neq 0.$$

Dette mindste tal har formen $\nu(d)$, hvor $d \in \mathfrak{a},\ d \neq 0$. Det påstås, at

$$\mathfrak{a} = (d).$$

Da $d \in \mathfrak{a}$, har vi trivielt $(d) \subseteq \mathfrak{a}$. Vi mangler at vise, for $a \in \mathfrak{a}$, at $a \in (d)$. Af forudsætningen følger, at vi kan finde $q \in R$ således, at differensen $r := a - qd$ opfylder uligheden,

$$\nu(r) < \nu(d).$$

Da $a \in \mathfrak{a}$ og $qd \in (d) \subseteq \mathfrak{a}$, vil også $r = a - qd \in \mathfrak{a}$. Hvis $r \neq 0$, er $\nu(r) < \nu(d)$ i modstrid med valget af d. Følgelig har vi $r = 0$, og dermed er $a = qd \in (d)$, som ønsket. $\square$

Et integritetsområde R kaldes en *euklidisk ring*, hvis der findes en funktion $\nu\colon R \to \mathbb{Z}$ med egenskaben i den numeriske betingelse. En euklidisk ring er altså et PID. Ringen $\mathbb{Z}$ er en euklidisk ring, idet funktionen $\nu(a) := |a|$ har egenskaben. Polynomiumsringen $L[X]$, med koefficienter i et legeme L, er euklidisk, idet funktionen $\nu(f) := \deg(f)$ har egenskaben (når nul-polynomiet tillægges graden -1).

(5.7) Sætning. *Antag, at R er et PID. Da er et element $p \in R$ irreducibelt, hvis og kun hvis det er et primelement. Hovedidealet (p) frembragt af et sådant element er et maksimalideal, og kvotientringen $R/(p)$ er et legeme.*

Bevis. Ifølge Lemma (5.3) gælder „hvis“ i ethvert integritetsområde. Antag omvendt, at $p \in R$ er irreducibelt. Ifølge Lemma (5.4)(5) er hovedidealet (p) så maksimalt blandt de ægte hovedidealer. Da alle idealer i R er hovedidealer, følger det, at (p) er maksimalt blandt de ægte idealer, altså at (p) er et maksimalideal. Ifølge Korollar (2.13) er et maksimalideal et primideal. Altså er (p) et primideal. Da $p \neq 0$, slutter vi af Lemma (5.4)(6), at p er et primelement.

Undervejs så vi, for et irreducibelt element p, at hovedidealet (p) er et maksimalideal. Af Sætning (2.12) følger, at kvotientringen $R/(p)$ er et legeme. ∎

(5.8) Definition. Lad a være et element i R. En fremstilling $a = d_1 \cdots d_s$, hvor $d_i \in R$, kaldes også en *opløsning* af a i *faktorerne* $d_1, \dots, d_s$. Opløsningen kaldes en *irreducibel opløsning*, hvis faktorerne er irreducible, og en *primopløsning*, hvis faktorerne er primelementer.

Ethvert element $a \in R$ har trivielle opløsninger med to faktorer af formen $a = u(u^{-1}a)$, hvor den ene faktor u er en enhed (og den anden er associeret med a); hver af de to faktorer har yderligere trivielle opløsninger. Et irreducibelt element har kun sådanne trivielle opløsninger. At en opløsning $a = q_1 \cdots q_s$ er irreducibel betyder altså, at de enkelte faktorer q_i kun trivielt kan opløses yderligere.

(5.9) Lemma. *Primopløsninger er entydige i følgende forstand: Er $p_1, \dots, p_s$ og $q_1, \dots, q_t$ primelementer i R, og er produktet $p_1 \cdots p_s$ associeret med produktet $q_1 \cdots q_t$, så er $s = t$, og efter en passende permutation af q_j'erne er q_i associeret med p_i for $i = 1, \dots, s$.*

Bevis. Det er antagelsen, at der findes en enhed $u \in R$ og en ligning,

$$up_1 \cdots p_s = q_1 \cdots q_t. \tag{1}$$

Specielt går primelementet p_s op i produktet $q_1 \cdots q_t$. Altså går p_s op i en af faktorerne q_j. Vi kan antage, at p_s er divisor i q_t. Da q_t er et irreducibelt element, jfr Lemma (5.3), må p_s endda være en triviel divisor i q_t, og da p_s ikke er en enhed, må p_s være associeret med q_t. Vi har altså $p_s = vq_t$ med en enhed $v \in R$. Ved indsættelse i (1) får vi,

$$uvp_1 \cdots p_{s-1}q_t = q_1 \cdots q_{t-1}q_t.$$

Da $q_t \neq 0$ kan vi bortforkorte q_t:

$$(uv)p_1 \cdots p_{s-1} = q_1 \cdots q_{t-1}.$$

Produktet $p_1 \cdots p_{s-1}$ er derfor associeret med produktet $q_1 \cdots q_{t-1}$. Induktivt, fx ved induktion efter s, følger det, at $s - 1 = t - 1$ og at der efter permutation af faktorerne $q_1, \dots, q_{t-1}$ gælder, at q_i er associeret med p_i for $i = 1, \dots, s - 1$. Altså er $s = t$, og da q_s var associeret med p_s, er det ønskede vist. ∎

(5.10) Opløsninger. Entydigheden i lemmaet gælder specielt, hvis de to produkter er ens. Hvis et element a i R har en primopløsning, $a = p_1 \cdots p_s$ med primelementer p_i, så er fremstillingen altså entydig i den forstand, at antallet s af faktorer er entydigt bestemt og de enkelte faktorer, på nær ombytning og associering, er entydigt bestemte.

Som vi senere skal se, gælder det tilsvarende resultat for irreducible opløsninger *ikke* i almindelighed. Hvis den tilsvarende entydighed gælder for vilkårlige irreducible opløsninger i et integritetsområde R, siger vi kort om R, at *irreducible opløsninger er entydige*.

Om R siger vi, med lidt løsagtighed i sprogbrugen, at primopløsninger *eksisterer* for *alle* elementer, hvis de eksisterer for alle elementer, der ikke er 0 eller en enhed, altså hvis ethvert sådant element kan skrives som produkt af primelementer. Tilsvarende siger vi, at irreducible opløsninger *eksisterer* for *alle* elementer, hvis hvert element a i R, som ikke er 0 eller en enhed, har en irreducibel opløsning.

De to egenskaber, eksistens og entydighed af irreducible opløsninger, er uafhængige. I de ringe, vi senere vil anvende teorien på, vil irreducible opløsninger eksistere, men de vil ikke nødvendigvis være entydige.

(5.11) Sætning. *For et integritetsområde R er følgende tre betingelser ækvivalente:*

(i) $\begin{cases} \text{(a) } \textit{Irreducible opløsninger eksisterer for alle elementer, og} \\ \text{(b) } \textit{irreducible opløsninger er entydige.} \end{cases}$

(ii) $\begin{cases} \text{(a) } \textit{Irreducible opløsninger eksisterer for alle elementer, og} \\ \text{(c) } \textit{hvert irreducibelt element i } R \textit{ er et primelement.} \end{cases}$

(iii) *Primopløsninger eksisterer for alle elementer.*

Bevis. Bemærk, at det er den samme betingelse (a), der indgår i både (i) og (ii).

Hvis (c) er opfyldt, er enhver irreducibel opløsning en primopløsning. Det følger derfor, at (ii) $\Rightarrow$ (iii). Da primopløsninger er entydige ifølge (5.9), følger det også, at (ii) $\Rightarrow$ (i).

Vi mangler at vise, at (i) $\Rightarrow$ (ii) og at (iii) $\Rightarrow$ (ii). Det følger af Lemma (5.3), at en primopløsning er en irreducibel opløsning. Følgelig vil (iii) $\Rightarrow$ (a). For at vise, at (iii) $\Rightarrow$ (ii), er det altså nok at vise, at (iii) $\Rightarrow$ (c). For at vise, at (i) $\Rightarrow$ (ii), skal det vises, at (i) $\Rightarrow$ (c).

Vi skal altså vise betingelsen (c), dels under antagelse af (iii), dels under antagelse af (a) og (b). Lad q være et irreducibelt element. Det skal vises, at q er et primelement.

Antag først, at (iii) er opfyldt. Betragt en primopløsning af q. Da q er irreducibelt, har det kun trivielle opløsninger. Primopløsningen har derfor kun én faktor. Følgelig er q et primelement.

Antag dernæst, at (a) og (b) er opfyldt. For at vise, at q er et primelement, antager vi, at $q \mid ab$. Det skal vises, at $q \mid a$ eller $q \mid b$. Ethvert element er divisor i 0, så vi kan antage, at a og b er forskellige fra 0. Da $q \mid ab$ har vi en ligning, med $r \in R$,

$$rq = ab. \tag{1}$$

Da $ab \neq 0$, er $r \neq 0$. Antag først, at intet af elementerne r, a, b er en enhed. Da kan vi ifølge eksistensantagelsen i (a) finde irreducible opløsninger: $a = a_1 \cdots a_s$ og $b = b_1 \cdots b_t$ og $r = r_1 \cdots r_u$. Indsættes i ligningen (1), fås ligningen,

$$r_1 \cdots r_u q = a_1 \cdots a_s b_1 \cdots b_t. \tag{2}$$

Alle faktorer i ligningen (2) er irreducible. Ifølge entydighedsantagelsen i (b) må den irreducible faktor q på venstresiden derfor også forekomme (på nær associering) på højresiden. Vi kan antage, at q er associeret med a_1. Men så er q specielt divisor i a_1. Da $a_1 \,|\, a$, følger det, at $q \,|\, a$.

Hvis et af elementerne r, a, b er en enhed, er det let at modificere argumentet. Igen er konklusionen, at q er divisor i a eller i b.

Hermed er de ønskede implikationer eftervist. ∎

(5.12) Definition. Integritetsområdet R kaldes en *faktoriel ring*, hvis de ækvivalente betingelser i Sætningen er opfyldt. En faktoriel ring hedder på engelsk et 'Unique Factorization Domain', og vi vil kort skrive *UFD* for faktoriel ring.

Vi bemærker, at ringen $\mathbb{Z}$ er et UFD. De irreducible elementer i $\mathbb{Z}$ er jo, bortset fra fortegn, primtallene, og at betingelsen (i), om eksistens og entydighed af irreducible opløsninger, er opfyldt, er indholdet i Aritmetikkens Fundamentalsætning.

For at vise, at et givet integritetsområde, R, er et UFD, skal man eftervise en af betingelserne (i), (ii), eller (iii). I praksis vil det ofte være forholdsvis let at indse, at hvert element a, der ikke er 0 eller en enhed, har en irreducibel opløsning: Hvis a ikke selv er irreducibelt, har vi en ikke-triviel faktorisering $a = a_1a_2$. Hvis de to faktorer ikke er irreducible, kan vi yderligere faktorisere, osv. Ved hver faktorisering stiger antallet af faktorer. Hvis der altså er betingelser på ringen R, som sikrer, at en sådan proces må stoppe, er betingelsen (a) således opfyldt. Det vil sædvanligvis være mindre oplagt, at (b) eller (c) er opfyldt.

(5.13) Lemma. *Lad R være en ring, hvori irreducible opløsninger ikke eksisterer for alle elementer. Da findes i R en uendelig følge af elementer $a_1, a_2, \dots$ således, at a_{i+1} er en ikke-triviel divisor i a_i for $i = 1, 2, \dots$.*

Bevis. Det er forudsætningen, at der i R findes elementer a med følgende egenskab: a er ikke 0, a er ikke en enhed, og a kan ikke skrives som produkt af irreducible elementer. Det er nok at vise, at hvert element a med denne egenskab har en ikke-triviel divisor a' med den samme egenskab.

Antag altså, at a ikke er 0 og ikke er en enhed og at a ikke kan skrives som produkt af irreducible elementer. Specielt kan a så ikke selv være et irreducibelt element. Vi kan derfor skrive $a = a'a''$, hvor a' og a'' er ikke-trivielle divisorer i a. Elementerne a' og a'' er begge forskellige fra 0, da $a'a'' = a \neq 0$. Ingen af dem er enheder, idet de begge er ikke-trivielle divisorer i a. Hvis både a' og a'' kunne skrives som produkt af irreducible elementer, ville vi ved indsættelse i $a = a'a''$ opnå en fremstilling af a som et produkt af irreducible elementer, i modstrid med antagelsen. Følgelig vil mindst en af de to divisorer a' og a'' opfylde, at den ikke kan skrives som et produkt af irreducible elementer; denne divisor er derfor en ikke-triviel divisor i a med den ønskede egenskab. ∎

(5.14) Note. *Antag for integritetsområdet R, at der er givet en funktion $\nu : R \to \mathbb{Z}$, som er nedad begrænset og opfylder, at for hvert $a \neq 0$ i R og hver ikke-triviel divisor a' i a er $\nu(a') < \nu(a)$. Da eksisterer irreducible opløsninger for alle elementer i R.*

Bevis. I modsat fald ville der nemlig findes en uendelig følge $a_1, a_2, a_3, \dots$ som angivet i Lemma (5.13), og så ville ulighederne,

$$\nu(a_1) > \nu(a_2) > \nu(a_3) > \cdots ,$$

være i modstrid med at $\nu\colon R \to \mathbb{Z}$ var nedad begrænset. □

(5.15) Hovedsætning. *Et PID er et UFD.*

Bevis. Antag, at R er et hovedidealområde. Vi efterviser betingelsen (5.11)(ii). Det skal altså vises, at irreducible opløsninger eksisterer, og det skal vises, at hvert irreducibelt element er et primelement. Det sidste er indeholdt i Sætning (5.7). Det første vises indirekte. Antag altså, at irreducible opløsninger ikke eksisterer for alle elementer. Af Lemma (5.13) fås, at der eksisterer en uendelig følge $a_1, a_2, \dots$ af elementer i R således, at a_{i+1} er en ikke-triviel divisor i a_i. For de tilhørende hovedidealer får vi af Lemma (5.4)(3),(4) de skarpe inklusioner,

$$(a_1) \subset (a_2) \subset (a_3) \subset \cdots .$$

Lad $\mathfrak{a}$ være foreningsmængden af idealerne (a_i). Det påstås, at $\mathfrak{a}$ er et ideal i R. Betragt to elementer a, b i foreningsmængden $\mathfrak{a}$. Vi har $a \in (a_i)$ og $b \in (a_j)$, med passende i og j. Antager vi for eksempel, at $i \leqslant j$, så er $(a_i) \subseteq (a_j)$, og derfor ligger både a og b i (a_j). Da (a_j) er et ideal, følger det at $a + b \in (a_j)$. Altså ligger $a + b$ i foreningsmængden $\mathfrak{a}$. For $r \in R$ ligger ra i (a_i), da (a_i) er et ideal; følgelig ligger ra i foreningsmængden. Endelig ligger nul-elementet i (a_1) og dermed i foreningsmængden.

Foreningsmængden $\mathfrak{a}$ er altså et ideal. Af forudsætningen følger derfor, at $\mathfrak{a}$ er et hovedideal. Der findes altså et element $c \in \mathfrak{a}$ således, at $\mathfrak{a} = (c)$. Elementet c ligger i foreningsmængden, og altså i (a_k) for passende k. Altså er $(c) \subseteq (a_k)$. Vi har nu inklusionerne,

$$(c) \subseteq (a_k) \subset (a_{k+1}) \subset \cdots \subseteq \mathfrak{a} = (c),$$

der øjensynlig er den ønskede modstrid. Hermed er Hovedsætningen bevist. □

(5.16) Eksempel. (1) I ringen $\mathbb{Z}$ af hele tal er enhederne tallene ± 1. At regne på nær associering betyder altså at regne på nær fortegn. Hvert tal forskelligt fra 0 er associeret med netop ét positivt tal. Efter den sædvanlige definition er primtallene de positive irreducible elementer i $\mathbb{Z}$. Som nævnt i (5.5) er ringen $\mathbb{Z}$ et PID, og derfor ifølge Hovedsætningen et UFD. Beviset for Hovedsætningen er essentielt et af de klassiske beviser for Aritmetikkens Fundamentalsætning.

Af Sætning (5.7), eller af betingelsen (5.11)(c), følger, at et primtal er et primelement i $\mathbb{Z}$, hvilket er den velkendte egenskab, at et primtal, der går op i et produkt, må gå op i en af faktorerne. Undervejs, i (5.7), genfandt vi resultatet, at kvotientringen $\mathbb{Z}/(p)$, for et primtal p, er et legeme.

(2) I polynomiumsringen $L[X]$, hvor L er et legeme, er enhederne de konstante polynomier forskellige fra 0. At regne på nær associering betyder altså at regne på nær multiplikation med en konstant forskellig fra 0. Hvert polynomium forskelligt fra 0 er associeret med netop ét normeret polynomium. Som nævnt i (5.5) er $L[X]$ et PID. Ifølge Hovedsætningen er $L[X]$ altså et UFD.

Spørgsmålet om hvilke (normerede) polynomier i $L[X]$, der er irreducible, afhænger i høj grad af legemet L. I almindelighed er alle førstegradspolynomier $X - a$ irreducible. Et polynomium, der har $a \in L$ som rod, er deleligt med førstegradspolynomiet $X - a$. Et polynomium af grad mindst 2, som har en rod, er derfor altid reducibelt. For polynomier af grad 2 eller grad 3 må en af faktorerne i en ikke-triviel faktorisering være af grad 1. Polynomier af grad 2 eller 3 er derfor irreducible, hvis og kun hvis de ikke har rødder i L.

Algebraens Fundamentalsætning udsiger, at ethvert polynomium af positiv grad i $\mathbb{C}[X]$ har en kompleks rod. Ethvert polynomium af grad mindst 2 i $\mathbb{C}[X]$ er derfor reducibelt. De irreducible polynomier i $\mathbb{C}[X]$ er altså netop førstegradspolynomierne. Lad os vise, at i ringen $\mathbb{R}[X]$ er de irreducible polynomier netop førstegradspolynomierne og andengradspolynomierne uden reelle rødder. Betragt hertil i $\mathbb{R}[X]$ et normeret irreducibelt polynomium f uden reelle rødder. Polynomiet f har en kompleks rod ξ. Da f har reelle koefficienter er det konjugerede tal $\bar{\xi}$ ligeledes rod i f, og da ξ ikke er reel, er $\xi \neq \bar{\xi}$. Tallene ξ og $\bar{\xi}$ er derfor to forskellige rødder i f. Følgelig er f delelig med produktet $g := (X - \xi)(X - \bar{\xi})$. Produktet g har reelle koefficienter, thi er $\xi = a + ib$ får vi $(X - \xi)(X - \bar{\xi}) = (X - a)^2 + b^2$. Vi har altså en faktorisering,

$$f = gh,$$

og da g og f har reelle koefficienter, har også h reelle koefficienter. Da f er irreducibel, må faktoriseringen være triviel, dvs h må være konstant. Da f og g er normerede, må vi have $h = 1$, og altså $f = g$. Vi har således vist, at de normerede irreducible polynomier i $\mathbb{R}[X]$ er førstegradspolynomierne $X - a$ og andengradspolynomierne $(X - a)^2 + b^2$, hvor $b \neq 0$.

Vi viser senere, at polynomierne $X^n - 2$ for $n = 1, 2, 3, \ldots$ er irreducible polynomier i $\mathbb{Q}[X]$. I polynomiumsringen $\mathbb{Q}[X]$ findes altså irreducible polynomier af enhver grad $\geqslant 1$.

(5.17) Bemærkning. Vi viser senere, at hvis R er en faktoriel ring, så er også polynomiumsringen $R[X]$ en faktoriel ring. Specielt, for $R = \mathbb{Z}$, følger det, at ringen $\mathbb{Z}[X]$ af polynomier med heltalskoefficienter er en faktoriel ring. Det sidste resultat skyldes Gauss, og det almindelige resultat kaldes *Gauss' Sætning*. Det følger induktivt, at en polynomiumsring i r variable,

$$R[X_1, \ldots, X_r],$$

med koefficienter i en faktoriel ring R, igen er en faktoriel ring.

(5.18) Note. I en faktoriel ring R tænkes ofte valgt et *repræsentantsystem for primelementerne*, dvs en mængde $\mathcal{P}$ af primelementer med den egenskab, at ethvert primelement i R er associeret med netop ét primelement i $\mathcal{P}$. Efter et sådant valg har primelementerne q i R altså en fremstilling $q = up$ med en entydigt bestemt enhed u og et entydigt bestemt primelement $p \in \mathcal{P}$. Indsætter vi i en primopløsning af et element $a \neq 0$,

$$a = q_1 \cdots q_s,$$

for de enkelte faktorer q_i en sådan fremstilling $q_i = up$, kan vi samle de fremkomne enheder u i et produkt af enheder og de fremkomne elementer $p \in \mathcal{P}$, der forekommer flere gange, kan vi skrive som potenser. Herved opnås en fremstilling,

$$a = up_1^{\alpha_1} \cdots p_r^{\alpha_r},$$

hvor u er en enhed og elementerne $p_1, \dots, p_r$ er forskellige elementer i $\mathcal{P}$. Idet vi om fornødent tilføjer potenser med eksponent 0, kan opløsningen skrives

$$a = u \prod_{p \in \mathcal{P}} p^{\alpha_p},$$

hvor produktet er over alle (sædvanligvis uendelig mange) elementer p i $\mathcal{P}$, men hvor kun endelig mange eksponenter α_p er forskellige fra 0. Denne fremstilling, som vi ofte også kalder *primopløsningen* af a, er entydig i den forstand, at enheden u og eksponenterne $\alpha_p \geqslant 0$, for $p \in \mathcal{P}$, er entydigt bestemt ved a. Det ses, at også enhederne i R har en sådan opløsning, nemlig med $\alpha_p = 0$ for alle $p \in \mathcal{P}$. Alle elementer forskellige fra 0 har altså en primopløsning i denne forstand.

Betragt endnu et element $d \neq 0$ i R, med primopløsningen,

$$d = v \prod_{p \in \mathcal{P}} p^{\delta_p}.$$

Af primopløsningernes entydighed følger, at d er divisor i a, hvis og kun hvis $\delta_p \leqslant \alpha_p$ for alle $p \in \mathcal{P}$

Specielt ses, at „på nær associering“ er antallet af divisorer i a bestemt som produktet,

$$\prod_{p \in \mathcal{P}} (\alpha_p + 1),$$

idet jo $\alpha_p + 1$ er antallet af eksponenter δ_p med $0 \leqslant \delta_p \leqslant \alpha_p$. Produktet er naturligvis endeligt i den forstand, at kun endelig mange faktorer er forskellige fra tallet 1.

(5.19) Note. I integritetsområdet R siges et element d at være *en største fælles divisor* for elementer a, b, hvis d er en fælles divisor for a, b (dvs d er divisor i både a og b), og hvis enhver fælles divisor for a, b er divisor i d. Tilfældet, hvor et af elementerne a, b er nul-elementet, er ikke så interessant: elementet b er en største fælles divisor for $0, b$, også hvis $b = 0$.

I ringen $\mathbb{Z}$ er elementerne totalt ordnet, og ordningen bruges i den sædvanlige definition af største fælles divisor for to hele tal. I den generelle situation er der ikke nogen ordning af elementerne, og i definitionen ovenfor er det i stedet en velkendt egenskab ved største fælles divisor, der er generaliseret. Det skal understreges, at i den generelle situation eksisterer en største fælles divisor ikke nødvendigvis.

Det følger af definitionen, at en største fælles divisor er entydig på nær associering: hvis både d_1 og d_2 er en største fælles divisor for a, b, så er d_1 divisor i d_2 og d_2 er divisor i d_1; følgelig er d_1 og d_2 associerede.

I et UFD eksisterer største fælles divisor altid. Betragt nemlig elementer a, b, d forskellige fra 0 i en faktoriel ring R, med primopløsninger,

$$a = u \prod_{p \in \mathcal{P}} p^{\alpha_p}, \quad b = v \prod_{p \in \mathcal{P}} p^{\beta_p}, \quad d = w \prod_{p \in \mathcal{P}} p^{\delta_p}.$$

Da er d en fælles divisor for a, b, hvis og kun hvis $\delta_p \leqslant \alpha_p$ og $\delta_p \leqslant \beta_p$ for alle p. Det fremgår umiddelbart, at det element d, der bestemmes ved at eksponenterne i primopløsningen er $\delta_p := \min\{\alpha_p, \beta_p\}$, er en største fælles divisor for a, b.

I et PID kan en største fælles divisor d for a, b skrives på formen $d = xa + yb$ med $x, y \in R$. Betragt nemlig for to elementer a, b i R summen $Ra + Rb$, bestående af elementer af formen $xa + yb$. Summen er øjensynlig et ideal i R. Da R er et PID, er summen et hovedideal. Der findes altså et element $d \in R$ således, at vi har ligningen,

$$Ra + Rb = Rd.$$

Elementet a ligger på venstresiden, og derfor i Rd. Altså er d divisor i a. Tilsvarende er d divisor i b. Elementet d er altså en fælles divisor for a, b. På den anden side ligger d i summen, så d har formen $d = xa + yb$. Det følger, at enhver fælles divisor for a, b også er divisor i d. Altså er d en største fælles divisor for a, b.

Lad os endelig bemærke, at i en euklidisk ring, jfr Bemærkning (5.6), kan den største fælles divisor bestemmes ved en algoritme, der er en umiddelbar generalisering af Euklid's klassiske algoritme.

(5.20) Opgaver.

1. Lad R være et integritetsområde. For elementer $a, b \in R\backslash\{0\}$ skriver vi $a \prec b$, hvis $a \,|\, b$ og a ikke er associeret med b. Vis, at '$\prec$' er en ordensrelation i mængden $R\backslash\{0\}$. Hvilke elementer i mængden $R\backslash\{0\}$ er minimale? Og maksimale? Er ordningen total? Er relationen 'går op i' en ordensrelation?

2. Vis, at relationen 'associeret med' er en ækvivalensrelation.

3. Begrund, at argumentet i (5.13) viser følgende: Et binært træ, som ikke er endeligt, har en uendelig gren.

4. Vis, for et primtal p, at talringen $\mathbb{Z}_{(p)}$ (bestående af alle brøker a/s, hvor $p \nmid s$) er et PID og at den kun indeholder ét primelement (på nær associering).

5. Vis, for et legeme L, at potensrækkeringen $L[[X]]$ er et PID og at den kun indeholder ét primelement (på nær associering).

6. Kvadratiske talringe.

(6.1) Indledning. Talringe er delringe af ringen $\mathbb{C}$ af komplekse tal; de er specielt kommutative integritetsområder. Den simpleste er ringen $\mathbb{Z}$ af hele tal. I dette kapitel kigger vi nærmere på en familie af talringe, de *kvadratiske talringe*. I disse talringe eksisterer der irreducible opløsninger for alle elementer; i nogen af talringene er irreducible opløsninger entydige. Som vi skal se, giver den generelle teori for faktorielle ringe ikke-trivielle, klassiske resultater om de hele tal.

(6.2) Setup. I det følgende betragter vi et fast normeret andengradspolynomium med heltalskoefficienter,

$$X^2 + bX + c \in \mathbb{Z}[X], \tag{6.2.1}$$

og vi betegner med ξ en af de to (komplekse) rødder i polynomiet.

Polynomiet har *diskriminanten* $D = b^2 - 4c$, så af den sædvanlige løsningsformel følger, at

$$\xi = \frac{-b \pm \sqrt{D}}{2}, \quad \text{hvor } D = b^2 - 4c; \tag{6.2.2}$$

her er $\sqrt{D}$ den sædvanlige (ikke-negative) kvadratrod, hvis $D \geqslant 0$, og $\sqrt{D} := i\sqrt{-D}$, hvis $D < 0$. Vi *antager* om polynomiet, at diskriminanten D ikke er et kvadrat (på et helt tal). Specielt er $D \neq 0$, så polynomiet har to forskellige rødder. Med ξ' betegner vi den anden rod. Vi kan fx vedtage, at ξ er roden, der fremkommer med fortegnet $+$ i (6.2.2), altså $\xi = (-b + \sqrt{D})/2$; så er $\xi' = (-b - \sqrt{D})/2$. Da ξ og ξ' er de to rødder i (6.2.1) følger det, at

$$\xi + \xi' = -b, \qquad \xi\xi' = c, \quad \text{og} \quad (\xi - \xi')^2 = D. \tag{6.2.3}$$

Tallet ξ kan være *reelt* (nemlig når $D > 0$) eller *imaginært* (nemlig når $D < 0$).

Antagelsen om at D ikke er et kvadrat medfører, at roden ξ er et irrationalt tal, dvs $\xi \notin \mathbb{Q}$. Antag nemlig, indirekte, at ξ var en brøk, $\xi = a/s$, hvor vi kan antage, at $s \geqslant 1$ og at a og s er primiske. Af ligningen $(a/s)^2 + b(a/s) + c = 0$ fås, ved multiplikation med s^2, at

$$a^2 = s(-ba - cs).$$

Ethvert primtal, der går op i s, går derfor også op i a^2 og dermed op i a. Det følger, at $s = 1$. Altså er $\xi = a$, og vi har ligningen $a^2 + ba + c = 0$. For diskriminanten får vi $D = b^2 - 4c = b^2 + 4(a^2 + ba) = (2a + b)^2$, i modstrid med at D ikke var et kvadrattal.

(6.3) Observation. *Under antagelserne i* (6.2) *gælder:* (1) *Delmængden af* $\mathbb{C}$,

$$\mathbb{Z}[\xi] := \{\, x + y\xi \mid x, y \in \mathbb{Z}\}, \tag{6.3.1}$$

er en delring.

(2) *For $\alpha \in \mathbb{Z}[\xi]$ gælder, at i fremstillingen $\alpha = x + y\xi$ med $x, y \in \mathbb{Z}$ er koefficienterne x, y entydigt bestemt.*

(3) *Konjugering, bestemt ved at tallet* $\alpha = x + y\xi \in \mathbb{Z}[\xi]$ *afbildes på tallet* $\alpha' := x + y\xi'$, *er en ringisomorfi af talringen* $\mathbb{Z}[\xi]$ *på sig selv. Den er involutorisk i den forstand, at* $\alpha'' = \alpha$.

(4) *For alle* $\alpha = x + y\xi \in \mathbb{Z}[\xi]$ *er tallene* $\alpha + \alpha'$ *og* $\alpha\alpha'$ *hele tal, og*

$$\mathrm{N}(\alpha) := \alpha\alpha' = x^2 - bxy + cy^2. \tag{6.3.2}$$

Endelig er $\alpha \mapsto \mathrm{N}(\alpha)$ *en multiplikativ afbildning* $\mathrm{N}\colon \mathbb{Z}[\xi] \to \mathbb{Z}$.

Bevis. (1) Tal $x \in \mathbb{Z}$ har fremstillingen $x = x + 0\xi$, så $\mathbb{Z} \subseteq \mathbb{Z}[\xi]$; specielt ligger tallene 1 og -1 i $\mathbb{Z}[\xi]$. Betragt to tal $\alpha_1 = x_1 + y_1\xi$ og $\alpha_2 = x_2 + y_2\xi$ i delmængden $\mathbb{Z}[\xi]$. For summen finder vi $\alpha_1 + \alpha_2 = (x_1 + x_2) + (y_1 + y_2)\xi$. Det følger, at $\mathbb{Z}[\xi]$ er stabil under addition. For produktet finder vi ligningen,

$$\alpha_1\alpha_2 = x_1x_2 + (x_1y_2 + y_1x_2)\xi + y_1y_2\xi^2. \tag{6.3.3}$$

Da ξ er rod i polynomiet (6.2.1) er $\xi^2 = -c - b\xi$. Indsættes dette udtryk for ξ^2 på ligningens højreside ses, at $\alpha_1\alpha_2$ ligger i $\mathbb{Z}[\xi]$. Altså er $\mathbb{Z}[\xi]$ også stabil under multiplikation. Følgelig er $\mathbb{Z}[\xi]$ en delring.

(2) Entydigheden af fremstillingen følger af, at ξ ikke er et rationalt tal: Af to fremstillinger, $\alpha = x + y\xi = x_1 + y_1\xi$, får vi nemlig ligningen $(y - y_1)\xi = x_1 - x$. Hvis $y_1 \neq y$, ville det følge af ligningen efter division med $y - y_1$, at ξ er et rationalt tal. Altså er $y_1 = y$, og så følger det af ligningen, at $x_1 = x$.

(3) Af definitionen $(x + y\xi)' := x + y\xi'$ følger umiddelbart, at konjugering er en additiv homomorfi, og at konjugering af hele tal er den identiske afbildning; specielt afbilder konjugering 1 på 1. Tallene ξ og ξ' er rødder i $X^2 + bX + c$, så vi har $\xi^2 = -c - b\xi$ og $(\xi')^2 = -c - b\xi'$. Konjugering afbilder derfor ξ^2 på $(\xi')^2$. Af ligningen (6.3.3) følger nu, at konjugering også er multiplikativ. Altså er konjugering en ringhomomorfi. Den første ligning i (6.2.3) kan omskrives:

$$\xi' = -b - \xi. \tag{6.3.4}$$

Heraf fremgår specielt, at $\xi' \in \mathbb{Z}[\xi]$. Da $\mathbb{Z}[\xi]$ er delring, følger det, at $\alpha' = x + y\xi' \in \mathbb{Z}[\xi]$. Konjugering afbilder altså delringen $\mathbb{Z}[\xi]$ ind i sig selv. Af (6.3.4) følger også, at $\xi'' = \xi$, og heraf følger videre, at $\alpha'' = \alpha$ for alle $\alpha \in \mathbb{Z}[\xi]$. Konjugering, som en afbildning af $\mathbb{Z}[\xi]$ ind i sig selv, er altså „sin egen inverse“; specielt er konjugering bijektiv. Hermed er (3) eftervist.

(4) Af (6.2.3) følger umiddelbart, at

$$(x + y\xi) + (x + y\xi') = 2x - by, \quad (x + y\xi)(x + y\xi') = x^2 - bxy + cy^2.$$

Specielt gælder (6.3.2). Da højresiderne øjensynlig er hele tal, er $\alpha + \alpha' \in \mathbb{Z}$ og $\alpha\alpha' \in \mathbb{Z}$. Da konjugering er en multiplikativ afbildning, følger det for $\alpha, \beta \in \mathbb{Z}[\xi]$, at

$$\mathrm{N}(\alpha\beta) = \alpha\beta(\alpha\beta)' = \alpha\beta\alpha'\beta' = \alpha\alpha'\beta\beta' = \mathrm{N}(\alpha)\,\mathrm{N}(\beta).$$

Afbildningen $\mathrm{N}\colon \mathbb{Z}[\xi] \to \mathbb{Z}$ er altså multiplikativ. □

(6.4) Definition. En delring $R \subseteq \mathbb{C}$, der er af formen $R = \mathbb{Z}[\xi]$ som beskrevet i (6.3), kaldes en *kvadratisk talring*, og tallene heri kaldes *kvadratiske tal*. Talringen kaldes *reel* eller *imaginær* eftersom tallet ξ er reelt eller imaginært (dvs ikke-reelt).

For $\alpha = x + y\xi \in \mathbb{Z}[\xi]$ kaldes tallet $\mathrm{N}(\alpha) = \alpha\alpha'$ med et gammelt ord for *normen* af α. Det følger af (6.3)(4), at normen er multiplikativ. Nulreglen gælder for komplekse tal, så hvis $\alpha\alpha' = 0$, så må en af faktorerne være 0. Hvis $\alpha' = 0$, så er også $\alpha = \alpha'' = 0$. Med andre ord: Normen $\mathrm{N}(\alpha)$ er kun 0, hvis $\alpha = 0$.

Ringen $\mathbb{Z}[\xi]$ omfatter de hele tal, og for et helt tal x følger det af definitionen, at $x' = x$. Normen af x er derfor kvadratet $\mathrm{N}(x) = x^2$.

Polynomiet (6.2.1) har specielt reelle koefficienter. Med roden ξ er derfor også det komplekst konjugerede tal $\bar{\xi}$ rod. Dette er naturligvis uinteressant i det reelle tilfælde, hvor $\bar{\xi} = \xi$. I det imaginære tilfælde er $\bar{\xi} \neq \xi$. Følgelig er $\bar{\xi} = \xi'$. Heraf følger videre, for $\alpha = x + y\xi \in \mathbb{Z}[\xi]$, at

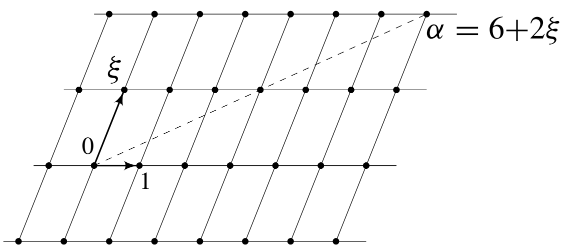
$$\bar{\alpha} = \overline{x + y\xi} = x + y\bar{\xi} = x + y\xi' = \alpha'.$$

Heraf ses i det imaginære tilfælde, at konjugering af tal i $\mathbb{Z}[\xi]$, som defineret i (6.3)(3), blot er sædvanlig kompleks konjugering. Det følger, at $\alpha\alpha' = \alpha\bar{\alpha}$, så i det imaginære tilfælde har vi ligningen

$$\mathrm{N}(\alpha) = \alpha\bar{\alpha} = |\alpha|^2;$$

normen $\mathrm{N}(\alpha)$ er altså kvadratet på den numeriske værdi af α; specielt er $\mathrm{N}(\alpha) \geqslant 0$.

I det imaginære tilfælde ($D < 0$), er tallet ξ ikke reelt. Idet vi på sædvanlig måde opfatter $\mathbb{C}$ som et 2-dimensionalt vektorrum over $\mathbb{R}$, er tallene 1 og ξ en basis. Tallene $\alpha = x + y\xi$ i R kan altså opfattes som de vektorer, der er heltalslinearkombinationer af de to basisvektorer; de kaldes også *gitterpunkter* mht basen $1, \xi$. Elementerne i $\mathbb{Z}[\xi]$ kan anskueliggøres på en figur:



og $\mathrm{N}(\alpha)$ er kvadratet på afstanden mellem punkterne 0 og α i planen.

I det reelle tilfælde er tallet ξ reelt, og dermed er alle tal i $\mathbb{Z}[\xi]$ reelle. Altså er $\mathbb{Z}[\xi]$ en delring af $\mathbb{R}$, og på en figur vil alle tallene i $\mathbb{Z}[\xi]$ ligge på den reelle akse. Det er ikke så svært at vise, at de ligger overalt tæt:

Normen $\mathrm{N}(\alpha)$ har ingen fortolkning i forhold til figuren.

(6.5) Note. Den kvadratiske talring $\mathbb{Z}[\xi]$ afhænger kun af diskriminanten D af polynomiet (6.2.1). Betragt nemlig endnu en kvadratiske talring $\mathbb{Z}[\xi_1]$, hvor ξ_1 er rod i et polynomium $X^2 + b_1X + c_1 \in \mathbb{Z}[X]$ med samme diskriminant, $b_1^2 - 4c_1 = D$. Det følger specielt, at $b_1 \equiv b \pmod 2$. I formlen (6.2.3) og den tilsvarende formel for ξ_1, kan vi antage, at $\sqrt{D}$ optræder med samme fortegn, idet vi ellers erstatter ξ med ξ'. Det følger, at $\xi_1 = k + \xi$, hvor $k := -(b_1 - b)/2$ er et helt tal. Specielt er $\xi_1 \in \mathbb{Z}[\xi]$. Da $\mathbb{Z}[\xi]$ er en ring, følger det, at $x + y\xi_1 \in \mathbb{Z}[\xi]$ for alle hele tal x, y. Altså er $\mathbb{Z}[\xi_1] \subseteq \mathbb{Z}[\xi]$. Symmetrisk har vi den modsatte inklusion, og dermed den påståede lighed.

Ethvert tal D, som modulo 4 er kongruent med 0 eller 1, er en diskriminant. Hvis D er lige, har vi nemlig $D = -4c$, så D er diskriminanten af polynomiet $X^2 + c$, og hvis D er ulige, er $D = 1 - 4c$, så D er diskriminanten af polynomiet $X^2 + X + c$. Øjensynlig er $-4c$ et kvadrattal, hvis og kun hvis $c = -d^2$ med et helt tal d, og $1 - 4c$ er et kvadrattal, hvis og kun hvis $c = -d(d-1)$ med et helt tal d. De kvadratiske talringe med henholdsvis lige og ulige diskriminanter er altså ringene $\mathbb{Z}[\xi]$, hvor ξ er rod i et polynomium, henholdsvis,

$$\begin{aligned} X^2 + c, &\quad \text{hvor } c \text{ ikke er af formen } -d^2, \\ X^2 + X + c, &\quad \text{hvor } c \text{ ikke er af formen } -d(d-1). \end{aligned}$$

De numerisk mindste diskriminanter,

$$-12, -11, -8, -7, -4, -3, 5, 8, 12, 13, 17, 20,$$

fås fra polynomierne,

$$\begin{gathered} X^2+3,\ X^2+X+3,\ X^2+2,\ X^2+X+2,\ X^2+1,\ X^2+X+1, \\ X^2+X-1,\ X^2-2,\ X^2-3,\ X^2+X-3,\ X^2+X-4,\ X^2-5. \end{gathered}$$

(6.6) Eksempel. (1) Tallet $i = \sqrt{-1}$ er rod i polynomiet $X^2 + 1$, der har diskriminant -4. Ringen $\mathbb{Z}[i]$ består af komplekse tal $x + yi$, hvor x, y er hele tal, altså af de komplekse tal, hvor real- og imaginærdel er hele tal. Ringen $\mathbb{Z}[i]$ kaldes *Gauss' talring*. Som eksempel på en udregning i $\mathbb{Z}[i]$ har vi ligningerne,

$$(5+i)^4 = (24+10i)^2 = 2^2(119+120i) = 2(1+i)(1-i)(119+120i) = 2(1+i)(239+i).$$

Ligningen giver relationer mellem de to siders argumenter og normer. Argumentet for tallet $x + iy$ er $\arctan \frac{y}{x}$, når $x > 0$. Ligningen i Gauss' talring giver derfor ligningen mellem argumenterne,

$$4 \arctan \frac{1}{5} = \frac{\pi}{4} + \arctan \frac{1}{239},$$

en formel, der er velegnet til beregning af π (Machin, 1706).

Tallet $x + yi$ har normen $x^2 + y^2$, som er kvadratet på den numeriske værdi. Specielt er $\mathrm{N}(5 + i) = 26 = 2 \cdot 13$. Ligningen i Gauss' talring giver derfor for normerne, at $2^4 \cdot 13^4 = 2^2 \cdot 2 \cdot (239^2 + 1)$, altså

$$2 \cdot 13^4 = 239^2 + 1.$$

(2) Tallet $\tau := (1+\sqrt{5})/2$ („det gyldne snit") er rod i polynomiet $X^2 - X - 1$, der har diskriminant 5. Ringen $\mathbb{Z}[\tau]$ består af tal $x + y\tau$, hvor x, y er hele tal, og regning i $\mathbb{Z}[\tau]$ foregår ved at udnytte, at $\tau^2 = \tau + 1$. Som eksempel på en udregning har vi ligningerne,

$$(2+\tau)^4 = (4+\tau^2+4\tau)^2 = (5+5\tau)^2 = 5^2(2+3\tau).$$

(6.7) Enhederne. *Betragt den kvadratiske talring $R = \mathbb{Z}[\xi]$. Et tal $\varepsilon \in R$ er da en enhed i R, hvis og kun hvis* $\mathrm{N}(\varepsilon) = \pm 1$.

Bevis. Normen er en multiplikativ afbildning $\mathrm{N}\colon R \to \mathbb{Z}$, og $\mathrm{N}(1) = 1$. Antag, at ε er en enhed i R, altså at der findes et tal $\eta \in R$ således, at $\varepsilon\eta = 1$. Heraf fås $\mathrm{N}(\varepsilon)\,\mathrm{N}(\eta) = \mathrm{N}(1) = 1$, og så følger det, at $\mathrm{N}(\varepsilon)$ er en enhed i $\mathbb{Z}$ (med $\mathrm{N}(\eta)$ som den inverse). Derfor er $\mathrm{N}(\varepsilon) = \pm 1$.

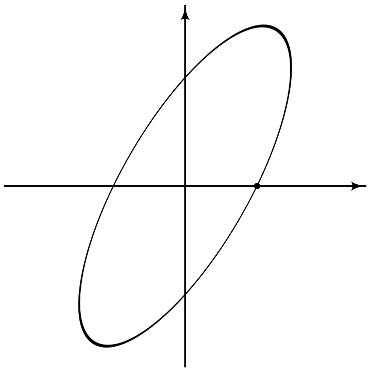
Antag omvendt, at $\mathrm{N}(\varepsilon) = \pm 1$, altså at $\varepsilon\varepsilon' = \pm 1$. Da er $\varepsilon(\pm\varepsilon') = 1$. Det følger, da $\pm\varepsilon' \in R$, at ε er invertibel i R (med $\pm\varepsilon'$ som den inverse). ∎

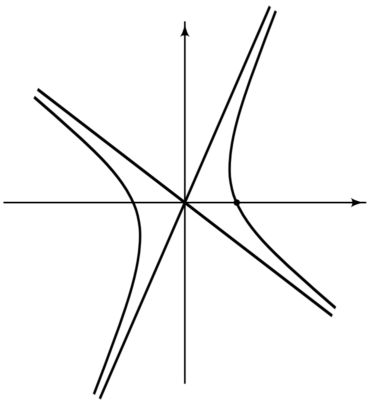
(6.8) Den kvadratiske ligning. Betragt den kvadratiske talring $R := \mathbb{Z}[\xi]$. Elementerne i R er tal af formen $\alpha = x + y\xi$, og x, y er entydigt bestemte hele tal. Derfor svarer tal $\alpha \in \mathbb{Z}[\xi]$ bijektivt til par $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ af hele tal. Ifølge (6.3.2) er $\mathrm{N}(x + y\xi) = x^2 - bxy + cy^2$. Vi udleder heraf:
For et givet helt tal k er der en bijektiv forbindelse mellem tal $\alpha \in R$ med $\mathrm{N}(\alpha) = k$ og par $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, som tilfredsstiller ligningen,

$$x^2 - bxy + cy^2 = k. \tag{6.8.1}$$

Ligningen er et af de simpleste eksempler på en såkaldt *diofantisk ligning*, dvs en ligning, hvortil man søger heltalsløsninger. I ligningen er b, c, k givne hele tal (og det er forudsat, at $D = b^2 - 4c$ ikke er et kvadrattal). At løse ligningen svarer altså til at bestemme de tal $\alpha \in R$, der har en given norm k. Som nævnt i (6.4) gælder $\mathrm{N}(\alpha) = 0$ kun for $\alpha = 0$. Heraf følger, at ligningen (6.8.1) for $k = 0$ kun har den trivielle løsning $(x, y) = (0, 0)$, men det er nu også let at se direkte.

Par (x, y) af hele tal kan opfattes som gitterpunkter i planen $\mathbb{R}^2$, dvs som punkter med heltalskoordinater. De reelle løsninger til ligningen (6.8.1) udgør et keglesnit i $\mathbb{R}^2$, og det diofantiske problem består i at bestemme hvilke gitterpunkter, der ligger på dette keglesnit. Mere præcist udgør løsningerne en ellipse, når $D < 0$ og $k > 0$, og en hyperbel, når $D > 0$ og $k \neq 0$.





I det imaginære tilfælde ($D < 0$) er det diofantiske problem trivielt: ellipsen er en begrænset delmængde af $\mathbb{R}^2$, og indeholder derfor kun endelig mange gitterpunkter.

Det reelle tilfælde ($D > 0$) er mere interessant. Man kan vise, at der på hyperblen er enten ingen eller uendelig mange gitterpunkter. Af speciel interesse er tilfældet $k = \pm 1$, altså ligningen,

$$x^2 - bxy + cy^2 = \pm 1. \tag{6.8.2}$$

Ligningen, med de to værdier $k = \pm 1$, bestemmer to hyperbler (altså fire hyperbelgrene). Som diofantisk ligning kaldes den også *Pell's ligning*. Det er et fundamentalt resultat af Lagrange, at Pell's ligning altid har uendelig mange løsninger, svarende til at hyperblerne indeholder uendelig mange gitterpunkter. At løse ligningen, med heltalsværdier af x, y, svarer ifølge (6.7) til at bestemme enhederne i ringen R. Ligningen har altid de trivielle løsninger $(x, y) = (\pm 1, 0)$, svarende til at tallene 1 og -1 er enheder i R. At ligningen (6.8.2) har uendelig mange løsninger betyder, at der i i ringen R findes uendelig mange enheder; specielt er der altid enheder $\varepsilon \neq \pm 1$ i det reelle tilfælde.

I det imaginære tilfælde ($D < 0$) udgør tallene i $\mathbb{Z}[\xi]$ et gitter i den komplekse plan, jfr (6.4), og normen er kvadratet på den numeriske værdi: $\mathrm{N}(\alpha) = |\alpha|^2$. Specielt er normen altid ikke-negativ, så ligningen (6.8.1) har ingen løsninger hvis $k < 0$. Hvis $k > 0$, ses det, at tallene α med $\mathrm{N}(\alpha) = k$ netop er gitterpunkterne på cirklen med radius $\sqrt{k}$. Det følger (igen), at ligningen (6.8.1) kun har endelig mange løsninger. Ligningen (6.8.2), for $k = 1$, svarer til at bestemme gitterpunkterne på enhedscirklen.

(6.9) Bemærkning. Imaginære enheder. Antag, at $D < 0$. Lad os her vise, at enhederne i $R = \mathbb{Z}[\xi]$ kun er ± 1, med undtagelse af følgende to tilfælde:

$$D = -3, \quad \text{hvor } R^* = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\},$$
$$D = -4, \quad \text{hvor } R^* = \{1, i, i^2, i^3\}.$$

hvor $\zeta = \frac{1}{2} + \frac{i}{2}\sqrt{3}$ er en 6'te enhedsrod (og i som sædvanlig er en 4'de enhedsrod).

Bevis. Det er klart, at vi altid har $\{\pm 1\} \subseteq R^*$, og vi skal (bl.a.) vise, at lighed gælder med mindre $D = -3$ eller $D = -4$. Antag, at inklusionen er ægte, altså at der findes en enhed $\varepsilon = u + v\xi \in R$ med $\varepsilon \neq \pm 1$. Da $D < 0$, er $\mathrm{N}(\alpha) \geqslant 0$. Specielt gælder for enheden ε, at $\varepsilon\varepsilon' = 1$. Polynomiet $(X - \varepsilon)(X - \varepsilon')$ har ε som rod, og det har hele koefficienter ifølge Observation (6.3)(4). Da $\varepsilon\varepsilon' = 1$, er ε altså rod i et polynomium,

$$X^2 + eX + 1 \qquad \text{med } e \in \mathbb{Z}. \tag{*}$$

Diskriminanten er $e^2 - 4$ og lig med kvadratet $(\varepsilon - \varepsilon')^2$. Da $\varepsilon = u + v\xi$, er $\varepsilon - \varepsilon' = v(\xi - \xi')$. Derfor er

$$e^2 - 4 = (\varepsilon - \varepsilon')^2 = (\xi - \xi')^2 v^2 = v^2 D.$$

Da $\varepsilon \neq \pm 1$, er $v \neq 0$. Da $D < 0$, må vi have $e^2 - 4 < 0$, og derfor er $e = \pm 1$ eller $e = 0$. I det først tilfælde er $v^2 D = 1 - 4 = -3$, og heraf følger $D = -3$ (og $v = \pm 1$). I det andet tilfælde er $v^2 D = -4$, og heraf følger $D = -4$ (og $v = \pm 1$) (da $D = -1$ er udelukket).

Polynomiet $X^2 - X + 1$ har diskriminant -3 og roden ζ. Hvis $D = -3$, følger det, jfr Note (6.5), at $R = \mathbb{Z}[\zeta]$. Enhederne bestemmes ved at løse ligningen $x^2 + xy + y^2 = 1$ med $x, y \in \mathbb{Z}$. Omskrivningen $(x + \frac{1}{2}y)^2 + \frac{3}{4}y^2 = 1$ viser, at $|y| \leqslant 1$, og herefter er det klart, at den fuldstændige løsning til ligningen er $\pm(1, 0)$, $\pm(0, 1)$, og $\pm(1, -1)$. Der er altså 6 løsninger, svarende til at de 6 potenser af ζ er samtlige enheder.

Polynomiet X^2+1 har diskriminant -4 og roden i. Hvis $D=-4$, følger det, jfr Note (6.5), at $R=\mathbb{Z}[i]$, hvor vi allerede har bestemt enhederne som de 4 anførte potenser af i. $\square$

Hermed er gruppen R^* af enheder bestemt i alle tilfælde. Oversat til et udsagn om løsninger $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ til den diofantiske ligning:

$$x^2-bxy+cy^2=1, \quad \text{hvor } b,c\in\mathbb{Z} \text{ og } D:=b^2-4c<0,$$

er det vist, at de eneste løsninger er de 2 trivielle løsninger $(\pm1,0)$, undtagen hvis $D=-3$, hvor der er yderligere 4 løsninger $\pm((b+1)/2,1)$ og $\pm((b-1)/2,1)$, eller hvis $D=-4$, hvor der er yderligere 2 løsninger $\pm(b/2,1)$.

Eksempel. Ligningen $x^2-5xy+7y^2=1$ har diskriminanten $D=5^2-4{\cdot}7=-3$. Den har derfor de 6 løsninger $\pm(1,0)$, $\pm(3,1)$ og $\pm(2,1)$ og ikke andre heltalsløsninger.

(6.10) Bemærkning. Reelle enheder. Antag, at $D>0$. Den diofantiske ligning (6.8.2) kaldes som nævnt Pell's ligning. At løse ligningen svarer til at bestemme enhederne i $R=\mathbb{Z}[\xi]$. Som nævnt kan man vise, at der altid findes enheder forskellige fra ±1 i R. Mere præcist kan man vise, at gruppen R^* af enheder ε består af alle elementer $\pm\varepsilon_1^n$ for $n\in\mathbb{Z}$, med en passende enhed $\varepsilon_1\neq\pm1$. Der er fire mulige valg af ε_1, nemlig med ε_1 også $-\varepsilon_1$ og $\pm\varepsilon_1^{-1}$. Disse fire enheder kaldes *grundenhederne*. Hvis grundenheden ε_1 har normen 1, så er $\mathrm{N}(\pm\varepsilon_1^n)=1$ for alle n; i dette tilfælde findes altså ingen enheder ε med $\mathrm{N}(\varepsilon)=-1$. Hvis grundenheden ε_1 har normen -1, så er $\mathrm{N}(\pm\varepsilon_1^n)=(-1)^n$. Enhederne med norm 1 er altså enhederne af formen $\varepsilon=\pm\varepsilon_2^m$, hvor $\varepsilon_2:=\varepsilon_1^2$.

Grundenheden har formen $\varepsilon_1=u_1+v_1\xi$ med hele tal u_1 og v_1. Oversat til et udsagn om løsninger $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ til Pell's ligning,

$$x^2-bxy+cy^2=\pm1, \quad \text{hvor } b,c\in\mathbb{Z} \text{ og } D:=b^2-4c>0,$$

og D ikke er et kvadrattal, er påstanden altså følgende: Der eksisterer altid en ikke-triviel *grundløsning*, dvs en løsning (u_1,v_1) således, at samtlige heltalsløsninger er

$$\pm(u_n,v_n), \quad \text{for } n\in\mathbb{Z},$$

hvor u_n og v_n er bestemt ved ligningen,

$$(u_1+v_1\xi)^n=u_n+v_n\xi.$$

Hvis grundløsningen løser ligningen $x^2-bxy+cy^2=1$, så har ligningen $x^2-bxy+cy^2=-1$ ingen løsninger. Hvis grundløsningen løser ligningen $x^2-bxy+cy^2=-1$, så fås samtlige løsninger til ligningen $x^2-bxy+cy^2=1$ ud fra løsningen (u_2,v_2).

Eksempel. Ligningen $x^2-13y^2=\pm1$ har diskriminanten $-4(-13)=52$. Parret $(18,5)$ er en løsning, idet $18^2-13{\cdot}5^2=-1$. Man kan vise, at $(18,5)$ er grundløsningen. For at bestemme en løsning til ligningen $x^2-13y^2=1$ udregner vi kvadratet,

$$(18+5\sqrt{13})^2=18{\cdot}18+5{\cdot}5{\cdot}13+2{\cdot}18\cdot5\sqrt{13}=649+180\sqrt{13}.$$

Parret $(649,180)$ er altså en løsning til $x^2-13y^2=1$. Den „næste“ løsning fås ved at kvadrere $649+180\sqrt{13}$, som giver løsningen $(842401, 233640)$.

(6.11) Divisorer. Betragt den kvadratiske talring $R=\mathbb{Z}[\xi]$. For to tal α og δ i R, med $\delta\neq0$, er δ divisor i α, hvis der findes et tal $\beta\in R$ således, at $\alpha=\beta\delta$. Ligningen $\alpha=\beta\delta$ medfører naturligvis, at β er det komplekse tal α/δ. At δ er divisor i α betyder altså, at kvotienten α/δ, som a priori blot er et komplekst tal, igen er et tal i R. Øjensynlig er

$$\frac{\alpha}{\delta} = \frac{\alpha\delta'}{\delta\delta'} = \frac{\alpha\delta'}{\mathrm{N}(\delta)}. \tag{6.11.1}$$

På højresiden ligger tælleren, $\alpha\delta'$, i $R = \mathbb{Z}[\xi]$, så tælleren har formen $x + y\xi$ med hele tal x, y. Nævneren, $n := \mathrm{N}(\delta)$, er et helt tal forskelligt fra 0. Kvotienten α/δ har altså formen $(x/n) + (y/n)\xi$ med hele tal x, y, n hvor $n \neq 0$, altså formen

$$\lambda + \mu\xi, \quad \text{hvor } \lambda, \mu \in \mathbb{Q}. \tag{6.11.2}$$

For et komplekst tal, der kan fremstilles på formen (6.11.2), er fremstillingen entydig, dvs koefficienterne λ og μ er entydigt bestemte; det er vist i Observation (6.3) under antagelse af at $\lambda, \mu \in \mathbb{Z}$, men beviset er det samme, når $\lambda, \mu \in \mathbb{Q}$. Specielt ligger et tal af formen (6.11.2) i $\mathbb{Z}[\xi]$, hvis og kun hvis de to koefficienter λ og μ er hele tal.

Det er således simpelt at afgøre, om δ, i ringen R, er divisor i α: Fremstil kvotienten α/δ ved hjælp af udregningen i (6.11.1) på formen (6.11.2), og undersøg, om de fremkomne rationale koefficienter λ og μ begge er hele tal. Det skal understreges, at problemet er helt trivielt, hvis $\delta = d$ er et helt tal. For $\beta = u + v\xi$ har vi nemlig, at $\beta d = (du) + (dv)\xi$; tallet $\alpha = x + y\xi$ er således deleligt med d, hvis og kun hvis både x og y er delelige med d, dvs hvis og kun hvis d er en fælles divisor for x, y.

Fx gælder i $\mathbb{Z}[i]$, at $2+5i$ er divisor i $4-19i$, idet

$$\frac{4-19i}{2+5i} = \frac{(4-19i)(2-5i)}{(2+5i)(2-5i)} = \frac{-87-58i}{29} = -3-2i.$$

(Ligningen $(2+5i)(-3-2i) = 4-19i$ giver naturligvis et enklere bevis for at $2+5i$ er divisor i $4-19i$.) Derimod er $2+5i$ ikke divisor i $4+19i$, idet

$$\frac{4+19i}{2+5i} = \frac{(4+19i)(2-5i)}{(2+5i)(2-5i)} = \frac{103+18i}{29} = \frac{103}{29} + \frac{18}{29}i.$$

Tilsvarende gælder i $\mathbb{Z}[\sqrt{3}]$, at $10-\sqrt{3}$ er divisor i $1-165\sqrt{3}$, idet

$$\frac{1-165\sqrt{3}}{10-\sqrt{3}} = \frac{(1-165\sqrt{3})(10+\sqrt{3})}{(10-\sqrt{3})(10+\sqrt{3})} = \frac{-485-1649\sqrt{3}}{97} = -5-17\sqrt{3}.$$

(6.12) Sætning. *Lad α og $\delta \neq 0$ være to tal i den kvadratiske talring $R = \mathbb{Z}[\xi]$. Hvis δ i ringen R er divisor i α, så gælder i ringen $\mathbb{Z}$, at $\mathrm{N}(\delta)$ er divisor i $\mathrm{N}(\alpha)$. Yderligere gælder, når δ er divisor i α, at δ er en triviel divisor, hvis og kun hvis $\mathrm{N}(\delta)$ i ringen $\mathbb{Z}$ er en triviel divisor i $\mathrm{N}(\alpha)$, dvs hvis og kun hvis enten $\mathrm{N}(\delta) = \pm\mathrm{N}(\alpha)$ eller $\mathrm{N}(\delta) = \pm 1$.*

Bevis. Antag, at $\alpha = \delta\beta$ med $\beta \in R$. Da $\mathrm{N}\colon R \to \mathbb{Z}$ er multiplikativ, får vi ligningen $\mathrm{N}(\alpha) = \mathrm{N}(\delta)\,\mathrm{N}(\beta)$ i ringen $\mathbb{Z}$. Heraf følger den første påstand. At δ er en triviel divisor i α betyder, at δ er en enhed eller at β er en enhed. Ifølge (6.7) indtræffer det, hvis og kun hvis enten $\mathrm{N}(\delta) = \pm 1$ eller $\mathrm{N}(\beta) = \pm 1$. Heraf følger den anden påstand. ▯

(6.13) Korollar. *I en kvadratisk talring $R = \mathbb{Z}[\xi]$ eksisterer irreducible opløsninger for alle elementer.*

Bevis. Dette følger af Note (5.14), idet vi som funktion $\nu\colon R \to \mathbb{Z}$ kan bruge funktionen $\nu(\alpha) := |\,\mathrm{N}(\alpha)|$. Øjensynlig er ν nedad begrænset, og det følger af Sætning (6.12), at hvis δ er en ikke-triviel divisor i α, så er $\nu(\delta) < \nu(\alpha)$. □

(6.14) Lemma. *Lad $R = \mathbb{Z}[\xi]$ være en kvadratisk talring, og lad $\pi = x + y\xi$ være et element i R, hvor koefficienterne x, y er primiske. Betragt følgende tre betingelser på π:*

(i) *π er et primelement i R.*
(ii) *$\mathrm{N}(\pi) = \pm p$, hvor p er et primtal.*
(iii) *π er irreducibelt i R.*

Da gælder: (i)⇒(ii)⇒(iii). *Hvis R er faktoriel, er alle tre betingelser ækvivalente.*

Bevis. (i)⇒(ii): Antag, at π er et primelement. Specielt er π så ikke 0 og ikke en enhed, og så er $|\,\mathrm{N}(\pi)| > 1$. Derfor har $|\,\mathrm{N}(\pi)|$ en primopløsning som et produkt af sædvanlige primtal. Primelementet π går op i $|\,\mathrm{N}(\pi)| = \pm\pi\pi'$; derfor går π op i en af produktets faktorer, lad os sige, at $\pi \mid p$, hvor p er et sædvanligt primtal. Nu er $p = \delta\pi$ med et element $\delta \in R$. For normerne følger det, at $p^2 = \mathrm{N}(\delta)\,\mathrm{N}(\pi)$. Heraf følger videre, at $\mathrm{N}(\pi) = \pm 1$ eller $\mathrm{N}(\pi) = \pm p$ eller $\mathrm{N}(\pi) = \pm p^2$. Den første mulighed kan udelukkes, da π ikke er en enhed. Den tredie mulighed kan også udelukkes: var nemlig $\mathrm{N}(\pi) = \pm p^2$, så var $\mathrm{N}(\delta) = \pm 1$, og dermed δ en enhed; er $\varepsilon = u + v\xi$ den inverse til δ, så følger af $p = \delta\pi$, at $\pi = \varepsilon p = pu + pv\xi$, altså $x = pu$ og $y = pv$, i modstrid med at x, y var primiske. Tilbage bliver altså den anden mulighed, $\mathrm{N}(\pi) = \pm p$, som ønsket.

(ii)⇒(iii): Antag, at $\mathrm{N}(\pi) = \pm p$, hvor p er et primtal. En ikke-triviel divisor i π ville så have en norm, der var en ikke-triviel divisor i primtallet p, hvilket er umuligt. Altså har π kun trivielle divisorer. Af (6.7) følger, at π ikke kan være en enhed, og trivielt er $\pi \neq 0$. Derfor er π irreducibel.

Når R er faktoriel, gælder som bekendt, at irreducible elementer og primelementer er de samme. Specielt gælder så, at (iii)⇒(i), og så er alle betingelserne ækvivalente. □

Mere generelt ses, som i beviset for (ii)⇒(iii), at hvis $|\,\mathrm{N}(\pi)| > 1$, og hvis intet element i R har en norm, der er en ikke-triviel divisor i $\mathrm{N}(\pi)$, så er π irreducibel i R.

Man kan vise, at betingelserne (i) og (ii) er ækvivalente uden forudsætning om at R er faktoriel, se Bemærkning (6.24).

(6.15) Eksempel. (1) Betragt Gauss' talring $R := \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$. For normen har vi $\mathrm{N}(x + iy) = x^2 + y^2$. For tallet $1 + i$ er $\mathrm{N}(1 + i) = 1^2 + 1^2 = 2$ et primtal; altså er $1 + i$ irreducibelt i R. Tilsvarende er $\mathrm{N}(2 + i) = 2^2 + 1^2 = 5$, så tallet $2 + i$ er irreducibelt. Ligningerne, i formen $2 = (1 + i)(1 - i)$ og $5 = (2 + i)(2 - i)$ viser også, at primtallene 2 og 5 er reducible i $\mathbb{Z}[i]$.

Ligningen $x^2 + y^2 = 3$ har øjensynlig ingen heltalsløsninger. Derfor har intet element i R normen 3. For tallet $3 \in R$ er $\mathrm{N}(3) = 3^2$, så en ikke-triviel divisor i 3 (inden for R) ville have norm 3, hvilket er udelukket. Derfor er primtallet 3 irreducibelt i R.

(2) Betragt ringen $R := \mathbb{Z}[\sqrt{-5}]$, med diskriminant $D = -20$. Med $\xi := \sqrt{-5}$ har vi $\mathrm{N}(x + y\xi) = x^2 + 5y^2$. Vi har $\mathrm{N}(1 + \sqrt{-5}) = 1 + 5 = 2 \cdot 3$. Ingen elementer i R har øjensynlig norm 2 eller norm 3. Altså kan intet element i R være en ikke-triviel divisor i $1 + \sqrt{-5}$. Tallet $1 + \sqrt{-5}$ er altså et irreducibelt element i R. Af samme grund følger det, at $1 - \sqrt{-5}$ er irreducibel. Da $\mathrm{N}(2) = 2^2$ og $\mathrm{N}(3) = 3^2$, følger det tilsvarende, at 2 og 3 er irreducible. Vi har altså i $\mathbb{Z}[\sqrt{-5}]$ to irreducible opløsninger af tallet 6,

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

(3) Betragt ringen $R := \mathbb{Z}[\sqrt{10}]$, med diskriminant 40. Det påstås, at tallene 2 og 5 irreducible. Det skal hertil vises, at ligningerne $x^2 - 10y^2 = \pm 2$ og $x^2 - 10y^2 = \pm 5$ ikke har heltalsløsninger. For den første ligning regnes modulo 5: for en løsning ville vi få $x^2 \equiv \pm 2$, i modstrid med at et kvadrat modulo 5 er kongruent med 0, 1, eller 4. For den anden ligning regnes modulo 8. Det er klart, at x må være ulige, og følgelig er $x^2 \equiv 1$. Videre er $-10y^2 \equiv 6y^2$ og $6y^2$ er kongruent med 0 når y er lige og kongruent med 6 når y er ulige. Altså er $x^2 - 10y^2$ kongruent med 1 eller 7, i modstrid med at $x^2 - 10y^2 = \pm 5$.

Nu følger det videre, at tallet $\sqrt{10}$ er irreducibelt, thi $\sqrt{10}$ har norm -10, og en ikke-triviel divisor i $\sqrt{10}$ måtte derfor have norm ± 2 eller ± 5. Vi har altså i $\mathbb{Z}[\sqrt{10}]$ to irreducible opløsninger af tallet 10,

$$10 = 2 \cdot 5 = \sqrt{10} \cdot \sqrt{10}.$$

(6.16) Sætning. (1) *De kvadratiske talringe* $\mathbb{Z}[i]$ (*Gauss' talring*) *og* $\mathbb{Z}[\sqrt{2}]$ *er hovedideal-områder* (*og dermed faktorielle ringe*).

(2) *De kvadratiske talringe* $\mathbb{Z}[\sqrt{-5}]$ *og* $\mathbb{Z}[\sqrt{10}]$ *er ikke faktorielle ringe.*

Bevis. (1) For $R := \mathbb{Z}[i]$ viser vi, at den ved $\nu(\alpha) := \mathrm{N}(\alpha) = |\alpha|^2$ definerede funktion $\nu \colon R \to \mathbb{Z}$ har den i Bemærkning (5.6) nævnte egenskab. Funktionen er nedad begrænset, idet $\nu(\alpha) \geqslant 0$. Vi skal altså vise, for givne tal δ, α i $\mathbb{Z}[i]$ med $\delta \neq 0$, at der findes et tal $\beta \in R$ med $\nu(\alpha - \beta\delta) < \nu(\delta)$. Denne ulighed er øjensynlig ensbetydende med uligheden,

$$\left| \frac{\alpha}{\delta} - \beta \right| < 1. \tag{*}$$

Idet tallene $\beta \in R$ er gitterpunkterne $x + yi$ med $x, y \in \mathbb{Z}$, ser vi, at der for ethvert komplekst tal $w \in \mathbb{C}$ findes et gitterpunkt β, hvis afstand til w højst er $\frac{1}{2}$ gange længden af diagonalen i et kvadrat med siden 1, altså højst $\sqrt{2}/2$. For hvert $w \in \mathbb{C}$ kan vi altså, med et gitterpunkt β, opfylde uligheden,

$$|w - \beta| \leqslant \frac{\sqrt{2}}{2};$$

specielt, for $w := \alpha/\delta$, kan vi opfylde uligheden (*).

For $R := \mathbb{Z}[\sqrt{2}]$ anvender vi igen resultatet (5.6), denne gang på funktionen $\nu : R \to \mathbb{Z}$ givet ved $\nu(\alpha) := |\,\mathrm{N}(\alpha)| = |\alpha\alpha'|$. Vi skal her, for givne tal $\alpha = a + b\sqrt{2}$ og $\delta = c + d\sqrt{2}$

med $\delta \neq 0$, bestemme $\beta = x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ således, at $\nu(\alpha - \beta\delta) < \nu(\delta)$. Efter division med $|\delta\delta'| = \nu(\delta)$ fås den ensbetydende ulighed,

$$\Bigl|\Bigl(\frac{\alpha}{\delta} - \beta\Bigr)\Bigl(\frac{\alpha'}{\delta'} - \beta'\Bigr)\Bigr| < 1. \tag{**}$$

Tallet α/δ har formen $\lambda + \mu\sqrt{2}$ med $\lambda, \mu \in \mathbb{Q}$, jfr (6.11), og det er let at se, at α'/δ' så har formen $\lambda - \mu\sqrt{2}$. Videre er $\beta = x + y\sqrt{2}$. Uligheden (**) kan derfor omskrives til følgende ulighed:

$$|(\lambda - x)^2 - 2(\mu - y)^2| < 1. \tag{***}$$

Her er λ, μ specielt reelle tal. Vi kan finde hele tal $x, y \in \mathbb{Z}$, så at $|\lambda - x| \leqslant \frac{1}{2}$ og $|\mu - y| \leqslant \frac{1}{2}$. Med dette valg af x og y er venstresiden i (***) endda højst lig med $(1/2)^2 + 2(1/2)^2 = 3/4$. Uligheden (***), og dermed (**), er altså specielt opfyldt.

Det fremgår af beviset, at de to talringe $\mathbb{Z}[i]$ og $\mathbb{Z}[\sqrt{2}]$ endda er euklidiske ringe.

(2) For ringene $R = \mathbb{Z}[\sqrt{-5}]$ og $\mathbb{Z}[\sqrt{10}]$ har vi vist i (6.15), at irreducible opløsninger ikke er entydige for alle elementer. Disse ringe er altså ikke faktorielle. □

(6.17) Bemærkning. I nogle tilfælde kan vi argumentere direkte for at givne elementer i R er irreducible. Antag, at $D < 0$, altså at $R = \mathbb{Z}[\xi]$ er imaginær. Vi viser for hele tal k, som opfylder $|k - b/2| \leqslant |D|/4 - 1$, at tallet $k + \xi$ i R kun har trivielle divisorer.

Antag hertil, at $1 + |k - b/2| \leqslant |D|/4$, og at δ er en ikke-triviel divisor i $k + \xi$. Koefficienten til ξ i $k + \xi$ er 1. De eneste hele tal, der går op i $k + \xi$ er derfor ± 1. Altså er $\delta = x + y\xi$, med $y \neq 0$. Af samme grund forekommer ξ med koefficient forskellig fra 0 i $(k + \xi)/\delta$. Denne koefficient bestemmes ved udregningen (hvor vi kun interesserer os for koefficienten til ξ),

$$\frac{k + \xi}{x + y\xi} = \frac{(k + \xi)(x + y\xi')}{(x + y\xi)(x + y\xi')} = \;\cdots + \frac{x - ky}{\mathrm{N}(x + y\xi)}\xi,$$

og den er altså et helt tal forskelligt fra 0. For koefficienten får vi udtrykket,

$$\frac{x - ky}{x^2 - bxy + cy^2} = \frac{1}{y} \cdot \frac{(x/y - b/2) - (k - b/2)}{(x/y - b/2)^2 + |D|/4}.$$

På højresiden er den første brøk, $1/y$, numerisk højst 1. I den anden brøk er nævner og tæller en sum af to led. Tælleren er numerisk højst lig med summen af de numeriske værdier. Ifølge forudsætningen har vi specielt, at $|k - b/2| < |D|/4$. Hvis $|x/y - b/2| \geqslant 1$, så er $|x/y - b/2| \leqslant (x/y - b/2)^2$; heraf følger umiddelbart, at tælleren numerisk er mindre end nævneren. Hvis $|x/y - b/2| < 1$, så er tælleren numerisk mindre end $1 + |k - b/2|$, og derfor mindre end $|D|/4$. Igen er tælleren altså numerisk mindre end nævneren. Den anden brøk er således i begge tilfælde numerisk mindre end 1. Højresiden er derfor numerisk mindre end 1. Da den var et helt tal forskelligt fra nul, er den ønskede modstrid opnået.

(6.18) Bemærkning. Man ved ikke, om der blandt de reelle kvadratiske talringe er uendelig mange faktorielle. For de imaginære kvadratiske talringe er situationen noget simplere. Vi vil her vise, for en lang række negative diskriminanter, at den tilhørende kvadratiske talring *ikke* er faktoriel.

De imaginære kvadratiske talringe har formen $R = \mathbb{Z}[\xi]$, hvor ξ er rod i $X^2 + X + c$ med ulige diskriminanent $1 - 4c$ eller rod i $X^2 + c$ med lige diskriminant $D = -4c$, for $c = 1, 2, \ldots$. Vi viser for en lang række værdier af c, at R *ikke* kan være UFD. Til $c = 1$ svarer $D = -3$ og $D = -4$, hvor ringen faktisk er PID. I det følgende antages, at $c \geqslant 2$.

I uligheden $|k - b/2| \leqslant -1 + |D|/4$ fra (6.17) er altså $b = 0$ eller $b = 1$. For $D = -4c$ og $b = 0$ er uligheden $|k| \leqslant -1 + c$ opfyldt for $k = 0, 1, \dots, c - 1$; for $D = 1 - 4c$ og $b = 1$ er uligheden $|k - 1/2| < -1 - 1/4 + c$ ligeledes opfyldt for $k = 0, 1, \dots, c - 1$. Det følger så af (6.17), for $0 \leqslant k \leqslant c - 1$, at tallet $k + \xi$ i R kun har trivielle divisorer. Tallet har norm $k^2 + c$, når D er lige, og norm $k^2 - k + c$, når D er ulige; da $c \geqslant 2$, er normen i begge tilfælde altså større end 1. *Tallet $k + \xi$ er derfor et irreducibelt element i R for $k = 0, \dots, c - 1$.*

Hvis R er faktoriel, følger det, for $k = 0, \dots, c - 1$, at $k + \xi$ er et primelement i R, og af Lemma (6.14) følger derfor, at normen $\mathrm{N}(k + \xi)$ er et primtal.

Betragt først tilfældet, hvor $D = -4c$ er lige. Normen er $\mathrm{N}(k + \xi) = k^2 + c$. *Hvis R er faktoriel, gælder altså, at $k^2 + c$ er et primtal for $k = 0, \dots, c - 1$.* Det følger først, for $k = 0$, at c er et primtal, og dernæst, for $k = 1$, at $1 + c$ er et primtal; altså er $c = 2$. Derfor er R *ikke* faktoriel, når $c > 2$, dvs for lige diskriminanter $D < -8$. Af imaginære talringe med lige diskriminant er det altså kun $\mathbb{Z}[i]$ med diskriminant -4 (svarende til $c = 1$, som vi udelod) og $\mathbb{Z}[\sqrt{-2}]$ med diskriminant -8 (svarende til $c = 2$), som kan være faktorielle.

Betragt dernæst tilfældet, hvor diskriminanten $D = 1 - 4c$ er ulige. Normen er $\mathrm{N}(k + \xi) = k^2 - k + c$. *Hvis R er faktoriel, gælder altså, at $k^2 - k + c$ er et primtal for $k = 0, \dots, c - 1$.* Det følger først, for $k = 0$, at c er et primtal. Videre er det nemt at udelukke mange primtalsværdier af c, fx følgende:

$$\begin{aligned}
c &= 7, \text{ fordi } 2^2 - 2 + 7 = 9; & c &= 37, \text{ fordi } 2^2 - 2 + 37 = 39;\\
c &= 13, \text{ fordi } 2^2 - 2 + 13 = 15; & c &= 43, \text{ fordi } 2^2 - 2 + 43 = 45;\\
c &= 19, \text{ fordi } 2^2 - 2 + 19 = 21; & c &= 47, \text{ fordi } 2^2 - 2 + 47 = 49;\\
c &= 23, \text{ fordi } 2^2 - 2 + 23 = 25; & c &= 53, \text{ fordi } 2^2 - 2 + 53 = 55;\\
c &= 29, \text{ fordi } 3^2 - 3 + 29 = 35; & c &= 59, \text{ fordi } 3^2 - 3 + 59 = 65;\\
c &= 31, \text{ fordi } 2^2 - 2 + 31 = 33; & c &= 61, \text{ fordi } 2^2 - 2 + 61 = 63.
\end{aligned}$$

Tilbage, for $c \leqslant 61$, er faktisk kun mulighederne $c = 1$ (som vi udelod) og $c = 2,3,5,11,17,41$. Sammen med de lige diskriminanter -4 og -8 får vi derfor følgende 9 mulige diskriminanter D med $-268 < D < 0$, hvor den kvadratiske talring kan være faktoriel:

$$-3,\ -4,\ -7,\ -8,\ -11,\ -19,\ -43,\ -67,\ -163.$$

Man kan vise, at de 9 kvadratiske talringe med disse diskriminanter faktisk er faktorielle, og (men det er ganske svært!) at der ikke er andre imaginære kvadratiske talringe, der er faktorielle.

Da ringen svarende til $c = 41$ er et UFD, må der gælde, at $k^2 - k + 41$ er et primtal for $k = 1, \dots, 40$ (hvilket jo også nemt vises direkte), et bemærkelsesværdigt fænomen, der allerede blev opdaget af Euler.

(6.19) Sætning. *Lad $R = \mathbb{Z}[\xi]$ være en kvadratisk talring, og lad p være et sædvanligt primtal. Betragt følgende fire betingelser på p:*

(i) *p er reducibel i R.*
(ii) *Ligningen $x^2 - bxy + cy^2 = \pm p$ har en løsning $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.*
(iii) *Kongruensen $z^2 - bz + c \equiv 0 \pmod p$ har en løsning $z \in \mathbb{Z}$.*
(iv) *p er ikke et primelement i R.*

Da gælder: (i)⇔(ii)⇒(iii)⇒(iv). *Hvis R er faktoriel, er alle fire betingelser ækvivalente.*

Bevis. (ii)⇒(i): Med $\alpha = x + y\xi$ betyder ligningen, at $\mathrm{N}(\alpha) = \pm p$, altså at $p = \alpha(\pm\alpha')$. Hvis ligningen er opfyldt, har p altså den ikke-trivielle divisor α.

(i)⇒(ii): Antag, at p har en ikke-triviel divisor π. Da $\mathrm{N}(p) = p^2$, følger det af Sætning (6.12), at $\mathrm{N}(\pi) = \pm p$. Med $\pi = x + y\xi$, er (x, y) så en løsning til ligningen i (ii).

(ii)⇒(iii): Antag, at ligningen $x^2 - bxy + cy^2 = \pm p$ er opfyldt. Tallet y kan ikke være deleligt med p, thi hvis $p \mid y$, følger det af ligningen, at $p \mid x^2$, og dermed at $p \mid x$, men så går p^2 op i ligningens venstreside, i modstrid med at højresiden er $\pm p$.

Modulo p følger det af ligningen, at vi har kongruensen $x^2 - bxy + cy^2 \equiv 0$. Ifølge det lige viste, er restklassen af y en primisk restklasse, så der findes et helt tal w med $wy \equiv 1 \pmod{p}$. Multiplicer kongruensen med w^2, og benyt at $wy \equiv 1$. Så fås $(wx)^2 - b(wx) + c \equiv 0$, og $z := wx$ er altså en en løsning til kongruensen i (iii).

(iii)⇒(iv): Antag, at z løser kongruensen i (iii), altså at der findes et helt tal d således, at $z^2 - bz + c = dp$. Denne ligning kan skrives

$$dp = (z + \xi)(z + \xi') = (z + \xi)(z - b - \xi),$$

så det fremgår specielt, at p går op i produktet $(z + \xi)(z - b - \xi)$. Men p går ikke op i nogen af faktorerne, da koefficienterne til ξ i de to faktorer er 1 og -1 og altså ikke delelig med p. Derfor er p ikke et primelement i R.

Antag endelig, at R er et UFD. Det følger så af generelle resultater, at et irreducibelt element er et primelement. Altså gælder implikationen (iv)⇒(i), og så er alle betingelserne ækvivalente. □

Bemærk, at biimplikationen (ii)⇔(iii), altså at den diofantiske ligning har løsninger, hvis og kun hvis kongruensen har løsninger, forudsætter, at den kvadratiske talring er faktoriel.

(6.20) Forgrening i faktorielle kvadratiske talringe. *Antag, at den kvadratiske talring $R = \mathbb{Z}[\xi]$ er faktoriel. Da vil hvert sædvanligt primtal p være af en af følgende tre typer:*

Type 1: *Primtallet p er irreducibelt i R.*

Type 2: *Primtallet p har i R en faktorisering $p = \pm\pi\pi'$, hvor π og det konjugerede element π' er primelementer, og π' ikke er associeret med π.*

Speciel type: *Primtallet p har i R en faktorisering $p = \pm\pi\pi'$, hvor π og det konjugerede element π' er primelementer, og π' er associeret med π.*

Yderligere gælder, at hvert primelement i R er associeret med et af de primelementer, der bestemmes ved at primopløse de sædvanlige primtal.

Bevis. Antag nemlig, at p ikke er af type 1, altså at p i R har en ikke-triviel divisor π. Da er $\mathrm{N}(\pi)$ en ikke-triviel divisor i $\mathrm{N}(p) = p^2$, og følgelig er $\mathrm{N}(\pi) = \pm p$. Altså er $p = \pm\pi\pi'$. Af (6.14) følger, at π og π' er irreducible i R, og da R er faktoriel, er de endda primelementer. Altså er p enten af type 2 eller af speciel type.

Typerne angiver primopløsningen i R af de sædvanlige primtal. Primtal af type 1 er selv primelementer, idet R er faktoriel, primtal af type 2 har en primopløsning med to faktorer π og π', og bestemmer to primelementer, og primtal p af speciel type har, pånær associering, en primopløsning som et kvadrat π^2, og bestemmer altså ét primelement i R. Ethvert element α, ikke 0 og ikke en enhed, er divisor i et helt tal større end 1, (idet α er divisor i $\alpha\alpha' = \mathrm{N}(\alpha)$), og dermed divisor i et produkt af sædvanlige primtal. Hvis α selv er et primelement i R, følger det først, at α er divisor i et sædvanligt primtal p, og dernæst, at α er associeret med et af de primelementer, der bestemmes ved at primopløse p. □

Inddelingen af primtallene i de 3 typer kaldes også primtallenes *forgrening* mht den givne (faktorielle) kvadratiske talring R.

(6.21) Forgrening i Gauss' talring. Vi har set i (6.16), at Gauss' talring $\mathbb{Z}[i]$ er et hovedideal-område, og dermed en faktoriel ring. Enhederne bestemmes ved at heltalsløse $x^2 + y^2 = 1$; det giver de 4 enheder $\{\pm 1, \pm i\}$. Vi vil her betragte forgreningen i $\mathbb{Z}[i]$.

Mht Gauss' talring $\mathbb{Z}[i]$ falder de sædvanlige primtal i følgende typer:
Type 1 er netop primtallene $q \equiv 3 \pmod 4$.
Type 2 er netop primtallene $p \equiv 1 \pmod 4$
Speciel type har kun primtallet 2 (med opløsningen $2 = (1+i)(1-i) = (-i)(1+i)^2$).

Bevis:. Primtallet $2 = (1 + i)(1 - i)$ er specielt, da $1 - i = (-i)(1 + i)$ er associeret med $1 + i$. Antag omvendt, at p er et specielt primtal. Så har vi i $\mathbb{Z}[i]$ en primopløsning $p = \pi\bar{\pi}$, hvor $\pi = x + iy$ og $\bar{\pi}$ er associeret med π, dvs $\bar{\pi} = \varepsilon\pi$ med $\varepsilon \in \{\pm 1, \pm i\}$. Med $\varepsilon = 1$ fås $\pi = \bar{\pi}$, hvoraf $\pi = x$ og $p = x^2$, og med $\varepsilon = -1$ fås tilsvarende $\pi = iy$ og $p = y^2$; begge dele er i modstrid med at p er et primtal. Med $\varepsilon = \pm i$ fås $\bar{\pi} = \pm i\pi$, hvoraf $y = \pm x$ og $p = 2x^2$; da p er et primtal, følger det, at $p = 2$.

Betragt dernæst et ulige primtal p. Hvis p er af type 2, så er $p = \pi\bar{\pi}$, og vi har en heltalsløsning til ligningen,

$$x^2 + y^2 = p.$$

Primtallet p var ulige. Af de to tal x, y må altså det ene være lige og det andet ulige. Modulo 4 er et lige kvadrat kongruent med 0 og et ulige kvadrat er kongruent med 1. Af ligningen følger derfor, at $p \equiv 1 \pmod 4$.

Antag omvendt, at $p \equiv 1 \pmod 4$. Det er velkendt, og let at vise, at kongruensen $z^2 + 1 \equiv 0 \pmod p$ da har løsninger. Det følger så af (6.19), at p ikke er irreducibelt i R, altså at p ikke kan være af type 1. Da p er ulige, kan p ikke være af Speciel type. Altså må p være af type 2.

Hermed er resultatet bevist. □

Euler's Sætning. *For hvert primtal $p \equiv 1 \pmod 4$ har ligningen,*

$$x^2 + y^2 = p,$$

heltalsløsninger (x, y).

Bevis. Et primtal $p \equiv 1 \pmod 4$ er af type 2 i $\mathbb{Z}[i]$; vi har altså $p = \pi\bar{\pi}$ med $\pi = x + iy$ i $\mathbb{Z}[i]$, og så er (x, y) en løsning. □

Løsninger for små værdier af p er lette at bestemme:

$$5 = 2^2 + 1^2,\ 13 = 3^2 + 2^2,\ 17 = 4^2 + 1^2,\ 29 = 5^2 + 2^2,\ 37 = 6^2 + 1^2,\ 41 = 5^2 + 4^2.$$

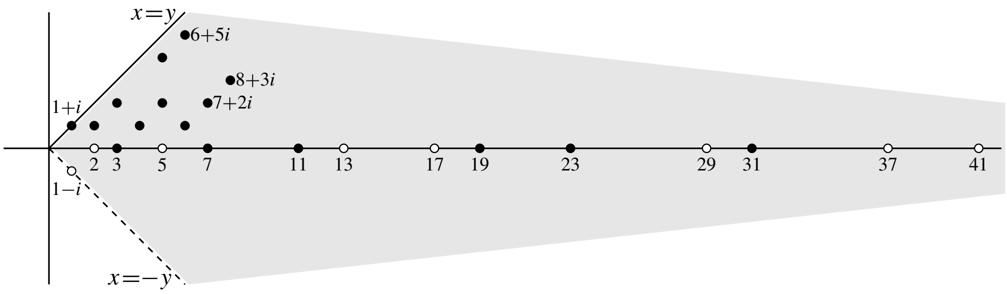
(6.22) Primelementer i Gauss' talring. For bedre at kunne udnytte primopløsninger i Gauss' talring $\mathbb{Z}[i]$ er det hensigtsmæssigt at fastlægge et repræsentantsystem for primelementerne. For hvert primelement π er de associerede tallene $\pi, i\pi, -\pi, -i\pi$. Da multiplikation med de 4 enheder $1, i, -1, -i$ svarer til drejninger med vinkler $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ [Bemærk, at der er to slags π'er i spil: et primelement og længden af en halvcirkel!], er hvert primelement associeret med netop ét primelement i området af komplekse tal med argument θ bestemt ved ulighederne,

$$-\frac{\pi}{4} < \theta \leqslant \frac{\pi}{4}.$$

Som repræsentantsystem $\mathcal{P}$ for primelementerne i $\mathbb{Z}[i]$ vælger vi primelementerne i dette område. Ifølge resultatet i (6.21) er primelementerne i $\mathcal{P}$ enten tallet $1+i$ (svarende til det specielle primtal 2, der har primopløsningen $2 = (-i)(1+i)^2$), eller de er sædvanlige primtal $q \equiv 3 \pmod 4$, eller de findes i par $\pi, \bar{\pi}$, hvor $\pi\bar{\pi} = p$ er et sædvanligt primtal $p \equiv 1 \pmod 4$.

Svarende til primtallene 2, 3, 5, 7, 11, 13, 17, ... får vi primelementerne i $\mathcal{P}$, ordnet efter voksende norm,

$$1+i,\ 2\pm i,\ 3,\ 3\pm 2i,\ 4\pm i,\ 5\pm 2i,\ 6\pm i,\ 5\pm 4i,\ 7,\ \ldots .$$



Der er kun afsat primelementer (markeret med sort) med ikke-negativ imaginærdel.

Hvert tal $\alpha \neq 0$ i $\mathbb{Z}[i]$ har da en entydig primopløsning af formen,

$$\alpha = \varepsilon(1+i)^{\lambda} q_1^{\nu_1}\cdots q_r^{\nu_r}\pi_1^{\mu_1'}\bar{\pi}_1^{\mu_1''}\cdots\pi_s^{\mu_s'}\bar{\pi}_s^{\mu_s''}, \tag{6.22.1}$$

hvor $\varepsilon \in \{1, i, -1, -i\}$ og primelementerne ligger i $\mathcal{P}$ (og specielt $q_i \equiv 3 \pmod 4$ og $\pi_j\bar{\pi}_j = p_j \equiv 1 \pmod 4$).

Normer i Gauss' talring. *Lad k være et naturligt tal med sædvanlig primopløsning,*

$$k = 2^l q_1^{n_1}\cdots q_r^{n_r} p_1^{m_1}\cdots p_s^{m_s}, \tag{6.22.2}$$

hvor $q_i \equiv 3 \pmod 4$ og $p_j \equiv 1 \pmod 4$. Ligningen,

$$x^2 + y^2 = k,$$

har da løsninger $(x, y) \in \mathbb{Z}\times\mathbb{Z}$, hvis og kun hvis eksponenterne $n_1, \ldots, n_r$ alle er lige. I bekræftende fald er antallet af løsninger bestemt som produktet,

$$4(m_1+1)\cdots(m_s+1).$$

Bevis. Løsninger $(x, y) \in \mathbb{Z}\times\mathbb{Z}$ til ligningen svarer til tal $\alpha = x + iy \in \mathbb{Z}[i]$ med $\mathrm{N}(\alpha) = k$. Tallet α er bestemt ved sin primopløsning (6.22.1); ved eventuelt at tilføje faktorer med eksponent 0 kan vi antage, at de indgående tal q_i og p_j i (6.22.1) og i (6.22.2) er de samme. Herefter er

$$\mathrm{N}(\alpha) = 2^{\lambda} q_1^{2\nu_1} \cdots q_r^{2\nu_r} p_1^{\mu_1' + \mu_1''} \cdots p_s^{\mu_s' + \mu_s''}.$$

Vi har altså $\mathrm{N}(\alpha) = k$, hvis og kun hvis eksponenterne i (6.22.1) opfylder ligningerne,

$$\lambda = l, \quad 2\nu_1 = n_1, \ldots, \; 2\nu_r = n_r, \quad \mu_1' + \mu_1'' = m_1, \ldots, \; \mu_s' + \mu_s'' = m_s.$$

Dette er naturligvis kun muligt, når eksponenterne n_i er lige. Hvis alle n_i er lige, kan vi løse ligningerne og frit vælge tallene μ_j' således, at $0 \leqslant \mu_j' \leqslant m_j$. Desuden har vi 4 mulige valg af enheden ε, altså i alt det anførte antal elementer α i $\mathbb{Z}[i]$, som opfylder ligningen $\mathrm{N}(\alpha) = k$. ▯

(6.23) Pytagoræiske talsæt. Det fremgår af beviset ovenfor, at vi eksplicit kan bestemme løsningerne til ligningen $x^2 + y^2 = k$ ud fra primopløsningen af tallet k i ringen $\mathbb{Z}[i]$. Og denne primopløsning fås ud fra den sædvanlige primopløsning ved at skrive hvert $p_j \equiv 1 \pmod 4$ på formen $p_j = \pi_j \bar{\pi}_j$, dvs ved at løse ligningerne $x_j^2 + y_j^2 = p_j$.

Som eksempel vil vi betragte *pytagoræiske talsæt*, dvs heltalsløsninger til ligningen,

$$x^2 + y^2 = z^2.$$

Vi vil kalde en løsning *primitiv*, hvis tallene x og y er primiske. Trivielt er $(0, 0, 0)$ en løsning. Enhver anden løsning fås fra en primitiv løsning: er (x, y, z) en løsning og er d den største fælles divisor for x, y, så er d også divisor i z, og vi har derfor $(x, y, z) = (dx', dy', dz')$, hvor (x', y', z') er en primitiv løsning. To løsninger er *essentielt ens*, hvis man kan komme fra den ene til den anden ved at skifte fortegn på nogle af tallene x, y, z eller ved at ombytte x og y.

Sætning om Pytagoræiske tal. *For et naturligt tal $k > 1$ med primopløsningen,*

$$k = p_1^{m_1} \cdots p_s^{m_s},$$

(hvor $m_j \geqslant 1$ for $j = 1, \ldots, s$) gælder, at den diofantiske ligning,

$$x^2 + y^2 = k^2,$$

har primitive løsninger, hvis og kun hvis $p_j \equiv 1 \pmod 4$ for $j = 1, \ldots, s$. Er dette opfyldt, har ligningen præcis 2^{s-1} essentielt forskellige, primitive løsninger (x, y).

Bevis. Skriv primopløsningen af k på formen i (6.22.2),

$$k = 2^l q_1^{n_1} \cdots q_r^{n_r} p_1^{m_1} \cdots p_s^{m_s}.$$

Vi skal vise, at ligningen har primitive løsninger, hvis og kun hvis

$$l = 0, \; n_1 = 0, \ldots, \; n_r = 0.$$

Af primopløsningen af k får vi, at

$$k^2 = 2^{2l} q_1^{2n_1} \cdots q_r^{2n_r} p_1^{2m_1} \cdots p_s^{2m_s} .$$

Det følger, at ligningen $x^2 + y^2 = k^2$ altid har løsninger, svarende til elementer $\alpha = x + yi$ i $\mathbb{Z}[i]$ med primopløsningen

$$\alpha = \varepsilon(1+i)^{2l} q_1^{n_1} \cdots q_r^{n_r} \pi_1^{\mu_1'} \bar{\pi}_1^{\mu_1''} \cdots \pi_s^{\mu_s'} \bar{\pi}_s^{\mu_s''}, \quad \text{hvor } \mu_j' + \mu_j'' = 2m_j.$$

For et naturligt tal $d > 1$ har vi, at d er divisor i både x og y, hvis og kun hvis d er divisor i $\alpha = x + iy$. Det sidste kan vi afgøre ud fra ovenstående primopløsning af α, og vi ser, at $\alpha = x + yi$ giver en primitiv løsning (x, y), netop når,

$$l = 0,\ n_1 = 0,\ \ldots,\ n_r = 0, \quad \text{og for hvert } j \text{ er enten } \mu_j' = 0 \text{ eller } \mu_j'' = 0.$$

Der er således primitive løsninger, hvis og kun hvis k har den angivne form. Er dette tilfældet, har vi for hvert j to mulige valg, og dermed $4 \cdot 2^s$ primitive løsninger. De primitive løsninger kommer i grupper på 8 essentielt ens løsninger (nemlig med α også $i\alpha$, $-\alpha$, $-i\alpha$ og de 4 konjugerede, som er 8 forskellige løsninger). Antallet af essentielt forskellige blandt de primitive løsninger er altså $\frac{1}{8} \cdot 4 \cdot 2^s = 2^{s-1}$. ▯

Eksempel. Bemærk, at vi også her får beskrevet løsningerne til $x^2 + y^2 = k^2$ ved at løse ligningerne $x_j^2 + y_j^2 = p_j$ for $j = 1, \ldots, s$. For eksempel har vi $5^2 + 2^2 = 29$; af

$$(5 + 2i)^2 = 21 + 20i,$$

følger derfor, at $20^2 + 21^2 = 29^2$.

For $k = 65 = 5 \cdot 13$ er der to løsninger. Vi har $5 = \mathrm{N}(2 + i)$ og $13 = \mathrm{N}(3 + 2i)$. Af udregningerne,

$$(2+i)^2(3+2i)^2 = (3+4i)(5+12i) = -33 + 56i,$$
$$(2+i)^2(3-2i)^2 = (3+4i)(5-12i) = 63 - 16i,$$

får vi løsningerne,

$$33^2 + 56^2 = 16^2 + 63^2 = 65^2.$$

(6.24) Bemærkning. For en given kvadratisk talring $R = \mathbb{Z}[\xi]$ er det fundamentalt at kunne afgøre, om et givet element $\pi = x + y\xi$ er et primelement eller et irreducibelt element. Spørgsmålet er delvis behandlet i (6.14) og (6.19). Her forstærker vi resultaterne.

Sætning 0. *Hvis tallet $\pi = x + y\xi \in R$ er irreducibelt i R, så er enten tallene x, y primiske eller π er associeret med et sædvanligt primtal p.*

Bevis. Lad d være den største fælles divisor for x, y. Så er $x = du$ og $y = dv$ med primiske hele tal u, v, og vi har faktoriseringen $\pi = d(u + v\xi)$. Hvis $d = 1$, har vi det første tilfælde. Antag derfor, at $d > 1$. Da kan d yderligere skrives som et produkt af sædvanlige primtal. Hvis π er irreducibel i R, må faktoriseringen være triviel: Altså må $d = p$ være et primtal, og faktoren $u + v\xi$ må være en enhed; det er det andet tilfælde. ▯

Sætning 1. *Tallet* $\pi := x + y\xi \in R$ *med primiske* x, y *er et primelement i* R, *hvis og kun hvis* $\mathrm{N}(\pi) = \pm p$, *hvor* p *er et primtal.*

Bevis. „hvis“: I beviset bruges, for et naturligt tal n, at kvotientringen $R/(n)$ er en endelig ring med n^2 elementer. Hertil bemærkes, at hovedidealet (n) i R består af alle tal $ns + nt\xi$, altså af alle tal $u + v\xi \in R$, hvor u og v er delelige med n. Modulo (n) er hvert element $u + v\xi \in R$ altså kongruent med ét af de n^2 elementer af formen $q + r\xi$, hvor $0 \leqslant q, r \leqslant n - 1$. Derfor er der n^2 ækvivalensklasser.

Antag nu for et primtal p, at $\mathrm{N}(\pi) = \pm p$, altså $p = \pm\pi\pi'$. Specielt er π så en ikke-triviel divisor i p, og derfor er $(p) \subset (\pi) \subset R$. Nu var $|R/(p)| = p^2$, og af inklusionerne følger, at ordenen af $R/(\pi)$ er en ikke-triviel divisor i ordenen af $R/(p)$. Altså er $|R/(\pi)| = p$. Af Sætning (1.14) følger så, at $R/(\pi)$ et legeme, og specielt et integritetsområde. Altså er (π) et primideal, og derfor er π et primelement.

„kun hvis“: det er implikationen (i)⇒(ii) fra Lemma (6.14). □

Sætning 2. *For et sædvanligt primtal* p *gælder:* p *er et primelement i* R, *hvis og kun hvis kongruensen,*

$$z^2 - bz + c \equiv 0 \pmod{p}, \tag{6.24.1}$$

ikke har løsninger $z \in \mathbb{Z}$.

Bevis. „kun hvis“: det er implikationen (iii)⇒(iv) fra Sætning (6.19).

„hvis“: Antag, at kongruensen ikke har løsninger. Det skal vises, at p er et primelement i R. Hertil betragtes i R en ligning $p\delta = \alpha\beta$. Det skal vises, at p er divisor i α eller i β. Af ligningen følger, at $\mathrm{N}(p) = p^2$ går op i produktet $\mathrm{N}(\alpha)\,\mathrm{N}(\beta)$. Da p er et primtal, følger det, at p går op i en af faktorerne; vi kan antage, at p går op i $\mathrm{N}(\alpha)$. Er $\alpha = x + y\xi$, har vi altså kongruensen $\mathrm{N}(\alpha) \equiv 0 \pmod{p}$, dvs,

$$x^2 - bxy + cy^2 \equiv 0 \pmod{p}. \tag{6.24.2}$$

Hvis p ikke går op i y, vil restklassen af y^2 modulo p være invertibel, og multiplikation af (6.24.2) med den inverse restklasse vil give en løsning til kongruensen (6.24.1); det er i modstrid med antagelsen. Derfor går p op i y. Af kongruensen (6.24.2) følger så, at p går op i x^2, og dermed i x. Altså går p op i $\alpha = x + y\xi$. □

Bemærk, at Sætning (6.19) indholder en karakterisering af, hvornår et sædvanligt primtal p er irreducibelt i R. Bemærk også, for et element π af formen i Sætning 1, at der ikke er nogen tilsvarende karakterisering af, hvornår π er irreducibelt i R.

(6.25) Opgaver.

1. Vis ved et eksempel, at i en kvadratisk talring kan to elementer godt have samme norm uden at være associerede.

2. Bestem en enhed $\varepsilon \neq \pm 1$ i ringen $\mathbb{Z}[\sqrt{7}]$.

3. Hvilke af tallene $4 + 3i$, $5 + 2i$ og $2 - 5i$ i $\mathbb{Z}[i]$ går op i $7 + 26i$?

4. Hvilke af tallene $3 \pm \sqrt{7}$ i ringen $\mathbb{Z}[\sqrt{7}]$ er divisorer i $15 - 7\sqrt{7}$?

5. Vis, at tallet 2 er reducibelt i ringen $\mathbb{Z}[\sqrt{7}]$.

6. Bestem $b, c \in \mathbb{Z}$ således, at $\xi = (-1 + \sqrt{17})/2$ er rod i $X^2 + bX + c$. Vis, at 5 er et primelement i $\mathbb{Z}[\xi]$.

7. Lad $R = \mathbb{Z}[\xi]$ være en kvadratisk talring. Vis, at tallene af formen $\lambda + \mu\xi$, hvor $\lambda, \mu \in \mathbb{Q}$, udgør brøklegemet for R.

8. Find en ikke-triviel løsning til den diofantiske ligning $x^2 - 31y^2 = 1$. [Vink: tallene er ikke helt små.]

9. Lad ζ være en 3'die enhedsrod, altså rod i polynomiet X^2+X+1. Vis, at den kvadratiske talring $\mathbb{Z}[\zeta]$ er et hovedidealområde.

10. Vis, at den kvadratiske talring $\mathbb{Z}[\tau]$, hvor $\tau = (1+\sqrt{5})/2$ er rod i X^2-X-1, er et PID.

11. Bestem i Gauss' talring $\mathbb{Z}[i]$ primopløsningen af $9+32i$.

12. Lad R og R_0 være kvadratiske talringe med diskriminanter D og D_0. Vis, at $R \subseteq R_0$, hvis og kun hvis $D = y^2 D_0$ med et helt tal y.

13. Løs ligningen $x^2+y^2 = 25^2$.

14. *Vis, at hvis den kvadratiske talring $R = \mathbb{Z}[\xi]$ er et UFD, så er diskriminanten D en *kvadratfri diskriminant* i den forstand, at D ikke kan skrives som et produkt $D = y^2 D_0$, hvor $y \geqslant 2$ og $D_0 \equiv 0, 1 \pmod 4$. [Vink: vis, (og brug) for α og δ i R, at hvis α/δ er et kvadratisk tal, så går δ op i α.]

15. *Lad R være en kvadratisk talring, og lad $n \geqslant 1$ være et naturligt tal. Vis, at R/Rn er en endelig ring med n^2 elementer. Lad $\mathfrak{a} \neq (0)$ være et ideal i R. Vis, at der findes et naturligt tal n i $\mathfrak{a}$. Vis, at $R/\mathfrak{a}$ er en endelig ring. Vis, at $\mathfrak{a}$ er et maksimalideal, hvis og kun hvis $\mathfrak{a}$ er et primideal.

16. *Vis, at en kvadratisk talring $R = \mathbb{Z}[\xi]$ er et PID, hvis (og kun hvis) den er et UFD. [Vink: Antag, at R er et UFD. Vis først, at maksimalidealerne i R er hovedidealerne $R\pi$ frembragt af primelementer π. Slut heraf, når $\mathfrak{a}$ er et ikke-trivielt ideal, at der findes et primelement π således, at $\mathfrak{a} \subseteq R\pi$.]

17. Betragt reelle løsninger (x, y) til ligningen $ax^2 - bxy + cy^2 = k$, hvor a, b, c, k er givne relle tal og $a > 0$. Sæt $D := b^2 - 4ac$. Vis, at når $D < 0$, så er løsningsmængden (afhængigt af k) enten $\emptyset$, en ellipse, eller punktet $(0, 0)$. Diskuter tilsvarende tilfældene $D = 0$ og $D > 0$. [Vink: ligningen er ækvivalent med ligningen $(2ax - by)^2 - Dy^2 = 4ak$.]

18. Lad p være et ulige primtal. Vis for hele tal b, c og $D := b^2 - 4c$, at kongruensen $z^2 - bz + c \equiv 0 \pmod p$ har løsninger, hvis og kun hvis kongruensen $x^2 \equiv D \pmod p$ har løsninger.

19. Lad ξ være et (irrationalt) kvadratisk tal med diskriminant D. Vis, for et ulige primtal p, at p er et primelement i $\mathbb{Z}[\xi]$, hvis og kun hvis D modulo p ikke er et kvadrat.

20. Afgør om den diofantiske ligning $x^2 + xy - y^2 = 17$ har løsninger.

21. *Lad $R = \mathbb{Z}[\xi]$ være en kvadratisk talring med diskriminant D. Vis, at R er euklidisk for $D = -3, -4, -7, -8, -11$. Vis, at R er euklidisk for $D = 5, 13$. Vis, at R er euklidisk for $D = 17$.

22. *Et berømt resultat af Lagrange udsiger, at ethvert naturligt tal er en sum af 4 ikke-negative kvadrater; her må nogle af kvadraterne altså være 0. Angiv eksplicit en funktion $f\colon \{5, 6, 7, \ldots\} \to \mathbb{N}$ således, at der for ethvert $k \geqslant 5$ gælder: Hvis $n \geqslant f(k)$, så er n en sum af k positive kvadrater.

23. Der gælder $3^2+4^2 = 5^2$ og $10^2+11^2+12^2 = 13^2+14^2$, og $21^2+22^2+23^2+24^2 = 25^2+26^2+27^2$. Ser du systemet? [Vink: Løs for et givet helt tal $n \geqslant 1$ ligningen herunder.]

$$\overbrace{x^2 + (x+1)^2 + \cdots + (x+n)^2}^{n+1 \text{ kvadrater}} = \overbrace{(x+n+1)^2 + \cdots + (x+2n)^2}^{n \text{ kvadrater}}.$$

Polynomier

Overalt i det følgende betegner R en *kommutativ* ring.

1. Polynomiumsringen.

(1.1) Definition. Ved et *polynomium* med koefficienter i R forstås en følge $f = (f_0, f_1, \dots)$ af elementer $f_i \in R$ således, at kun endelig mange f_i er forskellige fra nul-elementet 0 i R. Elementet f_i kaldes den i'te *koefficient* i f. Det antages altså, at der findes et tal n således, at $f_i = 0$ når $i > n$.

Et polynomium f vil vi oftest angive ved et formelt udtryk af formen,

$$f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n, \tag{1.1.1}$$

hvor $a_0, \dots, a_n$ er elementer i R. I sådanne udtryk er symbolet X^i – i hvert fald a priori – alene en „pladsholder“, der fortæller, at det element i R, der står foran X^i, er den i'te koefficient i f, og plus-tegnene tjener kun til at adskille de enkelte led. Ligningen (1.1.1) udtrykker altså, at den i'te koefficient i f er lig med a_i for $i = 0, \dots, n$ og lig med 0 for $i > n$. Med andre ord bestemmer ligningen (1.1.1) polynomiet $f = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots)$. Da X^i blot er en pladsholder, er rækkefølgen af leddene i udtrykket (1.1.1) underordnet.

Leddet a_iX^i i udtrykket kaldes polynomiets *led* af grad i. Leddet af grad 0, der er koefficienten a_0, kaldes også polynomiets *konstantled*. Oftest udelader man i udtrykket led a_iX^i, hvor koefficienten a_i er nul-elementet i R, altså led af formen $0X^i$. Led af formen a_iX^i hvor a_i er et-elementet $1 \in R$, altså $1X^i$, skrives blot X^i. Med denne konvention er symbolet X selv et polynomium, nemlig følgen $(0, 1, 0, 0, 0, \dots)$.

Et polynomium f kaldes *konstant*, hvis koefficienterne f_i er nul for $i > 0$, altså hvis f har formen $f = (a, 0, 0, 0, \dots)$ med a i R. Specielt er *nul-polynomiet* det konstante polynomium $(0, 0, 0, \dots)$. Det betegnes blot 0.

For et polynomium f, som ikke er nul-polynomiet, findes der tal $i \geqslant 0$ således, at koefficienten f_i er forskellig fra 0. Det største sådanne tal i kaldes *graden* af polynomiet f, og den tilhørende koefficient f_i kaldes den *ledende koefficient* i f. De mulige grader af polynomier $f \neq 0$ er tallene $0, 1, 2, \dots$. Det er en konvention (som vi vil følge), at tillægge nul-polynomiet graden $-\infty$. Specielt er altså graden af nul-polynomiet mindre end graden af ethvert polynomium $f \neq 0$. Graden af et polynomium f betegnes også $\deg(f)$. At et polynomium f har grad mindre end eller lig med n betyder, at det kan fremstilles ved et udtryk af formen (1.1.1). Polynomiet f bestemt ved (1.1.1) har graden n, netop når $a_n \neq 0$; i så fald er a_n den ledende koefficient i f.

Et polynomium f kaldes *normeret*, hvis $f \neq 0$ og den ledende koefficient i f er et-elementet 1 i R.

Mængden af polynomier med koefficienter i R betegnes $R[X]$. For at understrege, at et givet symbol f betegner et polynomium, kan man skrive $f(X)$ i stedet for f.

(1.2) Eksempel. Udtrykkene herunder definerer reelle polynomier,

$$f = 2X^3 - 3X^2 + 1, \quad g = 1 + X + \cdots + X^{n-1}, \quad h = \sum_{j=0}^{m} \binom{m}{j} X^j,$$

altså polynomier i $\mathbb{R}[X]$. Opfattet som følge er $f = (1, 0, -3, 2, 0, 0, 0, \dots)$. Graden er 3, konstantleddet er 1, og den ledende koefficient er 2; specielt er f ikke normeret. Tilsvarende er $g = (1, 1, \dots, 1, 0, 0, \dots)$ (med n et-taller), og g er et normeret polynomium af grad $n - 1$. For polynomiet h har vi $h_i = \binom{m}{i}$ med den sædvanlige konvention, at $\binom{m}{i} = 0$ for $i > m$, og h er et normeret polynomium af grad m.

De tre polynomier ovenfor har hele koefficienter. De kan derfor også opfattes som polynomier i $\mathbb{Z}[X]$ eller i $\mathbb{Q}[X]$ eller i $\mathbb{C}[X]$.

(1.3) Eksempel. Det er en pointe i definitionen, at enhver kommutativ ring kan indgå som ring af koefficienter for polynomier. Fx er restklasseringen $\mathbb{F}_p = \mathbb{Z}/p$ for et primtal p et legeme med p elementer, og polynomiet,

$$f = X^{p-1} - 1,$$

kan opfattes som polynomium i $\mathbb{F}_p[X]$. Det er et normeret polynomium.

De trigonometriske funktioner $\sin t$ og $\cos t$ er elementer i ringen $R := \mathcal{C}(\mathbb{R})$ af kontinuerte funktioner på $\mathbb{R}$. Følgelig kan

$$g = 1 - \sin^2 t \, X, \qquad \text{og} \qquad h = 1 + \cos^2 t \, X$$

opfattes som polynomier i $\mathcal{C}(\mathbb{R})[X]$. De har begge grad 1, og de er ikke normerede.

(1.4) Note. I forbindelse med funktioner er vi vant til at opfatte udtryk som for eksempel $2t^3 - 3t^2 + 1$ eller $1 + z + z^2 + z^3$ eller $1 + 2x + x^2$ som polynomier. Det skal understreges, at når vi i analysen betragter $2t^3 - 3t^2 + 1$ som et polynomium, så er t ikke et *bestemt* reelt tal. Det er underforstået, at udtrykket $2t^3 - 3t^2 + 1$ definerer en *funktion*, nemlig afbildningen,

$$t \mapsto 2t^3 - 3t^2 + 1;$$

det skal endda af sammenhængen fremgå, om vi tænker på funktionen som en reel funktion defineret for $t \in \mathbb{R}$, eller som en kompleks funktion defineret for $t \in \mathbb{C}$. Det er velkendt, at koefficienterne i en sådan polynomiumsfunktion er entydigt bestemt ved funktionen.

Den abstrakte definition af et polynomium i (1.1) er den ultimative konsekvens af denne observation: algebraisk defineres et polynomium som værende følgen af koefficienter. Symbolet X som betegnelse for pladsholderen er valgt for at fremhæve det algebraiske synspunkt, men der er intet i vejen for at vælge et andet symbol, og for eksempel bruge $R[t]$ som betegnelse for mængden af polynomier, hvorved det underforstås, at t er symbolet for pladsholderen.

(1.5) Sum og produkt. For to polynomier $f = (f_0, f_1, \dots)$ og $g = (g_0, g_1, \dots)$ i $R[X]$ defineres sum $s = f + g$ og produkt $p = fg$ som følgerne $s = (s_0, s_1, \dots)$ og $p = (p_0, p_1, \dots)$ bestemt ved ligningerne,

$$s_i = f_i + g_i, \qquad p_i = \sum_{j+k=i} f_j g_k,$$

hvor summen er over ikke-negative hele tal j, k. Hvis i er større end både $\deg(f)$ og $\deg(g)$, så er $f_i = g_i = 0$, og følgelig er $s_i = 0$. Hvis i er større end $\deg(f) + \deg(g)$ og $j + k = i$, så er enten $j > \deg(f)$ eller $k > \deg(g)$, og følgelig er $f_j g_k = 0$. Altså er $p_i = 0$ for $i > \deg(f) + \deg(g)$. Det ses altså, at begge følgerne s og p er polynomier.

Antag, at polynomierne f og g er givet ved udtryk af formen i (1.1),

$$f = a_0 + a_1 X + \dots + a_n X^n, \qquad g = b_0 + b_1 X + \dots + b_m X^m.$$

Det ses at summen $f + g$ fås ved at opfatte de to udtryk som summer og samle $a_i X^i + b_i X^i$ til leddet $s_i X^i$. Antages fx at $n \leqslant m$ fås udtrykket,

$$f + g = (a_0 + b_0) + (a_1 + b_1)X + \dots + (a_n + b_n)X^n + b_{n+1}X^{n+1} + \dots + b_m X^m,$$

hvor den sidste del falder væk hvis $m = n$. Tilsvarende fås produktet fg ved at opfatte de to udtryk som summer og gange dem sammen ved brug af den distributive lov, og så samle alle produkter $a_j b_k X^j X^k = a_j b_k X^{j+k}$, hvor $j + k = i$, til leddet $p_i X^i$. Vi får altså udtrykket,

$$fg = a_0 b_0 + (a_0 b_1 + a_1 b_0)X + (a_0 b_2 + a_1 b_1 + a_2 b_0)X^2 + \dots + a_n b_m X^{n+m}.$$

Det er let at vise, at med de to kompositioner er $R[X]$ en kommutativ ring og de konstante polynomier udgør en delring, som kan identificeres med den givne ring R. Nul-elementet i $R[X]$ er nul-polynomiet, dvs det konstante polynomium 0, og et-elementet er det konstante polynomium 1. Ringen $R[X]$ kaldes også *polynomiumsringen* i den ene *variabel* X.

(1.6) Eksempel. Som nævnt i (1.5) bestemmes sum og produkt af polynomier i $R[X]$ alene ved brug af regnereglerne i en kommutativ ring, herunder at $X^k X^l = X^{k+l}$. Fx finder vi for polynomiet f i Eksempel (1.2) faktoriseringen,

$$2X^3 - 3X^2 + 1 = (X^2 - 2X + 1)(2X + 1).$$

Polynomiet g indgår i ligningen,

$$(1 + X + \dots + X^{n-1})(X - 1) = X^n - 1.$$

Og for polynomiet h finder vi, ved binomialformlen,

$$(1 + X)^m = \sum \binom{m}{i} X^i.$$

I eksempel (1.3), for $p = 7$, finder vi i $\mathbb{F}_7[X]$ ligningen,

$$X^6 - 1 = (X^3 + 5X^2 + 6X + 2)(X^3 + 2X^2 + 5X + 3).$$

Endelig får vi i $\mathcal{C}(\mathbb{R})[X]$, ved hjælp af velkendte trigonometriske formler, ligningen,

$$(1 + \cos^2 t\, X)(1 - \sin^2 t\, X) = 1 + \cos 2t\, X - \tfrac{1}{4}\sin^2 2t\, X^2.$$

(1.7) Observation. Af de fundne udtryk for sum og produkt i (1.5) fremgår umiddelbart, at vi for polynomier $f, g \in R[X]$ har ulighederne,

$$\deg(f + g) \le \max\{\deg(f), \deg(g)\}, \tag{1}$$
$$\deg(fg) \le \deg(f) + \deg(g). \tag{2}$$

I uligheden (1) gælder lighed, når polynomierne f og g har forskellig grad. Har f og g samme grad, gælder den skarpe ulighed i (1) netop, når de ledende koefficienter i f og g er modsatte.

I uligheden (2) gælder lighed netop, når produktet af de ledende koefficienter er forskelligt fra 0. Specielt fremhæves, at lighed gælder i (2), når et af polynomierne er normeret. For integritetsområder får vi efterfølgende resultat.

(1.8) Sætning. *Antag, at R er et integritetsområde. Da gælder for alle polynomier f, g i $R[X]$ ligningen,*

$$\deg(fg) = \deg(f) + \deg(g). \tag{1.8.1}$$

Polynomiumsringen $R[X]$ er også et integritetsområde, og de invertible polynomier er netop de konstanter, der er invertible i ringen R.

Bevis. Ligningen (1.8.1) følger af observationen i (1.7). Ligningen er indholdsløs, hvis f eller g er nul-polynomiet, idet ligningens to sider så er $-\infty$. Hvis både f og g er forskellige fra 0, så følger det af ligningen, at $fg \neq 0$. Altså gælder nul-reglen i $R[X]$. Yderligere er $1 \neq 0$ i R og dermed $1 \neq 0$ i $R[X]$. Altså er $R[X]$ et integritetsområde.

Det er klart, at det konstante polynomium svarende til et invertibelt element a i R er invertibelt i $R[X]$ med det konstante polynomium a^{-1} som invers. Antag omvendt, at f er et invertibelt polynomium, altså at der findes et polynomium g således, at $fg = 1$. Konstanten 1 har grad 0. Det følger derfor af ligningen (1.8.1), at $\deg(f) = 0$ og $\deg(g) = 0$. Altså er f en konstant, og invertibel med konstanten g som den inverse. □

(1.9) Eksempel. Ringen $\mathbb{Z}[X]$ af polynomier med heltalskoefficienter er et integritetsområde. De invertible polynomier i $\mathbb{Z}[X]$ er konstanterne ± 1.

Ringen $\mathbb{Q}[X]$ af polynomier med rationale koefficienter er et integritetsområde. De invertible polynomier er konstanterne forskellige fra 0 i $\mathbb{Q}$.

Tilsvarende gælder, at polynomierne med koefficienter i et *legeme* L udgør et integritetsområde $L[X]$, og de invertible polynomier er netop konstanterne forskellige fra 0. Specielt er polynomiumsringene $\mathbb{R}[X]$ og $\mathbb{C}[X]$ og $\mathbb{F}_p[X]$ (for et primtal p) integritetsområder.

Restklasseringen $\mathbb{Z}/4$ er ikke et integritetsområde, idet der modulo 4 gælder, at $2^2 = 0$. Øjensynlig har vi i $(\mathbb{Z}/4)[X]$ ligningen,

$$(1 + 2X)^2 = 1.$$

Førstegradspolynomiet $1 + 2X$ er derfor invertibelt i $(\mathbb{Z}/4)[X]$ (med sig selv som det inverse polynomium).

(1.10) Note. Hvis ringen R er en delring af en kommutativ ring S, kan polynomier med koefficienter i R opfattes som polynomier med koefficienter i S. Det er klart, at $R[X]$ er en delring af $S[X]$.

For eksempler har vi inklusioner af delringe,

$$\mathbb{Z}[X] \subseteq \mathbb{Q}[X] \subseteq \mathbb{R}[X] \subseteq \mathbb{C}[X].$$

Antag mere generelt, at der er givet en ringhomomorfi $\varphi\colon R \to S$ fra R til en kommutativ ring S, dvs en afbildning φ, der er additiv og multiplikativ og afbilder 1_R i 1_S. For hvert polynomium f i $R[X]$ betegnes med $\varphi(f)$ det polynomium i $S[X]$, der fremgår af f ved at erstatte koefficienterne med deres billeder ved φ. For $f = a_n X^n + \cdots + a_1 X + a_0$ i $R[X]$ defineres altså $\varphi(f)$ i $S[X]$ ved ligningen,

$$\varphi(f) = \varphi(a_n)X^n + \cdots + \varphi(a_1)X + \varphi(a_0).$$

På de konstante polynomier er $f \mapsto \varphi(f)$ blot den givne afbildning $\varphi\colon R \to S$. Det er klart, at afbildningen $f \mapsto \varphi(f)$ er en ringhomomorfi $R[X] \to S[X]$, altså at den ligeledes er additiv og multiplikativ og afbilder 1 i 1. Den siges at være *induceret* af φ.

For eksempel kan vi, for et givet naturligt tal d, lade φ være den kanoniske homomorfi $\mathbb{Z} \to \mathbb{Z}/d$, der til et helt tal a lader svare restklassen $\bar{a}$ af a modulo d. Den inducerede homomorfi $\mathbb{Z}[X] \to (\mathbb{Z}/d)[X]$ afbilder et polynomium f med hele koefficienter på det polynomium $\bar{f}$ i $(\mathbb{Z}/d)[X]$, der fremkommer ved at erstatte koefficienterne i f med deres restklasser modulo d. Øjensynlig gælder, at $\bar{f}$ er nul-polynomiet i $(\mathbb{Z}/d)[X]$ netop når alle koefficienter i f er delelige med d.

(1.11) Bemærkning. Polynomierne behandlet i det foregående er polynomier i én variabel X. Ganske tilsvarende kan man definere og regne med polynomier i flere variable. For eksempel er udtrykket,

$$f = 1 + 3X - 5Y + X^2 - 2Y^2 + X^4 + 2X^3Y - 2X^2Y^2 + 2XY^5 - 4X^3Y^3,$$

et polynomium i to variable X, Y med koefficienter i $\mathbb{Z}$. Man regner med sådanne udtryk ligesom med polynomier i én variabel ved at bruge, at produktet af X^iY^j og X^kY^l er $X^{i+k}Y^{j+l}$. Polynomier i to variable med koefficienter i R udgør en kommutativ ring, betegnet $R[X, Y]$. I et polynomium i to variable kan leddene ordnes efter potenser af Y. Fx fremkommer for polynomiet ovenfor udtrykket,

$$f = (1 + 3X + X^2 + X^4) + (-5 + 2X^3)Y + (-2 - 2X^2)Y^2 - 4X^3Y^3 + 2XY^5.$$

I almindelighed fremkommer som koefficient til Y^i et polynomium i X, altså en koefficient i ringen $R[X]$. Polynomiumsringen $R[X, Y]$ kan herved opfattes som polynomiumsringen i én variabel Y med koefficienter i ringen $R[X]$. Vi har med andre ord ligheden,

$$R[X, Y] = R[X][Y].$$

Alternativt kan vi ordne efter potenser af X,

$$f = (1 - 5Y - 2Y^2) + (3 + 2Y^5)X + (1 - 2Y^2)X^2 + (2Y - 4Y^3)X^3 + X^4;$$

i almindelighed har vi ligheden $R[X, Y] = R[Y][X]$.

Mere generelt kan vi definere ringen $R[X_1, \dots, X_r]$ af polynomier i r variable enten tilsvarende, eller induktivt ved ligningen,

$$R[X_1, \dots, X_r] = R[X_1, \dots, X_{r-1}][X_r].$$

(1.12) Opgaver.

1. Bestem, i $\mathbb{C}[X]$, produktet $(X-1)(X-i)(X+1)(X+i)$.

2. Bestem, i $\mathbb{F}_2[X]$, kvadratet $(X^3 + X^2 + X + 1)^2$.

3. Bestem, i $(\mathbb{Z}/4)[X]$ sum og produkt af polynomierne $X^2 - 2X - 3$ og $X^3 + 2X^2 + 3X - 1$.

4. Hvordan bestemmes primringen i $R[X]$?

5. Bestem produktet $(X-1)(X-2)(X-3)(X-4)$ i ringen $(\mathbb{Z}/5)[X]$.

6. Vis, at polynomierne af grad højst n i $\mathbb{R}[X]$ på naturlig måde udgør et reelt vektorrum. Hvilken dimension har dette vektorrum? Angiv en basis.

7. Hvor mange polynomier af grad 3 findes i $\mathbb{F}_3[X]$. Hvor mange polynomier i $\mathbb{F}_p[X]$ har grad højst n.

8. Vis, at polynomiumsringen $R[X]$ har samme karakteristik som R.

9. Kan en polynomiumsring $R[X]$ være et legeme?

10. Vis, at mængden af *alle* følger $(f_0, f_1, \dots)$, hvor $f_i \in R$, med sum og produkt defineret som for polynomier, udgør en ring. Den kaldes ringen af formelle *potensrækker*, og betegnes $R[[X]]$. Følgen $f = (f_0, f_1, \dots)$ skrives også

$$f = f_0 + f_1X + f_2X^2 + \cdots,$$

idet X^i opfattes som en pladsholder, der fortæller, at koefficienten foran er følgens i'te element. Bestem, i $R[[X]]$, produktet af potensrækken $1 + X + X^2 + \cdots$ og polynomiet $1 - X$.

11. *Vis, at en potensrække $f_0 + f_1X + f_2X^2 + \cdots$ i $R[[X]]$ er invertibel, hvis og kun hvis konstantleddet f_0 er invertibelt i R.

12. Vis, at når R er et integritetsområde, så er også polynomiumsringen $R[X_1, \dots, X_r]$ et integritetsområde.

2. Division af polynomier.

(2.1) Sætning om division med rest. *Lad der være givet et normeret polynomium d i $R[X]$. Til hvert polynomium $f \in R[X]$ findes da entydigt bestemte polynomier $q, r \in R[X]$ således, at*

$$f = qd + r \quad \text{og} \quad \deg(r) < \deg(d)$$

[hvor uligheden mellem graderne omfatter muligheden, at r kan være nul-polynomiet].

Bevis. Lad n være graden af polynomiet d, altså $d = X^n + \cdots$, hvor de tre prikker står for en sum af led af grad mindre end n.

Eksistensen af fremstillingen vises ved fuldstændig induktion efter graden af f. Hvis polynomiet f har grad mindre end n (specielt hvis $f = 0$), har vi fremstillingen $f = 0d + f$, som er den ønskede fremstilling med $q := 0$ og $r := f$.

Antag derfor, at f har grad $m \geqslant n$. Hvis a er den ledende koefficient i f, har vi $f = aX^m + \cdots$. Da d er normeret, har polynomiet $aX^{m-n}d$ samme grad som f og samme ledende koefficient. Differensen $f - aX^{m-n}d$ har derfor mindre grad end f. Induktivt kan vi derfor antage, at differensen har en fremstilling af den ønskede form,

$$f - aX^{m-n}d = \tilde{q}d + r, \quad \deg(r) < \deg(d).$$

Heraf fås så den ønskede fremstilling af f,

$$f = (aX^{m-n} + \tilde{q})d + r.$$

For at vise entydigheden antages, at f har endnu en fremstilling $f = \hat{q}d + \hat{r}$, hvor $\deg \hat{r} < \deg d$. Det følger, at vi så har en ligning i $R[X]$,

$$(q - \hat{q})d = \hat{r} - r.$$

På højresiden har r og $\hat{r}$ begge grad mindre end graden n af polynomiet d. Altså har højresiden grad mindre end n. På venstresiden er faktoren d normeret af grad n. Som observeret i (1.7) følger det derfor, at enten har produktet på venstresiden grad mindst n eller også er faktoren $q - \hat{q}$ lig med 0. Det første er udelukket. Altså er $q = \hat{q}$, og af ligningen følger så, at også $\hat{r} = r$.

Hermed er også entydigheden bevist. □

(2.2) Definition. Antag, at R er et integritetsområde. Det følger af Sætning (1.8), at elementerne i R^*, altså de invertible elementer i R, opfattet som konstante polynomier netop er de invertible elementer i $R[X]$.

Et polynomium d siges at være *divisor* i polynomiet f, og vi skriver $d \mid f$, hvis der findes et polynomium q så at $qd = f$. Divisorer i f svarer altså til *faktoriseringer* af f som produkt af to polynomier, $f = qd$. Det er klart, at et normeret polynomium d er divisor i f, netop når division med rest, Sætning (2.1), fører til restpolynomiet $r = 0$.

De *trivielle divisorer* i f er dels konstanterne u for $u \in R^*$, dels polynomier af formen uf for $u \in R^*$. De trivielle divisorer svarer til de trivielle faktoriseringer,

$$f = (u^{-1}f)u = u^{-1}(uf).$$

Bemærk, at nul-polynomiet 0 indtager en særstilling. Ifølge definitionen ovenfor er ethvert polynomium divisor i 0, men 0 er ikke divisor i noget polynomium $f \neq 0$.

Et polynomium d siges at være en *største fælles divisor* for givne polynomier f og g, hvis d er en fælles divisor (dvs $d \mid f$ og $d \mid g$) og hvis enhver fælles divisor for f og g også er divisor i d. [ordet „største“ refererer ikke til en ordning af polynomierne.]

Det skal understreges, at en største fælles divisor for to givne polynomier f og g ikke nødvendigvis eksisterer.

Et polynomium $f \in R[X]$ kaldes *irreducibelt*, hvis følgende betingelser er opfyldt:

(1) f er forskelligt fra nul-polynomiet,
(2) f er ikke en invertibel konstant,
(3) f har kun trivielle divisorer.

(2.3) Eksempel. Det skal understreges, at begreberne betragtet i (2.2) naturligvis refererer til, og afhænger af, den givne ring R.

Betragt for eksempel polynomiet $f = 2X^2 - 4$. Det har hele koefficienter, og vi har ligningen,

$$f = 2X^2 - 4 = 2 \cdot (X^2 - 2). \tag{*}$$

Når f opfattes som polynomium i $\mathbb{Z}[X]$, er (*) en ikke-triviel faktorisering. De to faktorer, 2 og $X^2 - 2$, er ikke-trivielle divisorer i f.

Når vi i stedet opfatter f som polynomium i $\mathbb{Q}[X]$, så er faktoren 2 en enhed, med den inverse $\frac{1}{2}$. Faktorerne er altså trivielle divisorer i f. Vi skal senere se, at faktoren $g := X^2 - 2$ er et irreducibelt polynomium i $\mathbb{Q}[X]$.

Opfatter vi i stedet g som polynomium i $\mathbb{R}[X]$, så har vi faktoriseringen,

$$g = X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2}).$$

Polynomiet g er altså ikke irreducibelt i $\mathbb{R}[X]$.

(2.4) Observation. Af speciel interesse er tilfældet, hvor ringen R er et legeme L. Vi kan da *normere* et givet polynomium $d \neq 0$ i $L[X]$: når $d \neq 0$, er den ledende koefficient i d et element $u \neq 0$ i L, og ved at multiplicere d med konstanten u^{-1} fremkommer et normeret polynomium $u^{-1}d$. Hvis et polynomium $h \in L[X]$ er skrevet som et produkt, $h = qd$, hvor $d \neq 0$, så får vi for alle $u \neq 0$ i L ligningerne,

$$h = qd = (uq)(u^{-1}d).$$

Vælges u som den ledende koefficient i d, er den anden faktor på højresiden normeret. Vi kan derfor ofte, når et polynomium h med koefficienter i et legeme L er fremstillet som et produkt $h = qd$, antage, at faktoren d er et normeret polynomium.

Af denne observation følger for eksempel umiddelbart, at når R er et legeme L, så gælder Sætningen om division med rest, når blot polynomiet d antages forskelligt fra nul-polynomiet.

(2.5) Euklid's algoritme. *Antag, at L er et legeme. Lad $f, g \in L[X]$ være polynomier, hvoraf mindst ét ikke er nul-polynomiet. Da har f og g en største fælles divisor d, og d kan bestemmes ved følgende algoritme:*

Antag, at $g \neq 0$, og sæt $r_0 := f$ og $r_1 := g$. Bestem polynomiet $r_2 \in L[X]$ som restpolynomiet i Sætningen om division med rest,

$$r_0 = q_1 r_1 + r_2, \qquad \deg(r_2) < \deg(r_1) = \deg(g).$$

Hvis $r_2 \neq 0$, bestemmes polynomiet $r_3 \in L[X]$ som restpolynomiet,

$$r_1 = q_2 r_2 + r_3, \qquad \deg(r_3) < \deg(r_2).$$

Hvis $r_3 \neq 0$ fortsættes. I hvert skridt sænkes graden af restpolynomiet. Algoritmen stopper derfor efter et endeligt antal skridt med en fremstilling,

$$r_{n-1} = q_n r_n + r_{n+1}, \qquad \textit{hvor } r_{n+1} = 0.$$

Det fundne polynomium $d := r_n$ er så en største fælles divisor for f og g. Yderligere gælder, at der findes polynomier $p, s \in L[X]$ således, at $d = pf + sg$.

Bevis. Betragt, for $i = 1, \dots, n$, den i'te ligning,

$$r_{i-1} = q_i r_i + r_{i+1}.$$

Af ligningen følger umiddelbart, at et polynomium d er en fælles divisor for r_i, r_{i+1}, hvis og kun hvis d er en fælles divisor for r_{i-1}, r_i. Heraf ses, at d er en største fælles divisor for r_{i-1}, r_i, hvis og kun hvis d er en største fælles divisor for r_i, r_{i+1}.

For $i = n$ er situationen simpel, idet $r_{n+1} = 0$. Ethvert polynomium er således divisor i r_{n+1}. De fælles divisorer for r_n, r_{n+1} er derfor netop divisorerne i r_n. Specielt er så $d := r_n$ en største fælles divisor for r_n, r_{n+1}. Af ligningerne, for $i = n, \dots, 2, 1$ følger derfor, at $d := r_n$ er en største fælles divisor for r_0, r_1. Da $f = r_0$ og $g = r_1$, er sætningens første påstand hermed bevist.

Den anden påstand følger ved tilbageregning. Vi viser, ved aftagende induktion efter $i = n, \dots, 2, 1$, at vi har en fremstilling $d = p_i r_{i-1} + s_i r_i$ med polynomier p_i og s_i. For $i = n$ har vi ligningen $d = p_n r_{n-1} + s_n r_n$ med $p_n := 0$ og $s_n := 1$. Har vi for $i < n$ en fremstilling $d = p_{i+1} r_i + s_{i+1} r_{i+1}$ får vi, af den i'te ligning,

$$d = p_{i+1} r_i + s_{i+1} r_{i+1} = p_{i+1} r_i + s_{i+1}(r_{i-1} - q_i r_i) = s_{i+1} r_{i-1} + (p_{i+1} - q_i s_{i+1}) r_i,$$

hvilket er en fremstilling $d = p_i r_{i-1} + s_i r_i$ med $p_i := s_{i+1}$ og $s_i := p_{i+1} - q_i s_{i+1}$.

Fremstillingen for $i = 1$ har formen $d = p_1 r_0 + s_1 r_1 = p_1 f + s_1 g$, som ønsket. □

(2.6) Hovedidealsætningen. *Lad L være et legeme. Da er hvert ideal i polynomiumsringen $L[X]$ et hovedideal. Med andre ord: For hvert ideal $\mathfrak{I}$ i $L[X]$ (dvs en delmængde $\mathfrak{I} \subseteq L[X]$ som indeholder 0 og er stabil under addition og stabil under multiplikation med et vilkårligt element i $R[X]$) findes et polynomium $d \in L[X]$ således, at $\mathfrak{I} = (d)$, altså,*

$$\mathfrak{I} = \{\, qd \mid q \in L[X] \,\}. \tag{2.6.1}$$

Bevis. Hvis $\mathfrak{I} = \{0\}$, kan vi øjensynlig bruge $d := 0$. Antag derfor, at $\mathfrak{I} \neq \{0\}$. Vælg et polynomium $d \in \mathfrak{I} \setminus \{0\}$, hvis grad er mindst blandt alle grader af polynomier i $\mathfrak{I} \setminus \{0\}$. Vi kan antage, at d er normeret, thi hvis u er den ledende koefficient i d, så er polynomiet $u^{-1}d$ et normeret polynomium, og dette polynomium ligger ligeledes i idealet $\mathfrak{I}$, og det har samme grad som d. Det påstås, at ligningen (2.6.1) er opfyldt.

Da d er valgt i $\mathfrak{I}$ og $\mathfrak{I}$ er et ideal, ligger qd i $\mathfrak{I}$ for hvert polynomium q. Ligningens højreside er altså indeholdt i venstresiden.

For at vise den omvendte inklusion betragtes et polynomium f i $\mathfrak{I}$. Ifølge Sætningen om division med rest (2.1) har vi en fremstilling,

$$f = qd + r, \quad \deg(r) < \deg(d).$$

Da $\mathfrak{I}$ er et ideal og $f, d \in \mathfrak{I}$, vil også $f - qd$ tilhøre $\mathfrak{I}$. Altså er $r \in \mathfrak{I}$. Hvis $r \neq 0$, ville uligheden $\deg(r) < \deg(d)$ være i modstrid med at d havde den laveste grad blandt polynomier forskellige fra 0 i $\mathfrak{I}$. Følgelig er $r = 0$, og altså $f = qd \in (d)$. □

(2.7) Bemærkning. Et mindre algoritmisk bevis for eksistensen af d i Sætning (2.5) kan gives ved brug af Hovedidealsætningen. Betragt for givne polynomier $f, g \in L[X]$ følgende mængde af polynomier,

$$\mathfrak{I} := (f) + (g) = \{\, pf + sg \mid p, s \in L[X] \,\}.$$

Delmængden $\mathfrak{I}$ er øjensynlig et ideal. Altså er $\mathfrak{I}$ et hovedideal. Der findes derfor et polynomium $d \in L[X]$ så at $\mathfrak{I} = (d)$.

Polynomiet f kan skrives $f = 1f + 0g$, så f ligger i $\mathfrak{I}$ og dermed i (d). Af $f \in (d)$ følger, at d er divisor i f. Tilsvarende er d divisor i g. Altså er d en fælles divisor for f, g. Da d ligger i $\mathfrak{I}$, har d formen $d = pf + sg$. Enhver fælles divisor for f, g er derfor divisor i d. Følgelig er d en største fælles divisor for f, g.

(2.8) Opgaver.

1. Bestem, i $\mathbb{Z}[X]$, resten af $X^6 + X^5 + X + 1$ ved division med $X^2 + X + 1$.

2. Bestem, i $\mathbb{Z}[X]$, resten af X^5 ved division med $X^4 + X^3 + X^2 + X + 1$.

3. Bestem, i $(\mathbb{Z}/7)[X]$, resten af $X^6 + 1$ ved division med $X^2 + 3$.

4. Lad R være en delring af ringen S. Lad h, f være polynomier i $R[X]$. Vis, at hvis h er et normeret polynomium (eller R er et legeme og $h \neq 0$), så er $h \mid f$ i ringen $R[X]$, hvis og kun hvis $h \mid f$ i ringen $S[X]$.

5. Bestem de irreducible polynomier af grad 2 og 3 i $\mathbb{F}_2[X]$.

6. Bestem, for et integritetsområde R, alle irreducible, normerede førstegradspolynomier.

3. Rødder.

(3.1) Definition. Lad der være givet en kommutativ ring A, der indeholder R som delring, og i A et element α. Til et givet polynomium f i $R[X]$,

$$f = a_0 + a_1X + \cdots + a_nX^n,$$

kan vi da knytte elementet $f(\alpha)$ i A givet ved ligningen,

$$f(\alpha) := a_0 + a_1\alpha + \cdots + a_n\alpha^n.$$

Elementet $f(\alpha) \in A$ siges at fremkomme ved at *indsætte* elementet α i polynomiet f, eller ved at *evaluere* f i α, og $f(\alpha)$ kaldes også *værdien* af f i α. Hvis $f(\alpha) = 0$, siges α at være *rod* i (eller *nulpunkt* for) polynomiet f.

Evalueringsafbildningen, altså afbildningen,

$$f \mapsto f(\alpha),$$

er en ringhomomorfi $R[X] \to A$; den afbilder altså sum og produkt af polynomier i sum og produkt af billedelementerne, og det konstante polynomium 1 i et-elementet i A. Dette følger af, at vi ved bestemmelse af sum, $f+g$, og produkt, fg, af to polynomier f og g kun benytter regnereglerne i en kommutativ ring og at X^i er den i'te potens af X. De samme regneregler anvendt på $f(\alpha)$ og $g(\alpha)$ viser, at $f(\alpha) + g(\alpha) = (f+g)(\alpha)$ og $f(\alpha)\,g(\alpha) = (fg)(\alpha)$. Indsættelse af α i et konstant polynomium giver blot konstanten som element i A. Specielt ses, at evalueringsafbildningen afbilder et-elementet 1 i $R[X]$ på et-elementet $1 \in A$.

Kernen for evalueringsafbildningen består øjensynlig af de polynomier i $R[X]$, der har α som rod. Polynomierne i $R[X]$ med α som rod udgør altså en undergruppe i $R[X]$ (endda et såkaldt *ideal* i ringen $R[X]$, dvs en undergruppe som også er stabil under multiplikation med et vilkårlig element fra ringen).

Et vigtigt specialtilfælde fås for $A = R$, hvor vi altså indsætter et element $a \in R$ i polynomier fra $R[X]$. I dette tilfælde er evalueringsafbildningen en surjektiv ringhomomorfi $R[X] \to R$, idet elementet $b \in R$ fås ved at evaluere det konstante polynomium b.

(3.2) Eksempel. Definitionen ovenfor, for reelle polynomier, er velkendt. For et givet reelt polynomium f undersøges ved indsættelse om et givet komplekst tal α er rod. Det svarer til tilfældet, hvor $R = \mathbb{R}$ og $A = \mathbb{C}$. I dette tilfælde, for et givet $\alpha \in \mathbb{C}$, er evalueringsafbildningen en homomorfi $\mathbb{R}[X] \to \mathbb{C}$.

Fx ses ved indsættelse, at polynomiet $f = 2X^3 - 3X^2 + 1$ har tallene 1 og $-\frac{1}{2}$ som rødder.

Polynomiet $g = 1 + X + X^2$ har ingen reelle rødder, men det har to komplekse rødder, $-\frac{1}{2} \pm \frac{1}{2}i\sqrt{3}$.

Polynomiet $h = (1+X)^m$, for $m \geqslant 1$, har roden -1.

(3.3) Eksempel. Hvis ringen R er endelig, er det naturligvis en endelig opgave at bestemme hvilke elementer α i R, der er rod i et givet polynomium.

For $R := \mathbb{F}_7$ ses for eksempel ved indsættelse, at hver af de 6 restklasser 1, 2, 3, 4, 5, 6 er rod i polynomiet $X^6 - 1$. Restklassen 0 er ikke rod.

For $R = \mathbb{Z}/6$ ses, at samtlige 6 restklasser i $\mathbb{Z}/6$ er rødder i polynomiet $X^3 - X$.

(3.4) Sætning. *Polynomiet $f \in R[X]$ har elementet $a \in R$ som rod, hvis og kun hvis det kan skrives på formen,*

$$f = q \cdot (X - a), \tag{3.4.1}$$

med et polynomium $q \in R[X]$.

Bevis. Anvendes Sætningen om division med rest (2.1) på førstegradspolynomiet $d := X - a$ fås en (entydig) fremstilling $f = q \cdot (X - a) + r$, hvor $\deg r < 1$. Polynomiet $r \in R[X]$ har grad mindre end 1, og det må derfor være et konstant polynomium. Indsættelse af a giver ligningen $f(a) = q(a)0 + r = r$. Altså er $r = f(a)$ og fremstillingen har formen,

$$f = q \cdot (X - a) + f(a), \tag{3.4.2}$$

med et passende polynomium $q \in R[X]$. Heraf følger påstanden i Sætningen. Har nemlig f en fremstilling (3.4.1), så har vi $f(a) = 0 \cdot q(a) = 0$, og hvis omvendt $f(a) = 0$, så fås fremstillingen (3.4.1) af (3.4.2). ▯

(3.5) Korollar. *Hvert polynomium $f \neq 0$ af grad n i $R[X]$ har en fremstilling*

$$f = \tilde{f} \cdot (X - a_1) \cdots (X - a_k), \tag{3.5.1}$$

hvor $0 \leqslant k \leqslant n$ og $a_i \in R$ for $i = 1, \dots, k$ og hvor $\tilde{f} \in R[X]$ er et polynomium uden rødder i R.

Hvis R er et integritetsområde, så er fremstillingen entydig (bortset fra permutation af førstegradsfaktorerne), og a_i'erne er samtlige rødder fra R i f. Specielt er antallet af rødder fra R i f endeligt, og højst lig med graden af f.

Bevis. Hvis f ikke har rødder i R, får vi den ønskede fremstilling med $\tilde{f} := f$ og $k := 0$. Hvis f har en rod $a_1 \in R$, får vi af Sætning (3.4) en fremstilling $f = q \cdot (X - a_1)$ og da $X - a_1$ er normeret, er $\deg(q) = \deg(f) - 1 = n - 1$. Hvis q ikke har rødder er dette den ønskede fremstilling, med $k := 1$ og $\tilde{f} := q$. Hvis q har en rod a_2, anvender vi Sætning (3.4) på polynomiet q, og fortsætter. Ved hvert skridt falder graden med 1. Efter højst n skridt får vi derfor den ønskede fremstilling.

Antag nu, at R er et integritetsområde. Betragt en fremstilling (3.5.1). Hvert a_i giver nul ved indsættelse i højresiden og følgelig er a_i rod i f. Lad omvendt $a \in R$ være en rod i f. Indsættelse af a i (3.5.1) giver så ligningen $0 = \tilde{f}(a)(a - a_1) \cdots (a - a_k)$. Da R er et integritetsområde, følger det af ligningen, at en af faktorerne er 0. Faktoren $\tilde{f}(a)$ er ikke nul, da polynomiet $\tilde{f}$ ikke har rødder i R. Altså er $a - a_i = 0$ for et passende i, dvs roden a er et af a_i'erne.

Det er således vist, at a_i'erne netop er rødderne i f. Specielt er antallet af rødder i f højst k, og dermed højst lig med graden n af f.

Vi mangler at vise entydigheden af fremstillingen (3.5.1). Vi viser, ved induktion efter k, at hvis et polynomium f har en fremstilling (3.5.1) og yderligere en fremstilling,

$$f = \hat{f} \cdot (X - b_1) \cdots (X - b_l),$$

hvor $\hat{f}$ er et polynomium uden rødder i R, så er $\hat{f} = \tilde{f}$, og $l = k$, og, efter en passende permutation af rødderne b_i er $b_i = a_i$ for $i = 1, \dots, k$.

Påstanden er klar, hvis $k = 0$. Antag derfor, at $k > 0$. Da har polynomiet rødder, så specielt er $l > 0$. Elementet b_l er rod i f, altså ifølge det viste lig med et af a_i'erne. Vi kan antage, at $b_l = a_k$. Vi har så ligningen,

$$f = \tilde{f} \cdot (X - a_1) \cdots (X - a_{k-1}) \cdot (X - a_k) = \hat{f} \cdot (X - b_1) \cdots (X - b_{l-1}) \cdot (X - a_k),$$

og heraf fås (da nul-reglen gælder i $R[X]$) følgende ligning:

$$\tilde{f} \cdot (X - a_1) \cdots (X - a_{k-1}) = \hat{f} \cdot (X - b_1) \cdots (X - b_{l-1}).$$

Induktivt følger det af denne ligning, at $\hat{f} = \tilde{f}$, at $l - 1 = k - 1$ og (eventuelt efter permutation), at $b_i = a_i$ for $i = 1, \dots, k - 1$.

Hermed er entydigheden vist, og alle korollarets påstande bevist. □

(3.6) Multiplicitet. Det skal understreges, at det i fremstillingen (3.5.1) af polynomiet $f \neq 0$ ikke antages, at a_i'erne er forskellige. Et bestemt element $a \in R$ kan være *multipel* rod, dvs forekomme flere gange blandt a_i'erne. Mere præcist siges et element $a \in R$ at være *ν-dobbelt rod* eller at være en *rod af multiplicitet mindst* ν i polynomiet f, hvis f kan skrives på formen,

$$f = q \cdot (X - a)^\nu,$$

med et polynomium $q \in R[X]$. Hvis a er ν-dobbelt rod i f, kan vi øjensynlig bestemme en fremstilling (3.5.1), hvor a forekommer (mindst) ν gange blandt a_i'erne. Hvis R er et integritetsområde, så følger det af fremstillingens entydighed, at antallet af rødder fra R i f, talt med multiplicitet, højst er lig med graden af f.

(3.7) Observation. Antag, at ringen R er et integritetsområde. Hvis rødderne $a_i \in R$ (med multiplicitet) er bestemt i et givet polynomium f, så bestemmes polynomiet $\tilde{f}$ ved at dividere f med produktet af førstegradspolynomierne $X - a_i$. Hvis antallet af rødder er lig med graden af f, er denne division let. I dette tilfælde har $\tilde{f}$ nemlig graden 0, så $\tilde{f}$ er en konstant. Sammenligning af de ledende koefficienter giver, at denne konstant er den ledende koefficient i f. Specielt fremhæves, at hvis der i et normeret polynomium f af grad n i $R[X]$ er bestemt n forskellige rødder $a_1, \dots, a_n$ i R, så gælder i $R[X]$ ligningen,

$$f = (X - a_1) \cdots (X - a_n).$$

Entydigheden af fremstillingen udnyttes ofte i følgende situation. Antag, at polynomiet f er et produkt $f = gh$ af polynomier g og h. Antag videre, at der er givet fremstillinger svarende til (3.5.1) for polynomierne g og h. Specielt indgår heri polynomier $\tilde{g}$ og $\tilde{h}$ uden rødder i R. Da R er et integritetsområde, har produktet $\tilde{g}\tilde{h}$ så ikke rødder i R. Det følger, at fremstillingen for polynomiet f fås ved at multiplicere fremstillingerne for g og h. Specielt er $\tilde{f} = \tilde{g}\tilde{h}$.

(3.8) Eksempel. Polynomiet $f = 2X^3 - 3X^2 + 1$ i $\mathbb{Q}[X]$ har tallene 1 og $-\frac{1}{2}$ som rødder. Efter division med $X - 1$ fås polynomiet $2X^2 - X - 1$, som også har 1 som rod. Altså er

$$f = 2(X-1)^2(X + \tfrac{1}{2}),$$

hvilket er den søgte fremstilling af f, med $\tilde{f} = 2$. Roden 1 er altså dobbeltrod i f.

(3.9) Polynomiumsfunktioner. I (3.1) har vi, for et fast element $\alpha \in R$, betragtet værdien $f(\alpha)$ som funktion af polynomiet $f \in R[X]$. Det er evalueringsafbildningen $f \mapsto f(\alpha)$. Vi kan også betragte værdien, for et fast polynomium f, som funktion af α, altså afbildningen,

$$\alpha \mapsto f(\alpha) \quad \text{for } \alpha \in R. \tag{3.9.1}$$

Afbildninger $R \to R$, der er af denne form, kaldes *polynomiumsfunktioner*. Polynomiumsfunktionerne ligger i funktionsringen $\mathcal{F}(R, R)$ af alle afbildninger $R \to R$. Det er let at se, at afbildningen,

$$R[X] \to \mathcal{F}(R, R), \tag{3.9.2}$$

der til et polynomium $f \in R[X]$ knytter den tilhørende polynomiumsfunktion, er en ringhomomorfi. Billedringen, bestående af alle polynomiumsfunktioner, betegnes $\mathcal{P}ol(R, R)$.

Et polynomium f ligger i kernen for homomorfien (3.9.2) netop når den tilhørende polynomiumsfunktion er nul-funktionen, dvs netop når hvert element $\alpha \in R$ er rod i f.

Antag, at R er et integritetsområde med uendelig mange elementer. Da følger det af Korollar (3.5), at kun nul-polynomiet kan have alle elementer i R som rødder. Følgelig er homomorfien (3.9.2) injektiv. Polynomiumsringen $R[X]$ kan altså i dette tilfælde identificeres med ringen $\mathcal{P}ol(R, R)$ af polynomiumsfunktioner $R \to R$.

Bemærk, at forudsætningen om at der skal være uendelig mange elementer i R er nødvendig. Hvis R kun indeholder endelig mange elementer $a_1, \dots, a_k$, så er polynomiet $(X - a_1) \cdots (X - a_k)$ i $R[X]$ et normeret polynomium, og den tilhørende polynomiumsfunktion $R \to R$ er identisk nul.

(3.10) Algebraens Fundamentalsætning. Som bekendt udsiger Algebraens Fundamentalsætning, at ethvert polynomium af positiv grad i $\mathbb{C}[X]$ har en rod i $\mathbb{C}$. I fremstillingen (3.5.1) af et polynomium f i $\mathbb{C}[X]$ af grad $n \geqslant 1$ må polynomiet $\tilde{f}$ altså være konstant. Fremstillingen er altså den velkendte fremstilling,

$$f = u(X - \alpha_1) \cdots (X - \alpha_n), \tag{1}$$

hvor $u \in \mathbb{C}$ er den ledende koefficient i f og α_j'erne er rødderne i f, med multiplicitet.

Det følger, at et polynomium af grad mindst 2 i $\mathbb{C}[X]$ ikke kan være irreducibelt. De normerede irreducible polynomier i $\mathbb{C}[X]$ er altså førstegradspolynomierne $X - \alpha$ for $\alpha \in \mathbb{C}$.

For et polynomium $f \in \mathbb{C}[X]$ betegnes med $\bar{f}$ det komplekst konjugerede polynomium, dvs det polynomium, der fremkommer ved at erstatte koefficienterne i f med deres komplekst konjugerede. Kompleks konjugering er en ringhomomorfi $\mathbb{C} \to \mathbb{C}$. Heraf følger let, at afbildningen $f \mapsto \bar{f}$ er en ringhomomorfi $\mathbb{C}[X] \to \mathbb{C}[X]$. Fremstillingen (3.5.1) for det komplekst konjugerede polynomium $\bar{f}$ fremkommer altså af (1) ved at erstatte u med $\bar{u}$ og $X - \alpha_j$ med $X - \bar{\alpha}_j$ for $j = 1, \dots, n$. Rødderne i $\bar{f}$ er altså de komplekst konjugerede til rødderne i f, og de forekommer med samme multiplicitet i f og $\bar{f}$.

Antag nu, at polynomiet f har reelle koefficienter. Da er $\bar{f} = f$. Følgelig gælder, at hvis et ikke-reelt tal α forekommer blandt α_j'erne, så forekommer også $\bar{\alpha}$ blandt α_j'erne, endda det samme antal gange.

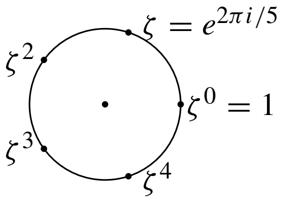
Denne observation kan udnyttes på følgende måde: I fremstillingen (1) forekommer blandt α_j'erne dels reelle rødder $\alpha = a$, hvor $a \in \mathbb{R}$, dels imaginære (dvs ikke-reelle) rødder $\alpha = b + ic$, hvor $b, c \in \mathbb{R}$ og $c \neq 0$. I produktet i (1) forekommer de imaginære faktorer i par bestående af $X - \alpha$ og $X - \bar{\alpha}$. For $\alpha = b + ic$ har vi $(X - \alpha)(X - \bar{\alpha}) = (X - b)^2 + c^2$. Idet vi således i (1) slår de imaginære faktorer sammen to og to, får vi en fremstilling,

$$f = u(X - a_1) \cdots (X - a_k) \cdot \big((X - b_1)^2 + c_1^2\big) \cdots \big((X - b_l)^2 + c_l^2\big), \tag{2}$$

hvor tallene på højresiden er reelle og c_j'erne er forskellige fra 0. Sammenligning af graderne giver $n = k + 2l$.

Polynomierne i $\mathbb{R}[X]$ af formen $(X - b)^2 + c^2$, hvor $c \neq 0$, er netop de normerede andengradspolynomier uden rødder. Det fremgår således af fremstillingen (2), at de normerede irreducible polynomier i $\mathbb{R}[X]$ er førstegradspolynomierne $X - a$ for $a \in \mathbb{R}$ og de normerede andengradspolynomier uden reelle rødder.

(3.11) Enhedsrødder. Polynomiet $X^n - 1$ har n rødder i $\mathbb{C}$, nemlig de såkaldte komplekse n'te *enhedsrødder*, dvs de komplekse tal af formen $\exp(2\pi ik/n)$ for $k = 0, 1, \dots, n - 1$. Enhedsrødderne ligger på enhedscirklen. De udgør hjørnerne i en regulær n-kant. Sættes $\zeta := \exp(2\pi i/n)$, så er $\exp(2\pi ik/n) = \zeta^k$. Enhedsrødderne er altså potenserne af ζ.



Som nævnt i (3.10) opnås følgende ligning i $\mathbb{C}[X]$:

$$X^n - 1 = (X - 1)(X - \zeta)(X - \zeta^2) \cdots (X - \zeta^{n-1}).$$

Af ligningen $X^n - 1 = (X - 1)(X^{n-1} + \cdots + X + 1)$ følger, at polynomiet $X^{n-1} + \cdots + X + 1$ har rødderne ζ^k for $k \not\equiv 0 \pmod{n}$. For dette polynomium har vi altså fremstillingen,

$$X^{n-1} + \cdots + X + 1 = (X - \zeta)(X - \zeta^2) \cdots (X - \zeta^{n-1}).$$

(3.12) Eksempel. Lad p være et primtal. Betragt polynomiet $X^{p-1} - 1$ i $\mathbb{F}_p[X]$. Ifølge Fermat's lille Sætning gælder for hvert element a i $\mathbb{F}_p^*$, altså for hver restklasse a forskellig fra nulklassen i $\mathbb{Z}/p$, at $a^{p-1} = 1$. Hvert af de $p-1$ elementer a i $\mathbb{F}_p^*$ er derfor rod i polynomiet $X^{p-1}-1$. Da polynomiet er normeret, har vi derfor i $\mathbb{F}_p[X]$ ligningen,

$$X^{p-1}-1 = \prod_{a\in\mathbb{F}_p^*}(X-a).$$

De $p-1$ elementer i $\mathbb{F}_p^*$ er restklasserne $[k]$ for $1 \leqslant k < p$. Alternativt kan ligningen derfor skrives,

$$X^{p-1}-[1] = \bigl(X-[1]\bigr)\bigl(X-[2]\bigr)\cdots\bigl(X-[p-1]\bigr).$$

Bemærk, at ligningen ovenfor, som enhver ligning mellem polynomier, udtrykker uendelig mange ligninger mellem koefficienterne, nemlig at den i'te koefficient på venstresiden er lig med den i'te koefficient på højresiden, for $i = 0, 1, 2, \dots$. Fx følger det af ligningen ovenfor, ved at betragte konstantleddene, at restklassen $-[1]$ er lig med produktet af restklasserne $-[k]$ for $k = 1, 2, \dots, p-1$. Det sidste produkt er restklassen af $(-1)^{p-1}(p-1)!$. Når p er et ulige primtal, er $(-1)^{p-1} = 1$, så resultatet kan udtrykkes ved *Wilson's Sætning*,

$$(p-1)! \equiv -1 \pmod{p}.$$

(3.13) Sætning. *Lad L være et legeme og lad G være en endelig undergruppe af den multiplikative gruppe L^*. Da er G en cyklisk gruppe.*

Bevis. Lad m være den maksimale orden af et element i G. Det er nok at vise, at $m = |G|$, thi et element af orden m frembringer en cyklisk undergruppe af orden m, og hvis $m = |G|$, må denne cykliske undergruppe være hele G.

Den multiplikative gruppe L^* er kommutativ, så specielt er G en endelig kommutativ gruppe. Det er derfor velkendt, at ordenen af et vilkårligt element $a \in G$ er divisor i den maksimale elementorden m, og følgelig er $a^m = 1$. Polynomiet $X^m - 1 \in L[X]$ har derfor hvert element a i G som rod. Altså er elementantallet i G højst lig med polynomiets grad, dvs $|G| \leqslant m$. Heraf følger umiddelbart, at $|G| = m$, som ønsket. □

(3.14) Eksempel. For legemet $L = \mathbb{C}$ er det let at se direkte, at de endelige undergrupper af $\mathbb{C}^*$ er de cykliske grupper C_n. Øjensynlig er $\{1\}$ og $\{\pm 1\}$ de eneste endelige undergrupper af $\mathbb{R}^*$.

Mere interessant er tilfældet, hvor L er et endeligt legeme. Her følger det specielt af Sætningen, at den multiplikative gruppe L^* er en cyklisk gruppe. Vi fremhæver specialtilfældet, hvor $L := \mathbb{F}_p$ er legemet af restklasser modulo et primtal p. Den multiplikative gruppe $\mathbb{F}_p^*$ er altså cyklisk, eller, med andre ord:

Sætning. *For hvert primtal p er den multiplikative gruppe $(\mathbb{Z}/p)^*$ cyklisk.*

(3.15) Observation. Antag, at R er et legeme L. Af resultatet i (3.4) fremgår, at et polynomium $f \in L[X]$, der har en rod $a \in L$, er deleligt med førstegradspolynomiet $X - a$. Et polynomium af grad større end 1, som har en rod i L, kan altså ikke være irreducibelt.

Et polynomium f af grad 1 har naturligvis en rod: Er $f = uX + b$, hvor $u \neq 0$, har vi $f = u(X-a)$, hvor $a := -u^{-1}b$, og a er rod i f. I øvrigt er polynomierne af grad 1 også irreducible: I en ikke-triviel faktorisering $f = gh$ skulle g og h jo have positiv grad, hvilket ikke er muligt, når summen af de to grader skal være 1.

For polynomier f i $L[X]$ af grad 2 eller 3 gælder, at f er irreducibelt, hvis og kun hvis f ikke har rødder i L. Antag nemlig, at f har en ikke-triviel faktorisering $f = gh$. Polynomierne g og h har så positiv grad, og summen af graderne er højst 3. Et af de to polynomier g, h er altså et førstegradspolynomium, og det har derfor en rod i L. Denne rod er øjensynlig også rod i f.

For polynomier af grad større end 3 er situationen mere kompliceret. Fx har ingen af polynomierne $f := X^4 + 4$ og $g := X^4 + 2$ reelle rødder, men det fremgår af (3.10), at begge polynomier i $\mathbb{R}[X]$ må være et produkt af to andengradspolynomier. Ingen af polynomierne er altså irreducible i $\mathbb{R}[X]$. Faktisk er

$$X^4 + 4 = (X^2 + 2X + 2)(X^2 - 2X + 2),$$

så $X^4 + 4$ er heller ikke irreducibelt i $\mathbb{Q}[X]$. Som vi senere skal se, er $X^4 + 2$ et irreducibelt polynomium i $\mathbb{Q}[X]$.

(3.16) Bemærkning. For et polynomium $f = a_0 + a_1X + \cdots + a_nX^n$ i $R[X]$ defineres det *afledede* polynomium f' ved ligningen

$$f' := a_1 + 2a_2X + \cdots + na_nX^{n-1},$$

hvor $ia_i = \overbrace{a_i + \cdots + a_i}^{i}$. Det er let at eftervise regnereglerne (svarende til sædvanlig differentiation af funktioner):

$$(f + g)' = f' + g', \quad (fg)' = f'g + fg'.$$

For et konstant polynomium bliver det afledede polynomium naturligvis nul-polynomiet. Det skal imidlertid understreges, at hvis ringen R har positiv karakteristik, så kan det indtræffe for polynomier af positiv grad, at det afledede polynomium er nul-polynomiet.

For et primtal p finder vi fx for polynomiet $f := X^p \in \mathbb{F}_p[X]$, at $f' = 0$, og for $g = X^p - X$ finder vi $g' = -1$.

Sætning. *Lad $f \neq 0$ være et polynomium i $R[X]$ og lad a være element i R. Da er a dobbeltrod i f, hvis og kun hvis a er rod i både f og f'.*

Bevis. Vi kan øjensynlig antage i beviset, at a er rod i f. Der findes altså en faktorisering $f = q \cdot (X - a)$, hvor $q \in R[X]$. Heraf fås ligningen,

$$f' = q' \cdot (X - a) + q\,. \tag{*}$$

Hvis a er dobbeltrod i f, kan vi i fremstillingen af f vælge q af formen $q = \hat{q} \cdot (X - a)$. Specielt er så a rod i q, og det følger af (*), at a er rod i f'.

Antag omvendt, at a er rod i f'. Så følger det af ligningen (*), at a er rod i q. Altså har q formen $q = \hat{q} \cdot (X - a)$. Følgelig er $f = \hat{q} \cdot (X - a)^2$, og a er dobbeltrod i f. □

(3.17) Opgaver.

1. Lad R være en ring, hvori tallet 2 er invertibelt, dvs således, at $1_R + 1_R$ er et invertibelt element i R. For et andengradspolynomium $f = aX^2 + bX + c \in R[X]$ defineres diskriminanten $D := b^2 - 4ac$. Antag, at a er invertibel i R. Vis, at f har en rod i R, hvis og kun hvis $g := X^2 - D$ har en rod i R, og beskriv sammenhængen mellem rødder i f og g.

2. Vis, at polynomiet $X^2 + 1 \in \mathbb{F}_{11}[X]$ ikke har rødder i $\mathbb{F}_{11}$.

3. Bestem et polynomium af grad 4 i $\mathbb{F}_2[X]$, som ikke har rødder.

4. Vis, at polynomiet $f = X^2 + 1 \in (\mathbb{Z}/65)[X]$ har fire rødder i $\mathbb{Z}/65$, og bestem to fremstillinger af formen $f = (X - a_1)(X - a_2)$.

5. Betragt funktionen $\cos 3t$ i ringen $R := \mathcal{C}^\infty(\mathbb{R})$. Vis, at funktionen $\cos t$ er rod i polynomiet $4X^3 - 3X - \cos 3t \in R[X]$. Har polynomiet flere rødder i R?

6. Lad R være et integritetsområde. I et normeret polynomium f af grad n i $R[X]$ kendes (med multiplicitet) $n - 1$ rødder. Vis, at f har n rødder. Hvordan bestemmes den n'te?

7. Vis, at polynomiet $X^{\varphi(n)} - 1$ i $(\mathbb{Z}/n)[X]$ har enhver af de $\varphi(n)$ primiske restklasser som rod. Undersøg, om ligningen $X^{\varphi(n)} - 1 = \prod(X - a)$ gælder; produktet er over de primiske restklasser $a \in (\mathbb{Z}/n)^*$.

8. Et tal $\xi \in \mathbb{C}$ kaldes *algebraisk*, hvis det er rod i et polynomium $f \neq 0$ i $\mathbb{Z}[X]$ (ækvivalent: rod i et normeret polynomium i $\mathbb{Q}[X]$), og *transcendent* ellers. Vis, at følgende tal er algebraiske: -7, $\frac{3}{8}$, $\sqrt{2}$, $(1 + \sqrt{5})/2$, i, $e^{2\pi i/7}$, $\sqrt[3]{1 + \sqrt{2} + \sqrt{3}}$, $\cos(2\pi/7)$.

9. *Vis, at de algebraiske tal udgør en delring af $\mathbb{C}$; – endda et legeme.

10. *Vis, at der findes reelle transcendente tal. [Vink: tallene e, π, og $\log 2$ er transcendente, men det er nu ikke så nemt at vise.]

11. Vis, for et ulige primtal p, at gruppen $\mathbb{F}_p^*$ har et element af orden 4, hvis og kun hvis $p \equiv 1 \pmod 4$. Slut heraf, at polynomiet $X^2 + 1$ har en rod i $\mathbb{F}_p$, hvis og kun hvis $p \equiv 1 \pmod 4$. [Vink: gruppen $\mathbb{F}_p^*$ er cyklisk.]

12. Faktoriser polynomiet $X^4 + 2$ i ringen $\mathbb{R}[X]$.

4. Rationale koefficienter.

(4.1). I (2.2) har vi, for et integritetsområde R, kaldt et polynomium $f \in R[X]$ irreducibelt, hvis f ikke er 0 og ikke er en invertibel konstant, og hvis f kun har trivielle divisorer. Specielt er konstante polynomier irreducible, netop når de er irreducible i R. Da R er et integritetsområde, er graden af et produkt af polynomier summen af faktorernes grader. Et polynomium f af positiv grad er derfor *reducibelt*, hvis og kun hvis der findes en faktorisering,

$$f = gh,$$

hvor enten begge faktorerne g og h er polynomier af grad mindre end graden af f eller hvor en af faktorerne er en konstant, der ikke er invertibel i R. Det er klart, at et polynomium f af positiv grad har en fremstilling,

$$f = h_1 \cdots h_r, \tag{4.1.1}$$

hvor hver faktor h_i er et polynomium af positiv grad, som ikke yderligere kan faktoriseres i to polynomier af lavere grad. Hvis R er et legeme, er faktorerne h_i øjensynlig irreducible polynomier; i dette tilfælde kan f altså skrives som produkt af irreducible polynomier. Hvis R ikke er et legeme, resterer muligheden at de enkelte faktorer h_i yderligere kan faktoriseres, idet de kan have konstanter som ikke-trivielle divisorer.

I dette kapitel ser vi nøjere på faktorisering for polynomier med hele og med rationale koefficienter, altså for polynomiumsringene $\mathbb{Z}[X] \subseteq \mathbb{Q}[X]$. Delringene af konstanter er henholdsvis $\mathbb{Z}$ og $\mathbb{Q}$. For at fremhæve, at en betegnelse ikke nødvendigvis står for en konstant, vil vi oftest bruge betegnelser som $f(X)$ og $\varphi(X)$ for polynomier. De græske bogstaver vil blive brugt for polynomier i $\mathbb{Q}[X]$.

En række af resultaterne kan umiddelbart generaliseres til såkaldte *faktorielle* ringe, dvs ringe for hvilke der findes en faktoriseringsteori svarende til Aritmetikkens Fundamentalsætning for ringen $\mathbb{Z}$. Denne generalisering omtaler vi kort til sidst.

(4.2) Definition. Lad der være givet et polynomium $f(X)$ i $\mathbb{Z}[X]$. En konstant $d \in \mathbb{Z}$ er divisor i $f(X)$, når der findes en faktorisering af formen,

$$f(X) = dg(X), \quad \text{hvor } g(X) \in \mathbb{Z}[X]; \tag{4.2.1}$$

det indtræffer, hvis og kun hvis tallet d er en fælles divisor for koefficienterne i $f(X)$. Polynomiet $f(X)$ kaldes *primitivt*, hvis tallet 1 er den største fælles divisor for koefficienterne. Ækvivalent er $f(X)$ altså et primitivt polynomium, hvis de eneste faktoriseringer af formen (4.2.1) er de trivielle, hvor tallet d er ± 1.

Når $f(X) \neq 0$, kan vi betragte faktoriseringen (4.2.1), hvor d er den største fælles divisor for koefficienterne i $f(X)$. Det er klart, at polynomiet $g(X)$ så er primitivt. Heraf følger, at ethvert polynomium $f(X)$ i $\mathbb{Z}[X]$, som ikke er nul eller en af konstanterne ± 1, kan skrives som produkt af irreducible polynomier. Antag nemlig først, at $f(X)$ har positiv grad. Vi har da en faktorisering (4.1.1), hvor hver faktor $h_i(X)$ er et polynomium af positiv grad, som ikke kan faktoriseres i polynomier af lavere grad. Skriver vi hver faktor som et produkt af en konstant og et primitivt polynomium, og samler vi produktet af konstanterne i en enkelt konstant, får vi en fremstilling,

$$f(X) = dh_1(X)\cdots h_r(X),$$

hvor faktorerne $h_i(X)$ er irreducible polynomier af positiv grad. En sådan fremstilling, med $r = 0$, har vi også, hvis $f(X)$ er konstant. I fremstillingen kan vi yderligere faktorisere konstanten d som et fortegn gange et produkt af primtal. Herved fås øjensynlig den ønskede fremstilling af $f(X)$ som produkt af polynomier, der er irreducible i $\mathbb{Z}[X]$.

(4.3) Lemma. *Hvis et primtal p er divisor i et produkt $f(X)g(X)$ af to polynomier i $\mathbb{Z}[X]$, så er p, i ringen $\mathbb{Z}[X]$, divisor i en af faktorerne.*

Bevis. Betragt ringhomomorfien $\mathbb{Z}[X] \to (\mathbb{Z}/p)[X]$ induceret af den kanoniske homomorfi $\mathbb{Z} \to \mathbb{Z}/p$, jfr (1.10). Herved afbildes et polynomium $k(X) \in \mathbb{Z}[X]$ på det polynomium $\bar{k}(X) \in (\mathbb{Z}/p)[X]$, der fremkommer ved at erstatte koefficienterne med deres restklasser modulo p. I produktet $f(X)g(X)$ er alle koefficienter ifølge forudsætningen delelige med p, så produktet afbildes på nul-polynomiet i $(\mathbb{Z}/p)[X]$. Vi har altså ligningen $\bar{f}(X)\bar{g}(X) = 0$ i ringen $(\mathbb{Z}/p)[X]$. Da p er et primtal, er restklasseringen $\mathbb{Z}/p$ et integritetsområde (endda et legeme). Ifølge Sætning (1.8) er polynomiumsringen $(\mathbb{Z}/p)[X]$ så et integritetsområde. Af ligningen $\bar{f}(X)\bar{g}(X) = 0$ følger derfor, at $\bar{f}(X) = 0$ eller $\bar{g}(X) = 0$. Og det betyder netop, at $f(X)$ eller $g(X)$ har alle koefficienter delelige med p, altså at p er divisor i $f(X)$ eller i $g(X)$. □

(4.4) Observation. Betragt et polynomium $\varphi(X) \neq 0$ i $\mathbb{Q}[X]$. Koefficienterne forskellige fra 0 er endelig mange brøker. De kan skrives med en fælles nævner s. Det følger så, at polynomiet $f(X) := s\varphi(X)$ har hele koefficienter. Er d den største fælles divisor for koefficienterne i $f(X)$, får vi altså en fremstilling,

$$\varphi(X) = \frac{d}{s}g(X), \tag{4.4.1}$$

hvor $g(X)$ er et primitivt polynomium i $\mathbb{Z}[X]$. Da $\varphi(X) \neq 0$, er også $d \neq 0$. Brøken d/s kan desuden antages at være uforkortelig, dvs vi kan antage, at d og s er primiske hele tal.

(4.5) Gauss' Lemma. *Lad $h(X)$ være et primitivt polynomium i $\mathbb{Z}[X]$. Da gælder for ethvert polynomium $\varphi(X) \in \mathbb{Q}[X]$ med rationale koefficienter, at hvis produktet $\varphi(X)h(X)$ har hele koefficienter, så har $\varphi(X)$ hele koefficienter.*

Bevis. Antag, at produktet $f(X) := \varphi(X)h(X)$ har hele koefficienter. Påstanden er triviel, hvis $\varphi(X) = 0$, så vi kan antage $\varphi(X) \neq 0$. Betragt en fremstilling $\varphi(X) = (d/s)g(X)$ af formen (4.4.1), hvor brøken d/s er uforkortelig og $g(X) \in \mathbb{Z}[X]$ er et primitivt polynomium. Vi vil bevise, at $s = \pm 1$, idet det så fremgår, at $\varphi(X) = \pm dg(X)$ har hele koefficienter.

Beviset er indirekte. Vi antager, at $s \neq \pm 1$. Følgelig findes et primtal p, der er divisor i s. Da d og s er primiske, er p ikke divisor i d. Af $f(X) = \varphi(X)h(X)$ og $\varphi(X) = (d/s)g(X)$ får vi ligningen,

$$sf(X) = dg(X)h(X).$$

Primtallet p går op i s og dermed i venstresiden. Men p går ikke op i d, og p går ikke op i $g(X)$ eller i $h(X)$, da disse polynomier er primitive. Lemma (4.3) giver nu den ønskede modstrid. □

(4.6) Korollar. *Lad $f(X) = a_0 + a_1X + \cdots + a_nX^n$ være et polynomium med hele koefficienter a_i, hvor $a_n \neq 0$. Antag, at $f(X)$ har en rational rod, skrevet som uforkortelig brøk r/s. Da er r divisor i a_0 og s er divisor i a_n.*

Bevis. Polynomiet $f(X)$ ligger i $\mathbb{Z}[X]$ og dermed i $\mathbb{Q}[X]$. Da brøken $r/s \in \mathbb{Q}$ er rod i $f(X)$, følger det af Sætning (3.4), at $f(X)$ i $\mathbb{Q}[X]$ er deleligt med polynomiet $X - r/s$. I $\mathbb{Q}[X]$ er $f(X)$ derfor også deleligt med $s(X - r/s) = sX - r$. Der findes altså en fremstilling,

$$f(X) = (sX - r)\varphi(X), \tag{1}$$

hvor $\varphi(X)$ er et polynomium i $\mathbb{Q}[X]$. På venstresiden har polynomiet $f(X)$ hele koefficienter. I den første faktor på højresiden er s og r primiske hele tal. Polynomiet $sX - r$ er derfor primitivt. Af Gauss' Lemma følger derfor, at polynomiet $\varphi(X)$ har hele koefficienter.

Det følger af ligningen (1), at den ledende koefficient i $f(X)$, altså tallet a_n, er lig med produktet af s og den ledende koefficient i $\varphi(X)$. Altså er s divisor i a_n. Tilsvarende er a_0 lig med produktet af $-r$ og konstantleddet i $\varphi(X)$. Altså er r divisor i a_0. □

(4.7) Korollar. *Antag, at et polynomium $h(X) \neq 0$ med hele koefficienter er et produkt $h(X) = \varphi(X)\psi(X)$ af polynomier $\varphi(X)$ og $\psi(X)$ med rationale koefficienter. Da findes et rationalt tal d/s forskelligt fra 0 således, at i ligningen,*

$$h(X) = \big(\tfrac{s}{d}\varphi(X)\big)\big(\tfrac{d}{s}\psi(X)\big), \tag{4.7.1}$$

har begge faktorer på højresiden hele koefficienter. Antages yderligere, at begge polynomier $\varphi(X)$ og $\psi(X)$ i fremstillingen $h(X) = \varphi(X)\psi(X)$ er normerede, så har de begge hele koefficienter.

Bevis. Af den givne ligning $h(X) = \varphi(X)\psi(X)$ følger, at ligningen (4.7.1) gælder for ethvert rationalt tal d/s forskelligt fra 0. Som nævnt i (4.4) kan d/s vælges således, at $\frac{s}{d}\varphi(X)$ er et primitivt polynomium i $\mathbb{Z}[X]$. Af Gauss' Lemma følger så, at også den anden faktor ligger i $\mathbb{Z}[X]$.

Antag yderligere, at $\varphi(X)$ og $\psi(X)$ normerede, og vælg d/s som ovenfor. Specielt er så begge brøker d/s og s/d hele tal, da de er de ledende koefficienter i de to faktorer. Derfor er begge brøker lig med ± 1. Multipliceres om nødvendigt begge faktorer med -1, kan det antages at begge brøker er lig med 1. De to faktorer er så $\varphi(X)$ og $\psi(X)$, som altså har hele koefficienter. □

(4.8) Korollar. *Et konstant polynomium i $\mathbb{Z}[X]$ er irreducibelt, hvis og kun hvis konstanten er $\pm p$, hvor p er et primtal. Et polynomium $h(X) \in \mathbb{Z}[X]$ af positiv grad er irreducibelt i $\mathbb{Z}[X]$, hvis og kun hvis $h(X)$ er et primitivt polynomium og irreducibelt i $\mathbb{Q}[X]$.*

Bevis. Den første påstand har vi allerede observeret i (4.2).

Antag nu, at $h(X) \in \mathbb{Z}[X]$ er et polynomium af positiv grad. Hvis $h(X)$ ikke er primitivt, så har $h(X)$ i $\mathbb{Z}[X]$ en ikke-triviel faktorisering $h = dg(X)$, hvor tallet d er en ikke-triviel fælles divisor for koefficienterne i $h(X)$. Vi kan derfor antage, at $h(X)$ er et primitivt polynomium. Det skal vises, at $h(X)$ er irreducibelt i $\mathbb{Z}[X]$, hvis og kun hvis $h(X)$ er irreducibelt i $\mathbb{Q}[X]$.

Hvis $h(X)$ har en ikke-triviel faktorisering $h(X) = f(X)g(X)$ i $\mathbb{Z}[X]$, så må begge faktorer have positiv grad, fordi $h(X)$ er primitivt. Faktoriseringen er altså en ikke-triviel faktorisering i $\mathbb{Q}[X]$. Antag omvendt, at $h(X)$ har en ikke-triviel faktorisering $h(X) = \varphi(X)\psi(X)$ i $\mathbb{Q}[X]$. Da har begge faktorer positiv grad. Det følger af Korollar (4.7), at vi ud fra denne faktorisering kan opnå en faktorisering af $h(X)$, hvor de to faktorer ligger i $\mathbb{Z}[X]$; de to faktorer har samme grad som de oprindelige. Hermed er opnået en ikke-triviel faktorisering af $h(X)$ i $\mathbb{Z}[X]$.

Hermed er korollaret bevist. ▯

(4.9) Eisenstein's Irreducibilitetskriterium. *Lad $h(X) = c_nX^n + c_{n-1}X^{n-1} + \cdots + c_0$ være et primitivt polynomium af positiv grad i $\mathbb{Z}[X]$. Antag, at der findes et primtal p således, at p går op i $c_{n-1}, \dots, c_0$ og p^2 ikke går op i c_0. Da er $h(X)$ irreducibelt i $\mathbb{Z}[X]$ og i $\mathbb{Q}[X]$.*

Bevis. Da $h(X)$ er primitivt, følger det af forudsætningerne, at p ikke går op i c_n. Ifølge Korollar (4.8) er det derfor nok at vise, at $h(X)$ er irreducibelt i $\mathbb{Z}[X]$. Da $h(X)$ er primitivt, er det nok at vise, at $h(X)$ ikke kan fremstilles som et produkt $h(X) = f(X)g(X)$, hvor polynomierne $f(X)$ og $g(X)$ ligger i $\mathbb{Z}[X]$ og er af lavere grad end $h(X)$.

Betragt hertil en faktorisering $h(X) = f(X)g(X)$, hvor polynomierne $f(X)$, $g(X)$ ligger i $\mathbb{Z}[X]$, altså en fremstilling,

$$h(X) = f(X)g(X) = (a_kX^k + \cdots + a_0)(b_lX^l + \cdots + b_0), \tag{1}$$

hvor $k + l = n$ og koefficienterne a_i og b_j ligger i $\mathbb{Z}$. Det skal vises, at $k = n$ eller $l = n$.

Konstantleddet c_0 i $h(X)$ er produktet a_0b_0. Da p^2 ikke går op i c_0, slutter vi, at a_0 og b_0 ikke begge kan være delelige med p. Vi kan antage, at p ikke går op i a_0.

Vi anvender nu homomorfien $\mathbb{Z}[X] \to (\mathbb{Z}/p)[X]$, som afbilder et polynomium $k(X)$ i $\mathbb{Z}[X]$ på det polynomium $\bar{k}(X)$ i $(\mathbb{Z}/p)[X]$, der fremkommer ved at erstatte koefficienterne i $k(X)$ med deres restklasser modulo p. Af ligningen $h(X) = f(X)g(X)$ får vi i $(\mathbb{Z}/p)[X]$ ligningen $\bar{h}(X) = \bar{f}(X)\bar{g}(X)$. Det følger af forudsætningerne, at $\bar{c}_i = 0$ for $i = 0, \dots, n-1$. Vi har altså $\bar{h}(X) = \bar{c}_nX^n$. Vi har antaget, at p ikke går op i a_0, så $\bar{a}_0 \neq 0$. Vi kan ikke have $\bar{b}_j = 0$ for alle j, thi da ville $g(X)$, og dermed $h(X)$, være delelig med p. Lad $\bar{b}_m$ være den første af koefficienterne $\bar{b}_0, \bar{b}_1, \dots, \bar{b}_l$, som ikke er 0. Af (1) får vi ligningen i $(\mathbb{Z}/p)[X]$,

$$\bar{c}_nX^n = (\bar{a}_kX^k + \cdots + \bar{a}_0)(\bar{b}_lX^l + \cdots + \bar{b}_mX^m). \tag{2}$$

Multiplikationen på højresiden giver leddet $\bar{a}_0\bar{b}_mX^m$, som ikke er 0, samt eventuelt yderligere led. På venstresiden er der kun det ene led $\bar{c}_nX^n$. Altså er $m = n$. Da $m \leqslant l \leqslant n$, følger det, at $l = n$.

Det er således vist, at i faktoriseringen $h(X) = f(X)g(X)$ har faktoren $g(X)$ samme grad som $h(X)$, hvormed beviset er fuldført. ▯

(4.10) Eksempel. Kriteriet kan fx anvendes på polynomiet $h(X) := X^n + 2$ (for $n \geqslant 1$) med $p := 2$. Det følger, at polynomiet $X^n + 2$ er irreducibelt i $\mathbb{Z}[X]$ og i $\mathbb{Q}[X]$. I $\mathbb{Q}[X]$ findes altså irreducible polynomier af enhver positiv grad.

Som yderligere eksempel vil vi vise, at polynomiet $f(X) = X^{p-1} + \cdots + X + 1$, hvor p er et givet primtal, er irreducibelt i $\mathbb{Q}[X]$. Vi kan naturligvis ikke umiddelbart anvende (4.9). Betragt i stedet polynomiet $f(X+1)$, der fås af $f(X)$ ved at indsætte $X+1$. Fra en faktorisering $f(X) = g(X)h(X)$ fås en faktorisering $f(X+1) = g(X+1)h(X+1)$, og omvendt, af en faktorisering $f(X+1) = \hat{g}(X)\hat{h}(X)$ får vi en faktorisering $f(X) = \hat{g}(X-1)\hat{h}(X-1)$. Det følger let, at $f(X)$ er irreducibelt, hvis og kun hvis $f(X+1)$ er irreducibelt.

For polynomiet $f(X)$ har vi ligningen,

$$f(X)(X-1) = X^p - 1.$$

Ved indsættelse af $X+1$ får vi derfor ligningen,

$$f(X+1)X = (X+1)^p - 1 = \sum_{i=1}^{p} \binom{p}{i} X^i,$$

som ved division med X giver ligningen,

$$f(X+1) = p + \binom{p}{2} X + \cdots + \binom{p}{p-1} X^{p-2} + X^{p-1}.$$

Polynomiet $f(X+1)$ har grad $p-1$, og den ledende koefficient er 1. De øvrige koefficienter, af grad mindre end $p-1$, er binomialkoefficienterne $\binom{p}{j}$, for $j = 1, \ldots, p-1$, som øjensynlig alle er delelige med primtallet p. Konstantleddet er $\binom{p}{1} = p$, der ikke er deleligt med p^2. Følgelig er forudsætningerne i Eisenstein's kriterium opfyldt for $f(X+1)$. Det følger, at polynomiet $f(X)$ er irreducibelt i $\mathbb{Q}[X]$.

Bemærk, at forudsætningen om at p er et primtal, er væsentlig. Fx er $X^3 + X^2 + X + 1$ ikke irreducibelt i $\mathbb{Q}[X]$, idet

$$X^3 + X^2 + X + 1 = (X+1)(X^2+1).$$

(4.11) Bemærkning. Resultaterne i dette kapitel hører naturligt hjemme i en ramme, der omfatter teorien for faktorielle ringe. For det første følger det nemlig, at polynomiumsringen $\mathbb{Z}[X]$ er en faktoriel ring.

Det skal hertil vises, at hvert polynomium $f(X)$ i $\mathbb{Z}[X]$, som ikke er nul og ikke er en invertibel konstant, kan skrives som produkt af irreducible polynomier. Desuden skal det vises, for ringen $\mathbb{Z}[X]$, at hvert irreducibelt polynomium er et primelement. Det første har vi allerede observeret i (4.2). For at vise det andet antages, at $h(X)$ er et irreducibelt polynomium i $\mathbb{Z}[X]$ og at $h(X)$ er divisor i et produkt $f(X)g(X)$. Det skal vises, at $h(X)$ er divisor i en af faktorerne. Hvis $h(X)$ er konstant, må konstanten være $\pm p$, hvor p er et primtal; i dette tilfælde er påstanden indholdet af Lemma (4.3). Antag, at $h(X)$ har positiv grad. Ifølge Korollar (4.8) er $h(X)$ et primitivt polynomium og $h(X)$ er irreducibelt i $\mathbb{Q}[X]$. Da $\mathbb{Q}$ er et legeme, er $\mathbb{Q}[X]$ en faktoriel ring, og $h(X)$ er derfor et primelement i $\mathbb{Q}[X]$. Det følger derfor, at $h(X)$, i ringen $\mathbb{Q}[X]$, er divisor i en af faktorerne $f(X)$ eller $g(X)$. Vi kan antage, at $h(X)$ er divisor i $f(X)$, altså at der findes en fremstilling $f(X) = \varphi(X)h(X)$ med et polynomium $\varphi(X)$. Af Gauss' Lemma (4.5) følger, at $\varphi(X)$ ligger i $\mathbb{Z}[X]$. Altså er $h(X)$, i ringen $\mathbb{Z}[X]$, divisor i $f(X)$.

For det andet er det ikke svært at se, at alle de foregående resultater (bortset fra eksemplerne) bevarer deres gyldighed, når ringen $\mathbb{Z}$ erstattes med en vilkårlig faktoriel ring R og legemet $\mathbb{Q}$ erstattes med brøklegemet for R. Specielt gælder altså følgende resultat:

Gauss' Sætning. *Hvis R er en faktoriel ring, så er også polynomiumsringen $R[X]$ en faktoriel ring.*

For polynomiumsringen $R[X_1, \dots, X_r]$ i r variable har vi ligheden,

$$R[X_1, \dots, X_r] = R[X_1, \dots, X_{r-1}][X_r].$$

Induktivt følger det derfor af Gauss' Sætning, at hvis R er en faktoriel ring, så er også polynomiumsringen $R[X_1, \dots, X_r]$ en faktoriel ring. Fx er $\mathbb{Z}[X_1, \dots, X_r]$ en faktoriel ring og, når L er et legeme, er $L[X_1, \dots, X_r]$ en faktoriel ring.

(4.12) Opgaver.

1. Hvilke konstante polynomier i $\mathbb{Z}[X]$ er primitive? Er et konstant, primitivt polynomium irreducibelt?

2. Angiv et polynomium $f(X)$ i $\mathbb{Z}[X]$ således, at $f(X)$ er irreducibel i $\mathbb{Z}[X]$, men ikke i $\mathbb{Q}[X]$. Og angiv $g(X)$ således, at $g(X)$ er irreducibel i $\mathbb{Q}[X]$, men ikke i $\mathbb{Z}[X]$.

3. Angiv, i $\mathbb{Z}[X]$, primopløsningen af $X^4 + 4X^3 + 6X^2 + 4X + 1$.

4. Angiv, i $\mathbb{Z}[X]$, primopløsningen af $2X^3 - 3X^2 + 1$.

5. Vis, at polynomiet $f_n(X) = X^{n-1} + \cdots + X + 1$ er reducibelt, når n ikke er et primtal.

6. Vis, for et primtal p, at idealet (p, X) i $\mathbb{Z}[X]$, bestående af alle polynomier af formen $pf + Xg$, ikke er et hovedideal. Vis, at idealet er et maksimalideal.

7. *Lad f være et heltalspolynomium. Antag, at konstantleddet er et primtal p, og at de nummeriske værdier af de øvrige koefficienter har sum mindre end p. Vis, at f er irreducibel i $\mathbb{Z}[X]$.

5. Adjunktion af rod.

(5.1) Indledning. En vigtig konstruktion i algebra er dannelsen af en kvotientring $A = R[X]/\mathfrak{I}$ af polynomiumsringen $R[X]$ modulo et givet ideal $\mathfrak{I}$. Det er klart, at kvotientringen A altid er en kommutativ ring. Vi vil her betragte konstruktionen i tilfældet, hvor $\mathfrak{I}$ er hovedidealet (d) frembragt af et givet normeret polynomium i $R[X]$ af positiv grad n,

$$d = X^n + d_{n-1}X^{n-1} + \cdots + d_1X + d_0.$$

Idealet $\mathfrak{I} = (d)$ består altså af alle polynomier af formen qd for $q \in R[X]$. Elementerne i kvotientringen $A := R[X]/(d)$ er ækvivalensklasser af polynomier: to polynomier f og g er ækvivalente, hvis differensen $f - g$ har formen qd med $q \in R[X]$.

Konstruktionen kan blandt andet anvendes til at konstruere legemer, og vi giver en række eksempler.

(5.2) Observation. Lad $f \mapsto \bar{f}$ betegne den kanoniske homomorfi af $R[X]$ ind i kvotienten A. For $a \in R$ betegnes med $\overline{a}$ ækvivalensklassen, der indeholder det konstante polynomium a. Afbildningen $a \mapsto \overline{a}$ er sammensat af inklusionshomomorfien af R ind i $R[X]$ og den kanoniske homomorfi af $R[X]$ på kvotientringen A. Følgelig er afbildningen en homomorfi $R \to A$. Dens kerne består kun af nul-elementet i R. At $\overline{a} = 0$, betyder nemlig, at det konstante polynomium a har formen qd; da d ifølge antagelsen har positiv grad, har qd grad mindst 1, med mindre q er nul-polynomiet. Ligningen $a = qd$ for et konstant polynomium a medfører derfor, at $a = 0$.

Da kernen for homomorfien $a \mapsto \overline{a}$ kun består af 0, er homomorfien injektiv. Vi kan derfor identificere elementerne a i R med deres billeder i A, og vi skriver blot a for $\overline{a}$. Med denne identifikation opfatter vi den givne ring R som delring af kvotientringen A.

(5.3) Struktur af polynomiumskvotient. *Betragt under forudsætningerne i* (5.1) *kvotientringen $A := R[X]/(d)$ med delringen R. Lad*

$$\xi := \overline{X} \in A$$

betegne ækvivalensklassen af X modulo hovedidealet (d). Da har hver ækvivalensklasse $\alpha \in A$ en fremstilling,

$$\alpha = r_0 + r_1\xi + \cdots + r_{n-1}\xi^{n-1}, \tag{5.3.1}$$

med entydigt bestemte elementer $r_0, \dots, r_{n-1}$ i delringen R. Yderligere gælder i kvotientringen A ligningen,

$$\xi^n = -d_0 - d_1\xi - \cdots - d_{n-1}\xi^{n-1}. \tag{5.3.2}$$

Bevis. Betragt et polynomium $f = a_0 + a_1X + \cdots + a_kX^k$ i $R[X]$. Den kanoniske homomorfi $f \mapsto \bar{f}$ er en ringhomomorfi $R[X] \to A$. Vi får derfor ligningerne,

$$\bar{f} = \overline{a_0 + a_1X + \cdots + a_kX^k} = \bar{a}_0 + \bar{a}_1\overline{X} + \cdots + \bar{a}_k\overline{X}^k = a_0 + a_1\xi + \cdots + a_k\xi^k,$$

hvor den sidste ligning følger af definitionen af ξ og identifikationen af ækvivalensklassen $\bar{a}$ med elementet a i R. Det fremgår, at billedet $\bar{f} \in A$ fås ved at indsætte elementet ξ i polynomiet f.

Det følger, at elementerne på højresiden af (5.3.1) netop er de ækvivalensklasser, der fremkommer ved at indsætte ξ i polynomier af grad mindre end n. Hver ækvivalensklasse α i A har formen $\bar{f}$ med et polynomium f. Den første påstand, om eksistens og entydighed af fremstillingen (5.3.1) udsiger altså, at hvert polynomium f modulo idealet (d) er ækvivalent med netop et polynomium r af grad mindre end n. At dette gælder, er netop indholdet af Sætningen om division med rest (2.1).

Ligningen (5.3.2) er ækvivalent med ligningen $d(\xi) = 0$, altså ækvivalent med, at $\bar{d}$ er nul-elementet i kvotientringen A. Vi har $\bar{f} = 0$, hvis og kun hvis f ligger i det givne ideal (d). Specielt er altså $\bar{d} = 0$.

Hermed er de to påstande bevist. □

(5.4) Regning i kvotienten. Struktursætningen fortæller, hvordan man „regner" i kvotientringen $A = R[X]/(d)$. For det første følger det, at elementerne α i kvotientringen A svarer til n-sæt $(r_0, \dots, r_{n-1})$ af elementer i R. Vi kan altså identificere A med produktmængden R^n. Under denne identifikation svarer addition i ringen A øjensynlig til koordinatvis addition i R^n. Den additive gruppe i ringen A er altså isomorf med produktet R^n.

Multiplikation i ringen A svarer under identifikationen til en komposition i mængden R^n. Specielt svarer multiplikation af elementer i delringen R og elementer i A til en ydre komposition $R \times R^n \to R^n$. Øjensynlig multipliceres et n-sæt i R^n med $a \in R$ ved at multiplicere med a på alle koordinater. Specielt ses, at når ringen R er et legeme, så er kvotientringen A naturligt et vektorrum over R, med en basis bestående af de n potenser $1, \xi, \dots, \xi^{n-1}$, og identifikationen af A og R^n er en isomorfi af vektorrum over R.

Multiplikationen i ringen A er bestemt af den anførte ligning (5.3.2). Af ligningen følger nemlig først, at

$$\xi^{n+1} = \xi^n \xi = -d_0\xi - d_1\xi^2 - \cdots - d_{n-2}\xi^{n-1} - d_{n-1}\xi^n,$$

og bruges ligningen igen, kan $-d_{n-1}\xi^n$ skrives som „linearkombination" af de n potenser $1, \xi, \dots, \xi^{n-1}$. Induktivt får vi fremstillinger af alle potenser $\xi^{n+1}, \xi^{n+2}, \dots$ som „linearkombinationer" af $1, \xi, \dots, \xi^{n-1}$. Disse fremstillinger af ξ^i, for $i = 0, \dots, 2n-2$ fortæller så, hvordan vilkårlige to elementer i A med fremstillinger af formen (5.3.1) skal multipliceres, eller, ækvivalent, hvordan to n-sæt i R^n skal multipliceres.

(5.5) Definition. Under forudsætningerne i Struktursætningen er R en delring af ringen $A = R[X]/(d)$. Det fremgår af ligningen (5.3.2), at det givne polynomium d i A har det specielle element ξ som rod. For et givet normeret polynomium $d \in R[X]$ giver konstruktionen altså en ring A, der har R som delring, og hvori d har en rod. Man siger også, at ringen A fremkommer af R ved *formelt at adjungere* en rod i polynomiet d.

(5.6) De komplekse tal. Betragt polynomiet $d := X^2 + 1$ i $\mathbb{R}[X]$. Det har graden $n = 2$. Ved formel adjunktion af en rod i $X^2 + 1$ fremkommer en ring A, der har $\mathbb{R}$ som delring, og hvori $X^2 + 1$ har en rod ξ. Elementerne α i A har formen,

$$\alpha = a + b\xi, \tag{5.6.1}$$

med entydigt bestemte $a, b \in \mathbb{R}$. At ξ er rod i $X^2 + 1$ betyder, at

$$\xi^2 = -1. \tag{5.6.2}$$

Det er herefter klart, at ringen A er det velkendte legeme $\mathbb{C}$ af komplekse tal, idet ξ identificeres med den komplekse enhed i. Alternativt kan vi opfatte konstruktionen af ringen A som *definitionen* af de komplekse tal. Det er et velkendt regnestykke, at A er et legeme: For α af formen (5.6.1) sættes $\bar{\alpha} := a - b\xi$. Under brug af (5.6.2) får vi så, at

$$\alpha\bar{\alpha} = a^2 + b^2.$$

Hvis $\alpha \neq 0$, så er enten a eller b forskellig fra 0, og så er $a^2 + b^2 > 0$. Vi kan derfor betragte $1/(a^2 + b^2) \in \mathbb{R}$, og udregningen ovenfor viser, at $\alpha[\bar{\alpha}/(a^2 + b^2)] = 1$. Hvert $\alpha \neq 0$ i A er derfor invertibelt, med $\bar{\alpha}/(a^2 + b^2)$ som den inverse.

Vi kan naturligvis også opfatte $X^2 + 1$ som polynomium i $\mathbb{C}[X]$. Adjungerer vi formelt en rod, får vi en ring B, der indeholder $\mathbb{C}$ som delring og indeholder en rod η i $X^2 + 1$. Hvert element α i B har en entydig fremstilling af formen (5.6.1), vel at mærke med komplekse tal a og b. Det skal understreges, at den konstruerede ring B *ikke* er et legeme. Fx gælder i B, at $(1 + i\eta)(1 - i\eta) = 1 - i^2\eta^2 = 0$. Altså gælder nul-reglen ikke i B.

(5.7) Eksempel. Betragt $d = X^2 + 1$ som polynomium i $\mathbb{F}_3[X]$, og adjunger formelt en rod. Herved fremkommer en ring A, der har $\mathbb{F}_3$ som delring, og hvori $X^2 + 1$ har en rod ξ. Hvert element $\alpha \in A$ har en fremstilling af formen (5.6.1), med $a, b \in \mathbb{F}_3$, og i A gælder ligningen (5.6.2). Der er 3 elementer i $\mathbb{F}_3$, nemlig restklasserne $0, 1, -1$. Der er følgelig $3 \cdot 3$ muligheder for (a, b). Ringen A indeholder altså 9 elementer.

Ringen A er et legeme. Argumentet er ganske som i (5.6), blot med $\mathbb{R}$ erstattet af $\mathbb{F}_3$: Det skal vises, at når to elementer $a, b \in \mathbb{F}_3$ ikke begge er 0, så er $a^2 + b^2 \neq 0$. Legemet $\mathbb{F}_3$ indeholder tre elementer $0, \pm 1$, og kvadraterne er følgelig $0, 1$. Det ses, at en sum af to kvadrater $a^2 + b^2$ kun bliver 0, hvis $a = b = 0$.

Den konstruerede ring, $\mathbb{F}_3[X]/(X^2 + 1)$, er altså et legeme med 9 elementer. Det betegnes ofte $\mathbb{F}_9$.

(5.8) Konstruktion af legemer. Antag, at ringen R er et legeme L. Det følger af Hovedidealsætningen (2.6), at hvert ideal i $L[X]$ er et hovedideal. Nul-polynomiet 0 frembringer det trivielle hovedideal (0). Et ideal forskelligt fra (0) er altså et hovedideal (d) frembragt af et polynomium $d \neq 0$. Hvis u er den ledende koefficient i d, så er $u^{-1}d$ et normeret polynomium, og det frembringer det samme hovedideal. Specielt ses, at de konstante polynomier forskellige fra 0 frembringer det trivielle hovedideal $(1) = L[X]$. De ikke-trivielle idealer i $L[X]$ er altså netop hovedidealerne (d) frembragt af et normeret polynomium d af positiv grad. Struktursætningen (5.3) omhandler således alle kvotientringe af $L[X]$ modulo ikke-trivielle idealer. Det er ofte nyttigt at kombinere Struktursætningen med det efterfølgende resultat.

Lemma. *Lad f være et irreducibelt polynomium i $L[X]$. Da er hovedidealet (f) et maksimalideal i $L[X]$, og følgelig er kvotientringen $A := L[X]/(f)$ et legeme.*

Bevis. Da f er irreducibelt, er f specielt ikke invertibelt i $L[X]$. Hovedidealet (f) indeholder derfor ikke polynomiet 1, og følgelig er (f) et ægte ideal. For at vise, at (f) er et maksimalideal, skal det vises, at intet ægte ideal $\mathfrak{I}$ i $L[X]$ er større end (f). Antag hertil, at $\mathfrak{I}$ er et ægte ideal, og at

$$(f) \subseteq \mathfrak{I}. \tag{1}$$

Som nævnt ovenfor er $\mathfrak{I}$ et hovedideal, $\mathfrak{I} = (d)$, frembragt af et polynomium d. Polynomiet d er forskelligt fra 0, fordi $f \in (d)$ og $f \neq 0$. Videre er d ikke en konstant forskellig fra 0, fordi (d) er et ægte ideal. Da $f \in (d)$, findes et polynomium $q \in L[X]$ så at $f = qd$. Da f kun har trivielle divisorer, og d har positiv grad, følger det, at q må være en konstant forskellig fra 0. Vi har derfor ligningen $d = q^{-1}f$, og det følger først, at $d \in (f)$ og dernæst, at $(d) \subseteq (f)$. Da $\mathfrak{I} = (d)$, må inklusionen i (1) altså være en lighed.

Hermed er vist, at (f) er et maksimalideal i $L[X]$. Det er velkendt, at kvotientringen $L[X]/(f)$ så er et legeme. □

(5.9) Endelige legemer. Lad p være et primtal og betragt legemet $\mathbb{F}_p$, altså restklasseringen $\mathbb{Z}/p$ med p elementer. Lad $d \in \mathbb{F}_p[X]$ være et normeret polynomium af grad $n \geqslant 1$. Formel adjunktion af en rod i d giver så en kvotientring $A = \mathbb{F}_p[X]/(d)$, hvori hvert element har en entydig fremstilling af formen (5.3.1) med $r_0, \dots, r_{n-1}$ i $\mathbb{F}_p$. Der er p muligheder for hvert r_i, og der er derfor p^n elementer i kvotientringen A. Hvis d er et irreducibelt polynomium, følger det af (5.8), at A er et legeme.

Man kan vise, at der for hvert $n \geqslant 1$ findes irreducible polynomier af grad n i $\mathbb{F}_p[X]$. For enhver primtalspotens p^n findes altså et endeligt legeme med p^n elementer. Man kan vise, at antallet af elementer i et endeligt legeme altid er en primtalspotens, og at to endelige legemer med samme antal elementer altid er isomorfe.

(5.10) Eksempel. Betragt polynomiet $d = X^3 + X + 1$ i $\mathbb{F}_2[X]$, og adjunger formelt en rod. Herved fremkommer en ring A, der indeholder $\mathbb{F}_2$ som delring. Hvert element α i A kan skrives på formen,

$$\alpha = a + b\xi + c\xi^2, \tag{5.10.1}$$

med entydigt bestemte $a, b, c \in \mathbb{F}_2$. Ringen A har altså $2^3 = 8$ elementer. Regning med elementer i A foregår ved brug af ligningerne,

$$\xi^3 = 1 + \xi, \quad \xi^4 = \xi + \xi^2,$$

hvor den første ligning blot er (5.3.2) og den anden følger af den første ved multiplikation med ξ.

Polynomiet d er irreducibelt, idet det har grad 3 og ingen af de to elementer i $\mathbb{F}_2$ øjensynlig er rod i d. Følgelig er A et legeme med 8 elementer; det betegnes også $\mathbb{F}_8$.

(5.11) Opgaver.

1. Konstruer et legeme med 25 elementer.

2. Legemet $\mathbb{F}_8$ består af alle elementer $a + b\xi + c\xi^2$, hvor $a, b, c \in \mathbb{F}_2$ og $\xi^3 = 1 + \xi$. Vis, for hvert af de 7 elementer $\alpha \in \mathbb{F}_8^*$, at $\alpha^7 = 1$.

3. *Lad L være et legeme, og lad $f \in L[X]$ være et polynomium af grad $n \geqslant 1$. Vis, at der findes et legeme K, med L som dellegeme, således, at f har n rødder (med multiplicitet) i K. [Vink: vælg et irreducibelt polynomium d, som er divisor i f, og start med formel adjunktion af en rod i d.]

6. Kvaternioner.

(6.1). Matrixringen $\mathrm{Mat}_2(\mathbb{C})$ indeholder som bekendt kvaterniongruppen bestående af 8 matricer, nemlig de 4 matricer,

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{i} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \mathbf{j} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix},$$

og deres 4 modsatte matricer, $-\mathbf{1}$, $-\mathbf{i}$, $-\mathbf{j}$, og $-\mathbf{k}$ (matricen $\mathbf{1}$ er enhedsmatricen og kunne blot betegnes med 1). Et produkt af vilkårlige to af disse matricer ligger igen i kvaterniongruppen, og er altså igen en af de 8 matricer. For at bestemme hvilken, er det faktisk nok at huske ligningerne,

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -\mathbf{1}.$$

Fx følger det af den sidste ligning ved at multiplicere med $-\mathbf{k}$ fra højre, at $\mathbf{ij} = \mathbf{k}$.

Skalarmatricerne i $\mathrm{Mat}_2(\mathbb{C})$ er matricerne af formen,

$$c\mathbf{1} = \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} \quad \text{med } c \in \mathbb{C};$$

de udgør en delring. Multiplikation af en matrix med matricen $c\mathbf{1}$ svarer til multiplikation med c på alle matricens pladser. Derfor kan man uden fare for misforståelser opfatte $\mathbb{C}$ som en delring af $\mathrm{Mat}_2(\mathbb{C})$, idet man identificerer $c \in \mathbb{C}$ med skalarmatricen $c\mathbf{1}$. Specielt kan legemet $\mathbb{R}$ opfattes som delringen $\mathbb{R} \subseteq \mathrm{Mat}_2(\mathbb{C})$ bestående af reelle skalarmatricer. Af de 8 matricer i kvaterniongruppen er det $\mathbf{1}$ og $-\mathbf{1}$, der er skalarmatricer.

Lad nu $\mathbb{H}$ være mængden af alle matricer $\alpha \in \mathrm{Mat}_2(\mathbb{C})$ af følgende form:

$$\alpha = a_0\mathbf{1} + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}, \quad a_0, a_1, a_2, a_3 \in \mathbb{R}. \tag{6.1.1}$$

Det er klart, at matricer af denne form udgør et vektorrum over $\mathbb{R}$; specielt er sum af to matricer af denne form igen af samme form. Som nævnt er produkt af vilkårlige to af de fire matricer $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ igen, borset fra fortegn, en af de disse fire matricer. Heraf følger let, at produkt af to matricer af formen (6.1.1) igen har samme form. Endvidere er $-\mathbf{1} \in \mathbb{H}$. Delmængden $\mathbb{H}$ er derfor en delring af $\mathrm{Mat}_2(\mathbb{C})$. Den er *ikke kommutativ*. Fx er $\mathbf{ij} = \mathbf{k}$ og $\mathbf{ji} = -\mathbf{k}$. Elementerne i $\mathbb{H}$ kaldes *kvaternioner*.

De reelle skalarmatricer, altså matricerne $c\mathbf{1}$ med $c \in \mathbb{R}$, er specielt kvaternioner. De reelle tals legeme kan altså opfattes som en delring,

$$\mathbb{R} \subseteq \mathbb{H}.$$

Udregning af linearkombinationen i (6.1.1) giver for α følgende matrix:

$$\alpha = a_0\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + a_1\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} + a_2\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} + a_3\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = \begin{bmatrix} a_0 + a_2 i & -a_1 + a_3 i \\ a_1 + a_3 i & a_0 - a_2 i \end{bmatrix}. \tag{6.1.2}$$

Specielt fremgår det, hvordan de 4 reelle koefficienter a_0, a_1, a_2, a_3 bestemmes ud fra matricen α. De fire kvaternioner $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ er altså lineært uafhængige, og udgør derfor en basis for vektorrummet af kvaternioner.

(6.2). For hver kvaternion $\alpha = a_0\mathbf{1} + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$ defineres den (*algebraiske*) *norm* som tallet,

$$\mathrm{N}(\alpha) := a_0^2 + a_1^2 + a_2^2 + a_3^2 = \det \alpha\,. \tag{6.2.1}$$

Ligheden af de to udtryk fremgår af udregningen (6.1.2). Det første udtryk viser, at tallet $\mathrm{N}(\alpha)$ er reelt og ikke-negativt, endda med $\mathrm{N}(\alpha) > 0$, når $\alpha \neq 0$. Af det andet udtryk følger, at normen er multiplikativ: For kvaternioner α, β gælder:

$$\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta). \tag{6.2.2}$$

Videre defineres for kvaternionen α den *konjugerede kvaternion* α^*:

$$\alpha^* := a_0\mathbf{1} - a_1\mathbf{i} - a_2\mathbf{j} - a_3\mathbf{k}. \tag{6.2.3}$$

En let udregning viser følgende ligninger:

$$\alpha\alpha^* = \alpha^*\alpha = \mathrm{N}(\alpha)\mathbf{1}. \tag{6.2.4}$$

(Det er nok at eftervise den anden ligning, idet den første, i formen $\alpha\alpha^* = \mathrm{N}(\alpha)\mathbf{1}$, så følger ved at erstatte a_ν med $-a_\nu$ for $\nu = 1, 2, 3$.) Hvis $\alpha \neq 0$, opnås følgende ligninger ved at multiplicere med skalaren $\mathrm{N}(\alpha)^{-1}$:

$$\alpha\,\frac{\alpha^*}{\mathrm{N}(\alpha)} = \frac{\alpha^*}{\mathrm{N}(\alpha)}\,\alpha = \mathbf{1}, \quad \text{når } \alpha \neq 0. \tag{6.2.5}$$

Altså er hver kvaternion $\alpha \neq 0$ invertibel (med $\alpha^* / \mathrm{N}(\alpha)$ som den inverse). Hermed er vist:

Delringen $\mathbb{H} \subseteq \mathrm{Mat}_2(\mathbb{C})$ af kvaternioner er et skævlegeme.

(6.3). Af udregningen (6.1.2) fremgår også, at udtrykt med de komplekse tal $a := a_0 + a_2 i$ og $b := a_1 + a_3 i$ kan kvaternionen α i (6.1.1) skrives

$$\alpha = \begin{bmatrix} a & -\bar{b} \\ b & \bar{a} \end{bmatrix}. \tag{6.3.1}$$

Alternativt kan kvaternionerne altså defineres som matricerne af denne form med $a, b \in \mathbb{C}$. For den konjugerede kvaternion fås:

$$\alpha^* = \begin{bmatrix} \bar{a} & \bar{b} \\ -b & a \end{bmatrix}.$$

Matricen på højresiden fås fra α ved at transponere og komplekst konjugere på de fire pladser. Dette kan naturligvis gøres med enhver kompleks matrix α; den fremkomne matrix kaldes så den *Hermitisk konjugerede* eller *adjungerede* til α, og den betegnes også i det generelle tilfælde med α^*. Transponering „vender" som bekendt matrixmultiplikation: $(\alpha\beta)^{\mathrm{tr}} = \beta^{\mathrm{tr}}\alpha^{\mathrm{tr}}$, og pladsvis kompleks konjugering vil trivielt „bevare" multiplikation: $\overline{\alpha\beta} = \bar{\alpha}\,\bar{\beta}$. Heraf følger for Hermitisk konjugering: $(\alpha\beta)^* = \beta^*\alpha^*$. Specielt gælder denne ligning altså for konjugering af kvaternioner:

$$(\alpha\beta)^* = \beta^*\alpha^*. \tag{6.3.2}$$

Videre fås for normen af kvaternionen α i (6.3.1):

$$\mathrm{N}(\alpha) = |a|^2 + |b|^2.$$

(6.4) Definition. En (ikke nødvendigvis kommutativ) ring A, som indeholder et legeme L som delring, kan specielt opfattes som vektorrum over L, idet multiplikation af en vektor α, dvs $\alpha \in A$, med en skalar c, dvs $c \in L$, blot er produktet $c\alpha$ i ringen A. At betingelserne for et vektorrum er opfyldt følger af betingelserne for addition og multiplikation i ringen A.

Hvis elementerne i L kommuterer med alle elementer i A, siger man, at A er en *algebra* over L (eller en L-*algebra*). Elementerne i L kaldes også *skalarer* i forhold til algebraen. Hvis A desuden er et skævlegeme, siger man, at A er en *divisionsalgebra* over L.

I praksis sidder legemet af skalarer ikke som en delring af algebraen A. I stedet er der givet en injektiv ringhomomorfi $\varphi\colon L \hookrightarrow A$ og ved hjælp af den „identificerer“ man skalaren $c \in L$ med elementet $\varphi(c) \in A$. I vektorrummet A er produktet $c\alpha$, af skalaren $c \in L$ med vektoren $\alpha \in A$, så bestemt ved

$$c\alpha := \varphi(c)\alpha.$$

Omvendt bestemmer denne ligning homomorfien φ, thi med $\alpha = 1_A$ fås

$$c1_A = \varphi(c).$$

En *homomorfi* mellem L-algebraer A og B er en afbildning $\mu\colon A \to B$, der både er en vektorrumshomomorfi (dvs en lineær afbildning) og en ringhomomorfi.

Polynomiumsringen $L[X]$ er en L-algebra af uendelig dimension. Den indeholder skalarerne som de konstante polynomier. En kvotientring $L[X]/(d)$, hvor d er et normeret n'tegradspolynomium, er en L-algebra; ifølge Struktursætningen (5.3) har den dimension n.

Matrixringen $\mathrm{Mat}_n(L)$ er en L-algebra, idet skalarerne i L er skalarmatricerne. Den har dimension n^2.

Over $\mathbb{R}$ udgør de reelle tal $\mathbb{R}$ en divisionsalgebra af dimension 1, de komplekse tal $\mathbb{C}$ udgør en divisionsalgebra af dimension 2, og kvaternionerne $\mathbb{H}$ udgør en divisionsalgebra af dimension 4.

(6.5) Evaluering. Lad A være en algebra over legemet L. Betragt i $L[X]$ et polynomium $f = c_nX^n + \cdots + c_1X + c_0$. Et element $\alpha \in A$ kan da *indsættes* i f: resultatet er elementet

$$f(\alpha) := c_n\alpha^n + \cdots + c_1\alpha + c_0 \in A;$$

man siger også, at $f(\alpha)$ fås ved at *evaluere* polynomiet f i α. Hvis $f(\alpha) = 0$, siges $\alpha \in A$ at være *rod* i f.

(6.6) Observation. *Evaluering i α, dvs afbildningen,*

$$\mathrm{Ev}_\alpha\colon L[X] \to A, \qquad f \mapsto f(\alpha),$$

er en homomorfi af L-algebraer, altså en lineær afbildning og en ringhomomorfi. Billedet er delalgebraen,

$$L[\alpha] := \{c_0 + c_1\alpha + \cdots + c_n\alpha^n \mid n \geqslant 0,\ c_0, \ldots, c_n \in L\},$$

bestående af alle linearkombinationer af potenserne $1, \alpha, \alpha^2, \dots,$ *og kernen er idealet i* $L[X]$ *bestående af polynomier med* α *som rod.*

For at indse, at evaluering er multiplikativ, bemærkes, at definitionen af produkt af to polynomier svarer til simple omformninger i en ring; det bruges specielt, at potenserne X^i kommuterer med koefficienterne i polynomierne. Det skal derfor blot bemærkes, at de samme omformninger med α indsat i de to polynomier fører til det element, der fås ved at indsætte α i produktpolynomiet; her bruges naturligvis, at α kommuterer med polynomiernes koefficienter, men det er jo en forudsætning i en L-algebra.

Det indses tilsvarende, at Ev_α er lineær, og altså specielt additiv. Endelig observeres, at et-elementet i $L[X]$, dvs et-elementet i L, afbildes på et-elementet i A.

Påstandene om billedet og kernen er umiddelbare konsekvenser af definitionen.

(6.7) Minimalt polynomium. Polynomier $c_0 + c_1X + \cdots + c_nX^n$ med α som rod svarer øjensynlig til lineære relationer,

$$c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0, \tag{6.7.1}$$

mellem potenserne $1, \alpha, \alpha^2, \dots$. At potenserne er lineært uafhængige, altså at der kun er de trivielle relationer med alle $c_\nu = 0$, betyder derfor, at α kun er rod i nul-polynomiet, altså at kernen for evaluering kun består af 0, eller, ækvivalent, at evalueringsafbildningen Ev_α er injektiv. Hvis det indtræffer, siges $\alpha \in A$ at være *transcendent* over L.

Hvis α ikke er transcendent over L, kaldes α *algebraisk* over L. Det betyder, at der findes en egentlig lineær relation (6.7.1) (ikke alle c_ν er lig med 0), eller ækvivalent, at kernen for evalueringsafbildningen Ev_α består af mere end 0.

Antag, at α er algebraisk over L. Kernen for evaluering er et ideal i $L[X]$, altså ifølge Hovedidealsætningen (2.6) et hovedideal (d), og da kernen består af mere end 0, er $d \neq 0$. Frembringeren d for idealet kan vælges normeret, og så er den entydigt bestemt. Dette entydigt bestemte polynomium kaldes det *minimale polynomium* for α over L.

Af bestemmelsen i beviset for Hovedidealsætningen (2.6) fremgår: Det minimale polynomium for α over L er bestemt som det normerede polynomium af mindst mulig grad med α som rod.

(6.8) Lemma. *Antag, at* D *er en divisionsalgebra, af endelig dimension over legemet* L. *Lad* α *være et element i* D. *Da er delalgebraen* $L[\alpha] \subseteq D$ *et legeme, og* α *algebraisk over* L. *Det minimale polynomium for* α *over* L *er et irreducibelt, normeret polynomium af grad lig med vektorrumsdimensionen* $\dim L[\alpha]$.

Bevis. Billedet ved evalueringsafbildningen, $L[\alpha] \subseteq D$, er en delring og et underrum, og $L[\alpha] \neq 0$, da D ikke er nul-ringen. Yderligere er billedringen kommutativ, fordi $L[X]$ er kommutativ. Betragt nu et element $\xi \neq 0$ i $L[\alpha]$, og multiplikation med ξ, altså $\eta \mapsto \xi\eta$ for $\eta \in L[\alpha]$; det er øjensynlig en lineær afbildning. Da nul-reglen gælder i D, gælder den specielt i delringen $L[\alpha]$; derfor er multiplikation med ξ en injektiv afbildning. Videre er $L[\alpha]$, som underrum af D, af endelig dimension. Multiplikation med ξ er således en injektiv, lineær afbildning i et endeligdimensionalt vektorrum; derfor er den bijektiv. Specielt er den surjektiv, så et-elementet ligger i billedet. Altså findes $\eta \in L[\alpha]$ med $\xi\eta = 1$. Derfor er ξ invertibel i $L[\alpha]$. Hermed er vist, at delringen $L[\alpha]$ er et legeme.

Dimensionen af $L[\alpha]$ er højst $N := \dim D$. Blandt flere end N potenser af α, fx $1, \alpha, \dots, \alpha^N$, må der følgerlig findes en egentlig lineær relation. Derfor er α algebraisk over L. Lad d være det minimale polynomium. Så har evalueringsafbildningen kernen (d). Ifølge Isomorfisætning for ringe findes derfor en isomorfi $L[X]/(d) \xrightarrow{\sim} L[\alpha]$. Da $L[\alpha]$ er et legeme, må altså også kvotienten $L[X]/(d)$ være et legeme. Som bekendt følger det så, at idealet (d) er et maksimalideal, og derefter videre, at d må været et irreducibelt polynomium. Endelig følger det af Struktursætningen (5.3), at $L[X]/(d)$ er et vektorrum af dimension lig med graden af d. Ifølge isomorfien har $L[\alpha]$ altså denne dimension. □

Mulighederne for d afhænger naturligvis af legemet L. Er fx $L = \mathbb{C}$, følger det som bekendt af algebraens fundamentalsætning, at de eneste irreducible polynomier er førstegradspolynomierne. Det minimale polynomium d må altså have formen $X - c$. At α er rod i dette polynomium, betyder, at $\alpha = c$. Konklusionen er altså, at hvis D er en endeligdimensional divisionsalgebra over $\mathbb{C}$, så er inklusionen $\mathbb{C} \subseteq D$ en lighed.

Som vi skal se, er der lidt flere muligheder for reelle divisionsalgebraer.

(6.9) Frobenius' Sætning. *Af endeligdimensionale divisionsalgebraer over* $\mathbb{R}$ *findes der på isomorfi nær kun* 3, *nemlig* $\mathbb{R}$ *selv af dimension* 1, *de komplekse tals legeme* $\mathbb{C}$ *af dimension* 2, *og kvaternionskævlegemet* $\mathbb{H}$ *af dimension* 4.

Bevis. Antag, at D er en endeligdimensional divisionsalgebra over $\mathbb{R}$. I inklusionen,

$$\mathbb{R} \subseteq D,$$

gælder lighed, præcis når $\dim_{\mathbb{R}} D = 1$; det er det første af de tre tilfælde. Antag derfor i det følgende, at inklusionen er skarp, og vælg et element $\iota \in D$ med $\iota \notin \mathbb{R}$. Betragt dellegemet

$$C := \mathbb{R}[\iota] \subseteq D.$$

Lad $d \in \mathbb{R}[X]$ være det minimale polynomium for ι. Da er ι rod i d, og d er normeret og irreducibelt i $\mathbb{R}[X]$. Heraf følger som bekendt, at d har grad 1 eller 2. I det første tilfælde har d formen $d = X - c$; at ι er rod, betyder, at $\iota = c \in \mathbb{R}$, hvad der ikke kan være tilfældet. Altså må graden være 2, så d har formen $d = (X-a)^2 + b^2$ med $b \neq 0$. At ι er rod, betyder, at $(\iota - a)^2 + b^2 = 0$; efter division med b^2 ses, at elementet $i := (\iota - a)/b$ opfylder, at

$$i^2 = -1.$$

Det er nu klart, at $C = \mathbb{R}[i] = \mathbb{R}[X]/(X^2+1)$ kan identificeres med legemet $\mathbb{C}$ af komplekse tal:

$$\mathbb{C} \subseteq D.$$

Øjensynlig gælder lighed i denne inklusion, hvis og kun hvis $\dim_{\mathbb{R}} D = 2$. Det er det andet af de tre tilfælde. Antag derfor i det følgende, at inklusionen er skarp.

Ved $s\colon \alpha \mapsto i\alpha i^{-1}$ defineres en afbildning $s\colon D \to D$. Øjensynlig er s multiplikativ og en $\mathbb{R}$-lineær afbildning, og s er en involution, dvs $s^2 = \mathrm{id}_D$. Derfor splitter D som vektorrum op i egenrum, $D = D^+ \oplus D^-$, hvor D^+ og D^- er egenrummene svarende til, henholdsvis, egenværdierne 1 og -1. Konkret er fremstillingen af α som sum af to egenvektorer givet ved ligningen $\alpha = (\alpha + s(\alpha))/2 + (\alpha - s(\alpha))/2$.

Egenrummet D^+ består af vektorerne $\alpha \in D$ med $s(\alpha) = \alpha$, altså $i\alpha i^{-1} = \alpha$, dvs $i\alpha = \alpha i$; det er de vektorer, som kommuterer med i. Elementerne i $\mathbb{R}$ kommuterer med alle elementer i D. Et element, som kommuterer med i, vil derfor kommutere med alle elementer af formen $a + ib$, for $a, b \in \mathbb{R}$, og dermed med alle elementer i $\mathbb{C}$. Altså består D^+ af de elementer i D, som kommuterer med alle elementer i $\mathbb{C}$; specielt er $\mathbb{C} \subseteq D^+$ og D^+ er en divisionsalgebra over $\mathbb{C}$. Af algebraens fundamentalsætning følger så, at $\mathbb{C} = D^+$.

Egenrummet D^- består af vektorerne $\alpha \in D$ med $s(\alpha) = -\alpha$, altså $i\alpha i^{-1} = -\alpha$, dvs $i\alpha = -\alpha i$. Da $D^+ = \mathbb{C} \subset D$, er $D^- \neq 0$. Der findes altså et element $j \neq 0$ i D^-. Elementet j ligger ikke i $\mathbb{R}$, så det minimale polynomium for j har grad 2. Derfor vil j opfylde en ligning af formen $(j - a)^2 + b^2 = 0$ med $a, b \in \mathbb{R}$, $b \neq 0$. Anvend afbildningen $s\colon \alpha \mapsto i\alpha i^{-1}$ på ligningen. Da s er en ringhomomorfi og $s(c) = c$ for $c \in \mathbb{R}$, fremkommer ligningen $(-j - a)^2 + b^2 = 0$. Trækkes den første ligning fra den anden, følger det, at $4aj = 0$. Altså er $a = 0$, og ligningen har formen $j^2 = -b^2$. Erstat j med j/b. Vi har stadig $j \in D^-$, dvs $ij = -ji$, og nu er

$$j^2 = -1.$$

Højremultiplikation med j, dvs $\alpha \mapsto \alpha j$, er bijektiv. Specielt har hvert element i D formen αj. Da afbildningen s er multiplikativ, er $s(\alpha j) = s(\alpha)s(j) = -s(\alpha)j$. Specielt ses, at

$$\alpha j \in D^- \iff \alpha \in D^+.$$

Her er $D^+ = \mathbb{C}$. Det følger altså, at $D^- = \mathbb{C}j$ består af alle elementer af formen zj for $z \in \mathbb{C}$, altså af alle elementer,

$$(a + bi)j = aj + bij, \quad \text{for } a, b \in \mathbb{R}.$$

Sættes $k = ij$, er elementerne j, k altså er $\mathbb{R}$-basis for D^-, og $1, i$ er en $\mathbb{R}$-basis for D^+. Derfor er $1, i, j, k$ en $\mathbb{R}$-basis for D. Da $j \in D^-$ er $ij = -ji$. Følgelig er $ijk = ijij = -i^2j^2 = (-1)^3 = -1$ og $k^2 = ijk = -1$. Alt i alt er altså

$$i^2 = j^2 = k^2 = ijk = -1.$$

Disse ligninger bestemmer multiplikationen i D, på samme måde som de tilsvarende ligninger i $\mathbb{H}$ for kvaternionenhederne $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$. Heraf ses, at den lineære isomorfi $D \xrightarrow{\sim} \mathbb{H}$, som afbilder $1, i, j, k$ på $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$, er en isomorfi mellem de to algebraer. □

(6.10) Opgaver.

1. Vis, at kvaternioner med norm 1 udgør en undergruppe af $\mathbb{H}^*$. Det er gruppen af *enhedskvaternioner*, betegnet $\mathbb{H}^*_1$.

2. Vis, at gruppen $\mathrm{U}_2(\mathbb{C}) \subseteq \mathrm{GL}_2(\mathbb{C})$ af unitære (2×2)-matricer er undergruppen bestående af matricerne af formen

$$\begin{bmatrix} a & -u\bar{b} \\ b & u\bar{a} \end{bmatrix}, \quad \text{med } |a|^2 + |b|^2 = 1, \quad |u| = 1.$$

Vis, for den specielle unitære gruppe $\mathrm{SU}_2(\mathbb{C})$ (bestående af unitære matricer med determinant 1), at $\mathrm{SU}_2(\mathbb{C}) = \mathbb{H}_1^*$.

3. De reelle skalarmatricer $a\mathbf{1}$ med $a \in \mathbb{R}$ kaldes også *skalarkvaternioner*. De udgør legemet $\mathbb{R}$ som delring af $\mathbb{H}$. Kvaternioner af formen $v = v_1\mathbf{i} + v_2\mathbf{j} + v_3\mathbf{k}$ kaldes *vektorkvaternioner*; de udgør et underrum V af $\mathbb{H}$, som via basen $\mathbf{i}, \mathbf{j}, \mathbf{k}$ kan identificeres med talrummet $\mathbb{R}^3$; herved svarer kvaternionen v til vektoren (v_1, v_2, v_3). Vis følgende formel for et produkt af to *vektorkvaternioner* v og w:

$$vw = -\langle v|w\rangle + v \times w, \tag{*}$$

hvor $\langle v|w\rangle$ er *skalarproduktet*, i koordinater $\langle v|w\rangle = v_1w_1 + v_2w_2 + v_3w_3$, og $v \times w$ er *vektorproduktet*, i koordinater bestemt ved

$$v \times w = \left(\begin{vmatrix} v_2 & w_2 \\ v_3 & w_3 \end{vmatrix}, \begin{vmatrix} v_3 & w_3 \\ v_1 & w_1 \end{vmatrix}, \begin{vmatrix} v_1 & w_1 \\ v_2 & w_2 \end{vmatrix} \right).$$

Vis, at „skalardelen“ af en kvaternion α er bestemt som $\frac{1}{2}(\alpha + \alpha^*)$ og at „vektordelen“ er bestemt som $\frac{1}{2}(\alpha - \alpha^*)$. Vis herved formlerne,

$$\langle v|w\rangle = -\frac{vw + wv}{2}, \quad v \times w = \frac{vw - wv}{2}.$$

[Historisk har skalarprodukt og vektorprodukt faktisk deres oprindelse i Hamilton's regning med kvaternioner: Af (*) fremgår, at skalarprodukt $\langle v|w\rangle$, bortset fra fortegn, er skalardelen af vw og at vektorprodukt $v \times w$ er vektordelen af vw.]

4. Eftervis, ved kvaternionregning, følgende relationer for vektorkvaternioner:

$$v \times w = -w \times v, \quad \langle v \times w \mid w\rangle = 0,$$
$$\mathrm{N}(v)\,\mathrm{N}(w) = \langle v|w\rangle^2 + \mathrm{N}(v \times w), \qquad u \times (v \times w) = -\langle u|v\rangle w + \langle u|w\rangle\, v.$$

[Vink: Tallet $\langle u|v\rangle$ er reelt, så $\langle u|v\rangle w = \frac{1}{2}(\langle u|v\rangle w + w\langle u|v\rangle)$.]

Antag, at $e \in V$ er en enhedsvektor, dvs $\mathrm{N}(e) = 1$. Vis for $x \in V$ følgende ligning:

$$x = \langle x|e\rangle\, e + (e \times x) \times e,$$

og vis, at dette er fremstillingen af x som sum af en vektor proportional med e og en vektor vinkelret på e.

5. Lad $V \subseteq \mathbb{H}$ være underrummet af vektorkvaternioner. For vektorer $u, v, w \in V$ defineres rumproduktet $[u, v, w]$ som -1 gange skalardelen af uvw. Vis, at

$$[u, v, w] = \langle u \times v \mid w \rangle = \langle u \mid v \times w \rangle = -\langle u \mid w \times v \rangle. = -\langle u \times w \mid v \rangle.$$

6. Hvilken plan bestemmes ved ligningen $\langle u \times v \mid x \rangle = 0$ (for faste u, v)? Bestem $(u \times v) \times (w \times z)$. I hvilke planer ligger denne vektor? Er der forudsætninger om u, v, w, z?

7. Lad $V \subseteq \mathbb{H}$ være underrummet af vektorkvaternioner, identificeret med $\mathbb{R}^3$. For $v \in V$ og $\alpha \in \mathbb{H}_1^*$ sættes $\rho_\alpha(v) := \alpha v \alpha^*$. Vis, at der herved defineres en bijektiv lineær afbildning $\rho_\alpha \colon V \to V$, altså et element $\rho_\alpha \in \mathrm{GL}_3(\mathbb{R})$. Vis, at $\alpha \mapsto \rho_\alpha$ er en gruppehomomorfi $\mathbb{H}_1^* \to \mathrm{GL}_3(\mathbb{R})$. Vis, at den lineære afbildning ρ_α er ortogonal, altså at ρ er en homomorfi $\rho \colon \mathbb{H}_1^* \to \mathrm{O}_3(\mathbb{R})$.

*Vis, at ρ er en surjektiv homomorfi,

$$\rho \colon \mathbb{H}_1^* \to \mathrm{SO}_3(\mathbb{R}),$$

med kernen ± 1. [Vink: Enhver enhedskvaternion $\alpha \in \mathbb{H}_1^*$ har formen

$$\alpha = (\cos\theta)1 + (\sin\theta)e,$$

hvor $\theta \in \mathbb{R}$ og $e \in V$ er en enhedsvektor ($\|e\| = 1$); med kravet $0 \leqslant \theta \leqslant \pi$ er fremstillingen entydig, når $\alpha \neq \pm 1$. Vis ved kvaternionregning, at ρ_α er drejningen med vinklen 2θ omkring linien bestemt ved e.]

8. Lad A være en algebra over legemet L. Vis, at *centret* i A, bestående af de elementer, der kommuterer med alle andre, er en kommutativ delalgebra. Bestem centret i kvaternionskævlegemet $\mathbb{H}$.

9. Bestem centret i $\mathrm{Mat}_n(L)$, hvor L er et legeme.

10. Lad A være en algebra over legemet L. For hver delmængde $W \subseteq A$ defineres *kommutanten for W* som delmængden $W^c \subseteq A$ bestående af de elementer, der kommuterer med alle elementer i W. Vis, at W^c er en delalgebra.

11. Lad A være en ring, som indeholder et legeme L som delring (det forudsættes altså ikke, at elementerne i L kommuterer med alle elementer i A). Specielt er A så et vektorrum over L. For et element $\alpha \in A$ defineres evaluering ganske som i (6.5); det er en lineær afbildning,

$$\mathrm{Ev}_\alpha \colon L[X] \to A.$$

Vis, at Ev_α er en ringhomomorfi, hvis og kun hvis α kommuterer med alle elementer i L.

12. Gør rede for, at et vektorrum V over et legeme L kan opfattes som vektorrum over ethvert dellegeme af L. Antag, at V er et endeligdimensionalt vektorrum over $\mathbb{C}$. Vis, at $\dim_{\mathbb{R}} V = 2 \dim_{\mathbb{C}} V$ og, mere præcist, vis, hvordan man ud fra en kompleks basis $(e_1, \ldots, e_n)$ for V kan opnå en reel basis.

Index.