Matematik 211, 1984

Anders Thorup

Algebra

Håndskrevne noter

STRUKTURER

1. Indledning
2. Kompositioner
3. Relationer
4. Harmoniske relationer
5. Harmoniske ordninger
6. Kongruensrelationer

GRUPPER

1. Gruppebegrebet
2. Permutationer
3. Virkninger
4. Lineære grupper
5. Hexaedergruppen
6. App.: Permutationsproblemer

RINGE

1. Ringbegrebet
2. Polynomiumsringen
3. Ringkonstruktioner
4. Algebraer

IDEALER

1. Ideal og hovedideal
2. Primideal og maksimalideal
3. Faktorielle ringe
4. Største fælles divisor
5. Gauss's talring
6. App.: Kvadratiske talringe

OPGAVER (mærket 6–31)

STRUKTURER

1. Indledning. 1.1-3: Mængder med struktur. 1.4-6: Homomorfier, isomorfier etc.

2. Kompositioner. 2.1: Komposition. 2.2: Stabil delmængde. 2.3: Kommutativ, associativ, neutralt element, regulært element, invertibelt element, forkortningsreglen. 2.5: Semigruppe, monoid, gruppe. Inverst element. 2.5: Eksempel. 2.6: Komposition af delmængder. 2.7: Homomorfi etc. 2.8: Flere kompositioner. Distributiv. 2.9: Multiplikativ og additiv skrivemåde. 2.10: Ring. 2.11: Undergruppe. 2.12: Delring.

3. Relationer. 3.1: Relation. 3.2: Refleksiv, irrefleksiv, symmetrisk, asymmetrisk, transitiv, total. 3.3: Homomorfi. 3.4: Ordensrelation. 3.5: Minimalt og første element. 3.6: Majorant og supremum. 3.7: Velordning. 3.8: Ækvivalensrelation. Kvotient og kanonisk afbildning. 3.9: Sprogbrug. 3.10: Udvidelsessætning for mængder. 3.11: Isomorfisætning for mængder.

4. Harmoniske relationer. 4.1: Definition. 4.2: Harmoniske relationer i grupper. Flere kompositioner.

5. Harmoniske ordninger. 5.1: Ordnet gruppe. 5.2: Sætning om ordning i grupper. 5.3: Absolutværdi. 5.4: Ordnet ring.

6. Kongruensrelation og kvotient. 6.1: Kongruensrelation og induceret komposition i kvotienten. 6.2: Kanonisk homomorfi. 6.3: Udvidelsessætning for mængder med komposition. 6.4: Isomorfisætning for mængder med komposition. 6.5-6: Normal undergruppe. Kvotientgruppe. 6.7: Udvidelsessætning for grupper. 6.8: Isomorfisætning for grupper. 6.9: Flere kompositioner. 6.10-11. Ideal. Kvotientring. 6.12: Udvidelsessætning for ringe. 6.13: Isomorfisætning for ringe.

STRUKTURER

1. Indledning.

1.1. Grundlæggende i al matematik er mængde- og afbildningsbegrebet. Mængder forekommer imidlertid yderst sjældent isolerede; de vil, afhængigt af situationen, være forsynet med en vis struktur. Vi kan ikke generelt definere, hvad det vil sige, at en mængde således er strukturmæssigt, men vi kan tost sige, at en struktur på en mængde består i, at den udover mængden er "givet nogit", som "opfylder visse betingelser". Det vil sædvanligvis være klart hvad der menes med at to mængder har strukturer af samme type.

1.2. EKSEMPLER PÅ STRUKTURTYPER. (1) Ordnede mængder. Strukturen på en mængde M er her en relation $<$ i M, dvs en delmængde $\subseteq M \times M$, som opfylder visse velkendte betingelser.

(2) Metriske rum. Strukturen på en mængde M er her en afbildning $dist : M \times M \to \mathbb{R}$, som opfylder visse velkendte betingelser.

(3) Komplekse, normerede vektorrum. Strukturen på en mængde M består her af tre afbildninger:

$$M \times M \to M \qquad \text{(vektoraddition)}$$
$$\mathbb{C} \times M \to M \qquad \text{(multiplikation med skalar)}$$
$$M \to \mathbb{R} \qquad \text{(norm)},$$

som opfylder visse betingelser.

1.3. Man kan angive, at en mængde er strukturmæssigt, ved efter betegnelsen for mængden at anføre symboler for

den givne struktur. I eksemplerne ovenfor kan vi således skrive $(M, <)$ for en ordnet mængde, $(M, dist)$ for et metrisk rum, og $(M, +, \mathbb{C}, \| \|)$ for et kompleks, normeret vektorrum.

1.4. En matematisk teori vil ofte omfatte studiet af mængder med strukturer af en given fast type. I en sådan teori vil der for mængder $(M, \$)$ og $(N, £)$ med strukturer af den givne type være visse afbildninger

$$f : M \to N,$$

der kan siges, at "have noget at gøre med strukturen" eller at "harmonere med strukturen" eller at "bevare (eller respektere) strukturen". Når det for en bestemt strukturtype er præciseret, hvilke afbildninger, der i en sådan forstand er relevante, kan disse afbildninger kaldes homomorfier. For en homomorfi $f : M \to N$ skrives også

$$f : (M, \$) \longrightarrow (N, £).$$

Ved denne sprogbrug er det altid underforstået, at sammensætning af to homomorfier igen er en homomorfi, og at den identiske afbildning $: x \mapsto x$ er en homomorfi $: (M, \$) \to (M, \$)$.

En homomorfi $f : (M, \$) \longrightarrow (N, £)$, der er bijektiv, og således at den inverse afbildning $f^{-1} : N \to M$ også er en homomorfi $: (N, £) \longrightarrow (M, \$)$, kaldes en isomorfi. At en homomorfi $f : (M, \$) \longrightarrow (N, £)$ er en isomorfi, angives ofte ved at skrive

$$f : (M, \$) \xrightarrow{\approx} (N, £).$$

Hvis der findes en sådan isomorfi, siges $(M, \$)$ og $(N, £)$ at være isomorfe. Herfor kan skrives

$$(M, \$) \approx (N, £).$$

En homomorfi $f: (M, \$) \to (M, \$)$ af $(M, \$)$ ind i sig selv kaldes også en endomorfi. En endomorfi, der er en isomorfi, kaldes også en automorfi

OBSERVATION. En homomorfi $f: (M, \#) \to (N, £)$ er en isomorfi, hvis og kun hvis der findes en homomorfi $g: (N, £) \to (M, \#)$, så at

$$g \circ f = Id_M \quad \text{og} \quad f \circ g = I_N,$$

thi af de to ligninger følger, at f er en bijektiv afbildning med g som den inverse.

1.5. Det skal understreges, at vi for en given strukturtype ikke i 1.4 har defineret, hvad en homomorfi (og dermed en isomorfi, ...) er. Når vi taler om homomorfier, skal det altid være præciseret, hvilke afbildninger, der er så interessante, at de fortjener denne betegnelse. For en bestemt strukturtype vil der ofte være flere lige gode valg. For ordnede mængder vil det forekomme ret naturligt, at homomorfierne er de afbildninger

$$f: (M, <) \to (N, <),$$

som opfylder: $x < y \Rightarrow f(x) < f(y)$. For metriske rum er situationen ikke så entydig. Vi kan betragte afbildninger

$$f: (M, dist) \to (N, dist),$$

som er afstandsbevarende, eller (svagt) afstandsformindskende, eller blot kontinuerte. Ved de to første valg bliver isomorfierne de såkaldte isometrier, ved det sidste valg bliver de homeomorfierne.

1.6. I det følgende behandles de fundamentale algebraiske strukturer afledt af kompositioner og relationer.

2. Kompositioner.

2.1. DEFINITION. En *komposition* $*$ i en mængde M er som bekendt en afbildning

$$* : M \times M \longrightarrow M.$$

Billedet i M af $(a,b) \in M \times M$ ved denne afbildning betegnes sædvanligvis $a * b$. Det kaldes *kompositet* af a med b [læses: "a stjerne b" eller "a komponeret med b"] For et fast $a \in M$ er

$$l_a : x \longmapsto a * x$$

en afbildning $: M \to M$. Den kaldes *venstrekomposition med* a. Tilsvarende er *højrekomposition med* a givet ved $r_a : x \longmapsto x * a$.

Mængden M med en given komposition $*$ betegnes kort $(M, *)$.

2.2. DEFINITION. I en mængde med en komposition $(M, *)$ siges en delmængde $S \subseteq M$ at være *stabil*, dersom

$$x \in S \wedge y \in S \Rightarrow x * y \in S.$$

Er dette tilfældet definerer kompositionen $*$ ved *restriktion* en komposition i S, kaldet den *inducerede komposition*.

2.3. DEFINITIONER. Lad $(M, *)$ være en mængde med en komposition. Elementer $x, y \in M$ siges at *kommutere*, hvis

$$x * y = y * x.$$

Gælder dette for alle $x, y \in M$ kaldes kompositionen *kommutativ*.

Den kaldes *associativ*, hvis der for alle $x, y, z \in M$ gælder:

$$(x * y) * z = x * (y * z).$$

Et element $e \in M$ kaldes *neutralt element*, hvis der for alle $x \in M$ gælder:

$$e * x = x * e = x.$$

Et element $a \in M$ kaldes <u>regulært</u>, hvis der for alle $x, y \in M$ gælder

$$a * x = a * y \Rightarrow x = y \quad \text{og} \quad x * a = y * a \Rightarrow x = y.$$

Et element $a \in M$ kaldes <u>invertibelt</u>, hvis der for hvert element $b \in M$ gælder, at hver af de to ligninger

$$a * x = b \qquad \text{og} \qquad z * a = b$$

har en og kun én løsning i M.

BEMÆRKNING. At et element $a \in M$ er regulært (resp. invertibelt) betyder, at venstrekomposition $: x \mapsto a * x$ og højrekomposition $: x \mapsto x * a$ er injektive (resp. bijektive) afbildninger $: M \to M$.

Hvis alle elementer er regulære, siges <u>forkortningsreglen</u> at gælde.

2.4. DEFINITIONER. En <u>semigruppe</u> $(M, *)$ er en mængde med en associativ komposition. Et <u>monoid</u> $(M, *)$ er en semigruppe med et neutralt element. En <u>gruppe</u> $(M, *)$ er et monoid, hvori alle elementer er invertible.

OBSERVATIONER. En komposition kan højst have ét neutralt element. I et monoid $(M, *)$ betegnes det neutrale element ofte e_M. I et monoid $(M, *)$ er et element a invertibelt, netop hvis der findes et element $a' \in M$ således at

$$a * a' = a' * a = e_M.$$

Elementet a' er i så fald entydigt bestemt. Det kaldes det <u>inverse</u> til a, og betegnes a^{-1}.

Det følger, at en mængde M med en komposition $*$ er en gruppe, hvis der findes et element $e \in M$, og for hvert element $x \in M$ et element $x^{-1} \in M$, så at ligningerne

$$(x * y) * z = x * (y * z)$$
$$e * x = x * e = x$$
$$x * x^{-1} = x^{-1} * x = e$$

gælder for alle $x, y, z \in M$.

SÆTNING. Lad $(M, *)$ være et monoid. Hvis a og b er invertible elementer, så er også $a * b$ invertibelt, og

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

De invertible elementer i M udgør en stabil delmængde, som med den inducerede komposition er en gruppe.
BEVIS. □

2.5. EKSEMPEL. Lad X være en mængde, og lad $\mathrm{End}(X)$ betegne mængden af alle afbildninger $: X \to X$ af mængden ind i sig selv. Vi kan opfatte sammensætning som en komposition $\circ$ i mængden $\mathrm{End}(X)$. Da sammensætning af afbildninger som bekendt er associativ, og da den identiske afbildning

$$Id_X : x \mapsto x$$

åbenlyst er neutralt element, er $(\mathrm{End}(X), \circ)$ et monoid. Gruppen af invertible elementer heri består netop af de bijektive afbildninger $: X \to X$. Denne gruppe betegnes også $\mathrm{Aut}(X)$.

2.6. NOTATION. I en mængde med en komposition $(M, *)$ er det ofte hensigtsmæssigt at bruge kompositionstegnet i forbindelse med delmængder. Er $A, B \subseteq M$, betegner vi således med $A * B$ delmængden.

$$A * B := \{ a * b \mid a \in A \wedge b \in B \}.$$

Tilsvarende sættes for $a \in M$ og $B \subseteq M$

$$a * B := \{ a * b \mid b \in B \},$$

og hvis $(M, *)$ er en gruppe:

$$B^{-1} = \{ b^{-1} \mid b \in B \}, \quad a * B * a^{-1} = \{ a * b * a^{-1} \mid b \in B \}.$$

2.7. DEFINITION. Lad $*$ være en komposition i mængden M og lad $*'$ være en komposition i mængden M'. En afbildning $f : M \to M'$ siges da at være

en <u>homomorfi</u>

$$f : (M,*) \longrightarrow (M',*'),$$

hvis der for alle $x, y \in M$ gælder

$$f(x * y) = f(x) *' f(y).$$

En bijektiv homomorfi $f : (M,*) \to (M',*')$ kaldes også en <u>isomorfi</u>. For en sådan er den inverse afbildning f^{-1} en homomorfi

$$f^{-1} : (M',*') \longrightarrow (M,*).$$

En homomorfi $f : (M,*) \to (M,*)$ kaldes også en <u>endomorfi</u> i $(M,*)$. Er den bijektiv, kaldes den også en <u>automorfi</u> i $(M,*)$.

OBSERVATION. For en <u>gruppehomomorfi</u>, dvs en homomorfi $f : (M,*) \to (M',*')$ mellem grupper $(M,*)$ og $(M',*)$, gælder

$$f(e_M) = e_{M'}, \quad f(x^{-1}) = f(x)^{-1}, \quad x \in M.$$

BEMÆRKNING. For en homomorfi $f : (M,*) \to (M',*')$ mellem monoider $(M,*)$ og $(M',*')$ gælder ikke i almindelighed, at

$$f(e_M) = e_{M'}.$$

Er denne betingelse opfyldt, kaldes homomorfien en <u>monoidhomomorfi</u>.

2.8. Vi vil ofte møde mængder M, i hvilke der er givet to (eller flere) kompositioner. I en sådan situation må man naturligvis præcisere på hvilken af kompositionerne de foregående definitioner anvendes. Er $(M, *, \square)$ en mængde med kompositioner $*$ og $\square$, kan en delmængde $S \subseteq M$ være stabil under $*$, og stabil under $\square$. Er den stabil under begge kompositioner kaldes den <u>stabil</u> i $(M, *, \square)$. Den kan i så fald selv opfattes som en mængde med inducerede kompositioner $(S, *, \square)$.

Er tilsvarende $(M', *', \square')$ en mængde med to kompositioner, kan en afbildning $f: M \to M$ være en homomorfi $f: (M, *) \to (M', *')$ og en homomorfi $f: (M, \square) \to (M, \square')$. Er begge dele opfyldt siges f at være en <u>homomorfi</u>

$$f: (M, *, \square) \longrightarrow (M', *', \square').$$

DEFINITION. I en mængde M med kompositioner $*$ og $\square$ siges $*$ at være <u>distributiv</u> m.h.t. $\square$, hvis der for alle $x, y, z \in M$ gælder

$$x * (y \square z) = (x * y) \square (x * z) \text{ og } (x \square y) * z = (x * z) \square (y * z)$$

2.9. NOTATION. En komposition i en mængde kan naturligvis betegnes med et hvilketsomhelst symbol. (Andre almindeligt brugte tegn er $\circ, \times, \cup, \cap, \vee, \wedge$.) Vi vil ofte skrive kompositionen <u>multiplikativt</u>, dvs bruge tegnet $\cdot$ for kompositionen. Kompositet $a \cdot b$ kaldes da <u>produktet</u>, og heri udelader vi ofte kompositionstegnet og skriver $ab = a \cdot b$. Et eventuelt neutralt element kan også kaldes et <u>et-element</u> og betegnes 1. Betingelsen er:

$$1x = x1 = x.$$

Visse kommutative kompositioner vil vi dog skrive <u>additivt</u>, dvs vi vil bruge tegnet $+$ for kompositionen. Kompositet $a+b$ kaldes da <u>summen</u>. Et eventuelt neutralt element kan kaldes et <u>nul-element</u> og betegnes 0. Betingelsen er: $0 + x = x$.
Et eventuelt inverst element til x kaldes da det <u>modsatte</u> til x og betegnes $-x$. Betingelsen er: $x + (-x) = 0$.

Er $(M, *)$ en kommutativ semigruppe og $I \neq \emptyset$ en endelig mængde, kan vi for en afbildning $a: I \to M$ definere elementet

$$\overset{*}{\underset{i \in I}{}} a_i \quad [\text{additivt: } \sum_{i \in I} a_i \text{; multiplikativt: } \prod_{i \in I} a_i]$$

som kompositet af elementerne $a_i, i \in I$ [Overvej dette!].
Har M et neutralt element e, er det hensigtsmæssigt at tillægge dette kompositum værdien e, når $I = \emptyset$.

2.10. DEFINITION. En ring $(\Lambda, +, \cdot)$ er en mængde Λ med kompositioner $+$ og $\cdot$ således at

(1) $(\Lambda, +)$ er en kommutativ gruppe.

(2) $(\Lambda, \cdot)$ er et monoid.

(3) $\cdot$ er distributiv m.h.t. $+$.

Nul-elementet i $(\Lambda, +)$ er ringens nul-element 0_Λ, og et-elementet i $(\Lambda, \cdot)$ er ringens et-element 1_Λ.

En ringhomomorfi $f : (\Lambda, +, \cdot) \to (\Gamma, +, \cdot)$ er en afbildning $f : \Lambda \to \Gamma$ mellem ringe, som opfylder

$$f(x+y) = f(x) + f(y),$$
$$f(xy) = f(x) f(y)$$
$$f(1_\Lambda) = 1_\Gamma.$$

2.11. DEFINITION. Lad $(G, \cdot)$ være en gruppe. En delmængde $H \subseteq G$ kaldes da en undergruppe, hvis den er stabil, og med den inducerede komposition selv er en gruppe. Det følger, at inklusionsafbildningen er en gruppehomomorfi : $(H, \cdot) \hookrightarrow (G, \cdot)$.

OBSERVATION. En delmængde H af en gruppe $(G, \cdot)$ er en undergruppe, netop når den gælder

$$x \in H \wedge y \in H \Rightarrow xy \in H$$
$$e_G \in H$$
$$x \in H \Rightarrow x^{-1} \in H.$$

2.12. DEFINITION. Lad $(\Lambda, +, \cdot)$ være en ring. En delmængde $\Delta \subseteq \Lambda$ kaldes da en delring, hvis den er stabil, og med de inducerede kompositioner selv er en ring med samme et-element som Λ. Den sidste betingelse er nødvendig for at sikre, at inklusionsafbildningen er en ringhomomorfi : $(\Delta, +, \cdot) \hookrightarrow (\Lambda, +, \cdot)$.

3. Relationer.

3.1. DEFINITION. En relation R i en mængde M er som bekendt en delmængde

$$R \subseteq M \times M.$$

Udsagnet $(x,y) \in R$ skrives sædvanligvis

$$xRy,$$

og dets negation skrives $x \not R y$.

3.2. DEFINITIONER. En relation R i en mængde M kaldes refleksiv, hvis den for alle $x \in M$ gælder

$$xRx,$$

og irrefleksiv, hvis den for alle $x \in M$ gælder

$$x \not R x.$$

Den kaldes symmetrisk, hvis den for alle $x,y \in M$ gælder

$$xRy \Rightarrow yRx,$$

og asymmetrisk, hvis den for alle $x,y \in M$ gælder

$$xRy \wedge yRx \Rightarrow x = y.$$

Den kaldes transitiv, hvis den for alle $x,y,z \in M$ gælder

$$xRy \wedge yRz \Rightarrow xRz.$$

Den kaldes total, hvis den for alle $x,y \in M$ gælder

$$x = y \vee xRy \vee yRx.$$

3.3. DEFINITION. Lad R være en relation i mængden M og lad R' være en relation i mængden M'. En afbildning $f: M \to M'$ siges da at respektere relationerne, eller at være en homomorfi

$$f: (M,R) \to (M',R'),$$

hvis der for alle $x, y \in M$ gælder:

$$x R y \Rightarrow f(x) R' f(y).$$

Er der kun givet en relation R i M siges en afbildning $f: M \to M'$ at <u>respektere relationen</u>, hvis der for alle $x, y \in M$ gælder:

$$x R y \Rightarrow f(x) = f(y).$$

3.4. DEFINITION. En transitiv relation R i en mængde M kaldes en <u>præ-ordning</u>. Den kaldes en <u>ordning</u>, hvis den desuden er asymmetrisk. Som betegnelse for en ordning bruges ofte et af tegnene $\prec$ og $\prec$ [læses: "går forud for"] eller $\succ$ og $\succ$ [læses: "følger efter"]. Til hver ordning $\prec$ hører en refleksiv ordning $\preceq$ defineret ved

$$x \preceq y \overset{\text{DEF}}{\iff} x \prec y \vee x = y,$$

og en irrefleksiv ordning $\precneqq$ defineret ved

$$x \precneqq y \overset{\text{DEF}}{\iff} x \prec y \wedge x \neq y.$$

Vi vil <u>reservere</u> tegnene $\leqslant$, $\subseteq$, $\geqslant$, $\supseteq$ (resp. $<$, $\subset$, $>$, $\supset$) som betegnelse for ordninger, som er refleksive (resp. irrefleksive).

En <u>ordnet mængde</u> $(M, \prec)$ er en mængde M med en given ordning $\prec$. Hvis relationen $\prec$ er total, kaldes $(M, \prec)$ <u>totalt ordnet</u>. Er relationen $\prec$ ikke nødvendigvis er total, siges $(M, \prec)$ også at være <u>partielt ordnet</u>.

For ordnede mængder $(M, \prec)$ og $(M', \prec')$ siges en afbildning $f: M \to M'$, som respekterer ordningerne, også at være en <u>ordenstro</u> afbildning

$$f: (M, \prec) \to (M', \prec').$$

En ordning $\prec$ i mængden M nedarves umiddelbart til enhver delmængde $N \subseteq M$. Med denne <u>inducerede</u> ordning i N er inklusionsafbildningen ordenstro: $(N, \prec) \hookrightarrow (M, \prec)$.

OBSERVATION. En relation R, som er transitiv og irrefleksiv, er også asymmetrisk (og altså en ordning).

3.5. DEFINITION. I en ordnet mængde $(M, \prec)$ siges et element a at være *minimalt*, hvis der for alle $x \in M$ gælder

$$x \prec a \Rightarrow x = a,$$

og at være *første element*, hvis der for alle $y \in M$ gælder

$$a \preceq y.$$

Tilsvarende defineres *maksimalt element* og *sidste element*

BEMÆRK: "Minimalt" betyder, at ingen elementer går ægte forud, "første element" betyder, at alle elementer følger efter. De to definitioner stemmer kun overens for totalt ordnede mængder. I almindelighed kan der godt være flere minimale elementer (men højst ét første element).

3.6. DEFINITION. Lad $(M, \prec)$ være en ordnet mængde, og lad $N \subseteq M$ være en delmængde. Et element $a \in M$ kaldes en *majorant for N*, hvis der for alle $y \in N$ gælder $y \preceq a$. Et element $b \in M$, der er første element i delmængden af majoranter for N, kaldes også *supremum for N*. Herfor skrives

$$b = \sup N.$$

Tilsvarende defineres *minorant*, *infimum* og $\inf N$.

Hvis der findes majoranter for N, siges N at være *opad begrænset*. Er der også minoranter, kaldes N *begrænset*.

3.7. DEFINITION. En ordnet mængde $(M, \prec)$ kaldes *velordnet*, hvis enhver ikke-tom delmængde af M har et første element.

3.8. DEFINITION. En relation R i en mængde M kaldes en ækvivalensrelation, hvis den er refleksiv, symmetrisk og transitiv. Ækvivalensklasserne er da de delmængder af M, der har formen

$$\{ x \in M \mid xRa \}, \quad \text{med } a \in M.$$

De udgør en klassedeling af M, dvs en mængde af ikke-tomme, parvis disjunkte delmængder, hvis foreningsmængde er M.

Mængden af ækvivalensklasser kaldes kvotienten (eller kvotientmængden) af M m.h.t. R og betegnes M/R [læses: "M over R" eller "M modulo R"].

En ækvivalensklasse X kan altså opfattes dels som en delmængde $X \subseteq M$, dels som et element i den nye mængde M/R. Hvis $x \in X$, siges x at være en repræsentant for X.

Idet vi for hvert $x \in M$ med $\textcircled{x}$ [læses: "x cirkel"] betegner ækvivalensklassen, der indeholder x, altså

$$\textcircled{x} = \{ x' \mid x'Rx \},$$

defineres ved $x \mapsto \textcircled{x}$ en surjektiv afbildning

$$\circ : M \to M/R,$$

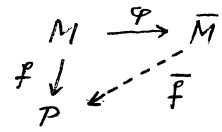
kaldet den kanoniske afbildning. At elementet $x \in M$ er repræsentant for ækvivalensklassen X betyder således, at $\textcircled{x} = X$. Bemærk, at

$$\textcircled{x} = \textcircled{y} \iff xRy.$$

Elementet $\textcircled{x} \in M/R$ kan også betegnes $x \bmod R$.

3.9. SPROGBRUG. Lad der være givet en afbildning $\varphi : M \to \bar{M}$. En afbildning $\bar{f} : \bar{M} \to P$ siges da at udvide afbildningen $f : M \to P$ m.h.t. φ, hvis

$$\bar{f} \circ \varphi = f.$$



Hvis det er underforstået hvilken afbildning $M \to \bar{M}$, der er givet, siger vi blot at $\bar{f}$ er en udvidelse f.

3.10. Med denne sprogbrug gælder følgende triviella:
UDVIDELSESSÆTNING FOR MÆNGDER. Lad R være en ækvivalensrelation i M, og lad $O: M \to M/R$ være den kanoniske afbildning ind i kvotienten. Enhver afbildning $f: M \to P$, som respekterer ækvivalensrelationen R, kan da entydigt udvides til en afbildning $\bar{f}: M/R \to P$ fra kvotienten.

BEVIS. At $\bar{f}$ er en udvidelse af f betyder, at $\bar{f} \circ O = f$, altså at

$$\bar{f}(\textcircled{x}) = f(x), \quad x \in M.$$

Heraf følger påstanden lit, da hvert element $X \in M/R$ har formen $X = \textcircled{x}$ □

DEFINITION. Den entydigt bestemte udvidelse siges også at være <u>induceret</u> af f.

3.11. DEFINITION. Lad $f: M \to P$ være en afbildning. <u>Billedet ved f</u> er da billedmængden

$$f(M) := \{ f(x) \mid x \in M \},$$

og den til <u>f hørende relation</u> er relationen $\tilde{f}$ defineret ved

$$x' \mathrel{\tilde{f}} x \overset{\text{DEF}}{\iff} f(x') = f(x).$$

Det er klart, at afbildningen f respekterer relationen $\tilde{f}$.

ISOMORFISÆTNING FOR MÆNGDER. Lad $f: M \to P$ være en afbildning. Da er billedet en delmængde af P, og relationen $\tilde{f}$ er en ækvivalensrelation i M. Den inducerede afbildning er en bijektion $\bar{f}: M/\tilde{f} \xrightarrow{\approx} f(M)$ af kvotienten på billedet.

BEVIS. Relationen $\tilde{f}$ er åbenbart en ækvivalensrelation, så ifølge udvidelsessætningen inducerer f en afbildning $\bar{f}: M/\tilde{f} \to P$. Billedmængden heraf er netop $f(M)$, så vi kan opfatte $\bar{f}$ som en surjektiv afbildning

$$\bar{f}: M/\tilde{f} \longrightarrow f(M),$$

og skal vise, at den er injektiv: Lad X og Y være elementer i kvotienten $M/\tilde{f}$, således at $\bar{f}(X) = \bar{f}(Y)$. Vælges repræsentanter x for X og y for Y har vi

$$f(x) = \bar{f}(\textcircled{x}) = \bar{f}(X) = \bar{f}(Y) = \bar{f}(\textcircled{y}) = f(y),$$

men så er $x \tilde{f} y$, og altså $X = \textcircled{x} = \textcircled{y} = Y$ ▨

BEMÆRKNING. Idet vi med $\iota: f(M) \hookrightarrow P$ betegner inklusionsafbildningen, er den givne afbildning en sammensætning $f = \iota \circ \bar{f} \circ O$

$$\begin{array}{ccc} M & \xrightarrow{f} & P \\ {\scriptstyle O}\downarrow & & \uparrow{\scriptstyle \iota} \\ M/\tilde{f} & \xrightarrow{\bar{f}} & f(M) \end{array}$$

af en surjektiv afbildning O, en bijektiv afbildning $\bar{f}$ og en injektiv afbildning ι.

4. Harmoniske relationer

4.1. DEFINITION. Lad M være en mængde med en komposition $*$ og en relation R. Relationen siges da at <u>harmonere med højrekomposition</u>, hvis der for alle $x, y, a \in M$ gælder

$$x R y \Rightarrow x*a \; R \; y*a,$$

og at <u>harmonere med venstrekomposition</u>, hvis der for alle $x, y, a \in M$ gælder

$$x R y \Rightarrow a*x \; R \; a*y.$$

Er begge dele opfyldt, siges relationen R at <u>harmonere</u> med kompositionen $*$, eller at være en <u>harmonisk</u> relation i $(M, *)$.

BEMÆRKNING. Betingelserne udsiger, at højrekomposition $x \mapsto x*a$ og venstrekomposition $x \mapsto a*x$ er homomorfier $: (M, R) \to (M, R)$.

OBSERVATION. Hvis en harmonisk relation R i $(M, *)$ er transitiv, så gælder for alle $x, x', y, y' \in M$, at

$$x R x' \wedge y R y' \Rightarrow x*y \; R \; x'*y'.$$

4.2. OBSERVATION. En relation R i en <u>gruppe</u> $(G, \cdot)$ (med neutralt element e), som harmonerer med venstremultiplikation, er helt bestemt ved delmængden $\{z \in G \mid eRz\}$, idet vi har

$$x R y \Leftrightarrow x^{-1}y \in \{z \in G \mid eRz\}.$$

Omvendt gælder følgende

SÆTNING. Lad $(G, \cdot)$ være en gruppe med neutralt element e. For hver delmængde $N \subseteq G$ definerer da ved

$$x R_N y \overset{\text{DEF}}{\Leftrightarrow} x^{-1}y \in N$$

en relation R_N i G, som harmonerer med venstremultiplikation, og for hvilken

$$\{ z \in G \mid e \, R_N \, z \} = N.$$

Om relationen R_N gælder yderligere:

(1) R_N er harmonisk $\Leftrightarrow$ $a^{-1} N a \subseteq N$ for alle $a \in G$.
(2) R_N er refleksiv $\Leftrightarrow$ $e \in N$
(3) R_N er irrefleksiv $\Leftrightarrow$ $e \notin N$
(4) R_N er symmetrisk $\Leftrightarrow$ $N^{-1} \subseteq N$.
(5) R_N er asymmetrisk $\Leftrightarrow$ $N \cap N^{-1} \subseteq \{e\}$.
(6) R_N er transitiv $\Leftrightarrow$ $N \cdot N \subseteq N$ ($\Leftrightarrow$: N er stabil).
(7) R_N er total $\Leftrightarrow$ $G = \{e\} \cup N \cup N^{-1}$.

BEVIS. Den første påstand følger af at

$$(ax)^{-1}(ay) = x^{-1} a^{-1} a y = x^{-1} y.$$

(1), "$\Rightarrow$": Vi skal vise for $a \in G$ og $z \in N$, at $a^{-1} z a \in N$. Da $z \in N$, har vi $e R_N z$, og da R_N harmonerer med højremultiplikation, følger heraf $ea \, R_N \, za$, altså

$$a^{-1} z a = (ea)^{-1}(za) \in N.$$

(1), "$\Leftarrow$": Vi skal vise, at R_N harmonerer med højremultiplikation. Antag derfor, at $x R_N y$, og lad $a \in G$. Da er $(xa)^{-1}(ya) = a^{-1}(x^{-1}y)a \in N$, thi $x^{-1}y \in N$, og $a^{-1} N a \subseteq N$.

De øvrige påstande vises analogt $\square$

BEMÆRKNINGER. Ud fra en delmængde $N \subseteq G$ kan vi analogt ved

$$x \, R_N^h \, y \overset{\text{DEF}}{\Leftrightarrow} y x^{-1} \in N$$

definere en relation R_N^h, som harmonerer med højremultiplikation. Det er let at se, at R_N og R_N^h er den samme relation, netop når betingelsen (1) er opfyldt.

Vi kan yderligere, ved at betragte produkterne $y^{-1}x$ og xy^{-1} definere endnu to relationer. Hvis både (1) og (4) er opfyldt, bliver disse 4 relationer ens, idet

udsagnene

$$x^{-1}y \in N, \quad yx^{-1} \in N, \quad y^{-1}x \in N, \quad xy^{-1} \in N$$

så er ensbetydende.

NOTATION. I en kommutativ gruppe er betingelsen 4.2.(1) altid opfyldt. Vi fremhæver, at for en delmængde N i en kommutativ, additivt skrevet gruppe $(G,+)$, er relationen R_N bestemt ved

$$x R_N y \overset{\text{DEF}}{\iff} y - x \in N,$$

og at denne relation altid er harmonisk. De øvrige betingelser har udseendet:

(2) R_N er refleksiv $\iff$ $0 \in N$

(3) R_N er irrefleksiv $\iff$ $0 \notin N$

(4) R_N er symmetrisk $\iff$ $-N \subseteq N$

(5) R_N er asymmetrisk $\iff$ $N \cap (-N) \subseteq \{0\}$

(6) R_N er transitiv $\iff$ $N + N \subseteq N$

(7) R_N er total $\iff$ $G = \{0\} \cup N \cup (-N)$.

TILFØJELSE. Er der i den kommutative gruppe $(G,+)$ givet endnu en komposition $*$, der er distributiv m.h.t. $+$, gælder

(8) R_N harmonerer med $*$ $\iff$ $a*N \subseteq N$ og $N*a \subseteq N$ for alle $a \in G$.

BEVIS. Som de foregående. Det er nødvendigt at udnytte

$$a*0 = 0*a = 0, \quad a*(-x) = -(a*x), \quad (-x)*a = -(x*a). \square$$

5. Harmoniske ordninger

5.1. DEFINITION. En ordnet gruppe $(G,\cdot,<)$ er en mængde G forsynet med en komposition $\cdot$ og en relation $<$ således at

(1) $(G,\cdot)$ er en gruppe.

(2) $(G,<)$ er en totalt, irrefleksivt ordnet mængde.

(3) Relationen $<$ harmonerer med kompositionen $\cdot$.

Den sidste betingelse udsiger, at der for alle $x,y,a\in G$ gælder

$$x<y \Rightarrow xa<ya \wedge ax<ay.$$

Vi skal hovedsagelig beskæftige os med kommutative (additivt skrevne) ordnede grupper $(G,+,<)$. For en sådan udsiger betingelsen (3), at

$$x<y \Rightarrow x+a<y+a.$$

Af transitiviteten følger, at vi kan "addere uligheder":

$$x\leqslant y \wedge a\leqslant b \Rightarrow x+a\leqslant y+b.$$

5.2. DEFINITION. Et element a i en kommutativ, ordnet gruppe $(G,+,<)$ kaldes positivt, hvis $0<a$. Delmængden bestående af positive elementer betegnes

$$G_+ := \{a\in G \mid 0<a\}.$$

Vi har øjensynlig

$$x<y \Leftrightarrow y-x\in G_+.$$

Af betingelserne (3), (6) og (7) i Sætning 4.2 følger, at vi har $0\notin G_+$, at G_+ er stabil og at der for hvert element $x\neq 0$ i G gælder $x\in G_+$ eller $-x\in G_+$. Endvidere følger det, at vi omvendt har:

SÆTNING. Lad $(G,+)$ være en kommutativ gruppe,

og lad $P \subseteq G$ være en stabil delmængde, således at $0 \notin P$ og således at der for hvert element $x \neq 0$ i G gælder $x \in P$ eller $-x \in P$. Da definerer ved

$$x < y \overset{\text{DEF}}{\iff} y - x \in P$$

en relation $<$ i G således at $(G, +, <)$ er en ordnet gruppe med $G_+ = P$.

BEVIS. ∎

5.3. DEFINITION. Lad a være et element i en kommutativ ordnet gruppe $(G, +, <)$. Ved <u>absolutværdien</u> af a, betegnet $|a|$, forstås det største af elementerne a og $-a$.

Vi har

$$\boxed{\begin{array}{l} |a| \geqslant 0, \text{ med } "=" \text{ kun når } a = 0. \\ |-a| = |a|. \\ |a+b| \leqslant |a| + |b|. \quad (\text{Trekantsuligheden}). \end{array}}$$

Af ulighederne $\left.\begin{matrix} a \\ -a \end{matrix}\right\} \leqslant |a|$ og $\left.\begin{matrix} b \\ -b \end{matrix}\right\} \leqslant |b|$ fås nemlig ved addition, at $\left.\begin{matrix} a+b \\ -a-b \end{matrix}\right\} \leqslant |a|+|b|$,

og det er netop trekantsuligheden.

Heraf følger let, at

$$\boxed{\big|\, |a| - |b| \,\big| \leqslant |a-b|.}$$

5.4. DEFINITION. En <u>ordnet ring</u> $(\Lambda, +, \cdot, <)$ er en mængde Λ med kompositioner $+$ og $\cdot$ og en relation $<$ således at

(1) $(\Lambda, +, \cdot)$ er en ring.

(2) $(\Lambda, <)$ er en totalt, irrefleksivt ordnet mængde.

(3) Relationen $<$ harmonerer med additionen $+$ og med multiplikation med positive elementer.

Den sidste betingelse udsiger, at der for alle $x, y, a \in \Lambda$ gælder

$$x < y \Rightarrow x + a < y + a$$

$$x < y \wedge 0 < a \Rightarrow xa < ya \wedge ax < ay.$$

Da $(\Lambda, +, <)$ specielt er en ordnet gruppe, følger af det foregående, at delmængden

$$\Lambda_+ := \{a \in \Lambda \mid 0 < a\}$$

bestående af <u>positive elementer</u> bestemmer ordningen, idet

$$x < y \iff y - x \in \Lambda_+,$$

og at Λ_+ m.h.t. addition har egenskaberne nævnt i 5.2. Ydermere er Λ_+ stabil under multiplikation, thi af $0 < a$ og $0 < b$ følger $0 = a \cdot 0 < ab$.
Omvendt har vi:
SÆTNING. Lad $(\Lambda, +, \cdot)$ være en ring, og lad $P \subseteq \Lambda$ være en stabil (m.h.t. $+$ og $\cdot$) delmængde, således at $0 \notin P$ og således at der for hvert $x \neq 0$ i Λ gælder $x \in P$ eller $-x \in P$. Da defineres ved

$$x < y \overset{DEF}{\iff} y - x \in P$$

en relation $<$ i Λ således at $(\Lambda, +, \cdot, <)$ er en ordnet ring med $\Lambda_+ = P$.
BEVIS. Det skal blot vises, at relationen harmonerer med multiplikation med positive elementer, og det følger let af at P er stabil under multiplikation □

OBSERVATION. For absolutværdien gælder $|xy| = |x||y|$. Endvidere er $0_\Lambda < 1_\Lambda$ (med mindre Λ er nulringen).

6. Kongruensrelation og kvotient.

6.1. DEFINITION. Lad $(M,*)$ være en mængde med en komposition. En ækvivalensrelation $\sim$ i M, der harmonerer med kompositionen $*$, kaldes også en kongruensrelation i $(M,*)$. En relation $\sim$ i M er altså en kongruensrelation, hvis den er refleksiv, symmetrisk og transitiv, samt opfylder

$$x' \sim x \Rightarrow x'*a \sim x*a \quad \wedge \quad a*x' \sim a*x.$$

For en ækvivalensrelation er den sidste betingelse ensbetydende med

$$x' \sim x \quad \wedge \quad y' \sim y \Rightarrow x'*y' \sim x*y.$$

Er $\sim$ en kongruensrelation i $(M,*)$, kan vi i kvotientmængden $M/\sim$ definere en komposition $\tilde{*}$ på følgende måde: Lad X og Y være ækvivalensklasser, og vælg en repræsentant x for X og en repræsentant y for Y. Kompositet $X \tilde{*} Y$ af ækvivalensklasserne er da ækvivalensklassen

$$X \tilde{*} Y := \overline{x*y},$$

der indeholder kompositet af repræsentanterne. At dette er veldefinert, altså at ækvivalensklassen $\overline{x*y}$ ikke afhænger af de foretagne valg, følger af betingelsen ovenfor.

Den således definerede komposition $\tilde{*}$ i kvotientmængden kaldes den inducerede komposition. Den betegnes sædvanligvis med samme symbol som den givne komposition i M. Kvotientmængden $M/\sim$

med den inducerede komposition $*$ kaldes også kvotienten af $(M,*)$, og skrives

$$(M/\sim\ ,\ *) \quad = \quad (M,*)/\sim .$$

6.2. Er $\sim$ en kongruensrelation i $(M,*)$, følger det af definitionen på den inducerede komposition, at vi har

$$\textcircled{x} * \textcircled{y} \quad = \quad \textcircled{x*y} \quad , \quad x,y \in M.$$

Dette betyder imidlertid, at den kanoniske afbildning: $x \mapsto \textcircled{x}$ er en homomorfi

$$O : (M,*) \longrightarrow (M/\sim\ ,\ *).$$

Den kaldes også den kanoniske homomorfi.

OBSERVATION. Da den kanoniske homomorfi

$$O : (M,*) \longrightarrow (M/\sim\ ,\ *)$$

er surjektiv, vil en lang række egenskaber ved $(M,*)$ nedarves til kvotienten $(M/\sim,*)$. Som eksempler på sådanne egenskaber kan nævnes kommutativitet, associativitet, eksistens af neutralt element, eksistens af inverst element.

Lad os f.eks. vise, at associativitet nedarves: Er X,Y,Z elementer i kvotienten, vælges repræsentanter: $X = \textcircled{x}$, $Y = \textcircled{y}$, $Z = \textcircled{z}$. Vi finder så:

$$(X*Y)*Z = \textcircled{x*y} * Z = \textcircled{(x*y)*z}$$

og

$$X*(Y*Z) = X * \textcircled{y*z} = \textcircled{x*(y*z)}.$$

Af $(x*y)*z = x*(y*z)$ følger derfor

$$(X*Y)*Z = X*(Y*Z).$$

6.3. UDVIDELSESSÆTNING FOR MÆNGDER MED KOMPOSITION.
Lad $\sim$ være en kongruensrelation i $(M,*)$, og lad $O: (M,*) \to (M/\sim, *)$ være den kanoniske homomorfi ind i kvotientm. Enhver homomorfi $f: (M,*) \to (P,*)$, som respekterer $\sim$, kan entydigt udvides til en homomorfi $\bar{f}: (M/\sim, *) \to (P,*)$ fra kvotientm.

$$\begin{array}{ccc} (M,*) & \xrightarrow{O} & (M/\sim, *) \\ f \downarrow & \swarrow_{\bar{f}} & \\ (P,*) & & \end{array}$$

BEVIS. I følge Udvidelsessætning 3.10 skal det blot vises, at den inducerede afbildning $\bar{f}: M/\sim \to P$ er en homomorfi, og det følger let af definitionerne □

6.4. For en homomorfi $f: (M,*) \to (P,*)$ kan vi, jfr. 3.11, betragte dels billedet $f(M)$, dels den til f hørende relation

$$x' \underset{f}{\sim} x \overset{\text{DEF}}{\iff} f(x') = f(x).$$

ISOMORFISÆTNING FOR MÆNGDER MED KOMPOSITION. Lad $f: (M,*) \to (P,*)$ være en homomorfi. Da er billedet $f(M)$ en stabil delmængde i $(P,*)$, og relationen $\underset{f}{\sim}$ er en kongruensrelation i $(M,*)$. Den inducerede homomorfi er en isomorfi $\bar{f}: (M/\underset{f}{\sim}, *) \to (f(M), *)$ af kvotientm på billedet.
BEVIS. Følger af Isomorfisætning 3.11 □

BEMÆRKNING. Homomorfien f er således en sammensætning $f = \iota \circ \bar{f} \circ O$ af en surjektiv homomorfi $O: M \to M/\underset{f}{\sim}$, en isomorfi $\bar{f}: M/\underset{f}{\sim} \xrightarrow{\sim} f(M)$ og den injektive inklusionshomomorfi $\iota: f(M) \hookrightarrow P$.

6.5. DEFINITION. Lad $(G,\cdot)$ være en gruppe. En <u>normal undergruppe</u> N i G er da en undergruppe N, således at $a\cdot N\cdot a^{-1}\subseteq N$ for alle $a\in G$.

SÆTNING. Lad $(G,\cdot)$ være en gruppe. Kongruensrelationerne i $(G,\cdot)$ er da netop relationerne $\equiv_N$ definerede ved

$$x \equiv_N y \overset{\text{DEF}}{\iff} x^{-1}y \in N,$$

hvor $N\subseteq G$ er en normal undergruppe.

BEVIS. Af 4.2 følger, at relationerne i $(G,\cdot)$, der harmonerer med venstremultiplikation netop er relationerne R_N definerede ved

$$x\, R_N\, y \overset{\text{DEF}}{\iff} x^{-1}y \in N,$$

hvor $N\subseteq G$ er en delmængde. Af betingelserne (1), (2), (4) og (6) i Sætning 4.2 aflæses, at R_N er en kongruensrelation i $(G,\cdot)$, netop når N er en normal undergruppe i G ▨

6.6. DEFINITION. Lad N være en normal undergruppe i en gruppe $(G,\cdot)$. Kongruensrelationen $\equiv_N$ defineret ovenfor kaldes da "<u>kongruens modulo N</u>". Da den kanoniske homomorfi $\sigma:(G,\cdot)\to(G/\equiv_N,\cdot)$ er surjektiv, følger det let, at kvotienten, med den inducerede komposition $\cdot$, igen er en gruppe. Den kaldes <u>kvotientgruppen</u> af G m.h.t. N og betegnes G/N.

Elementerne i kvotienten G/N er ækvivalensklasserne ved $\equiv_N$. Det er øjensynlig delmængderne i G af formen

$$x\cdot N,\quad x\in G.$$

De kaldes også <u>sideklasser modulo N</u>. Det neutrale element i kvotienten er sideklassen $e\cdot N = N$.

6.7. For en gruppehomomorfi $f: (G,\cdot) \to (H,\cdot)$ gælder som bekendt, at $f(e_G) = e_H$ og at $f(x^{-1}) = f(x)^{-1}$. Det følger let, at en gruppehomomorfi $f: (G,\cdot) \to (H,\cdot)$ respekterer relationen $\underset{N}{\equiv}$, netop når

$$f(z) = e_H \quad \text{for alle } z \in N.$$

Er dette opfyldt siges homomorfien at <u>forsvinde på N</u>.

Af Udvidelsessætning 6.3 får vi derfor - med de nye betegnelser - følgende:

UDVIDELSESSÆTNING FOR GRUPPER. Lad N være en normal undergruppe i en gruppe $(G,\cdot)$, og lad $\sigma: (G,\cdot) \to (G/N,\cdot)$ være den kanoniske homomorfi ind i kvotienten. Enhver gruppehomomorfi $f: (G,\cdot) \to (H,\cdot)$, der forsvinder på N, kan da entydigt udvides til en homomorfi $\bar{f}: (G/N,\cdot) \to (H,\cdot)$ fra kvotienten ▨

6.8. DEFINITION. For en gruppehomomorfi $f: (G,\cdot) \to (H,\cdot)$ defineres <u>kernen</u> som originalmængden

$$f^{-1}(e_H) = \{ z \in G \mid f(z) = e_H \}$$

til det neutrale element i H. Det er klart, at f forsvinder på sin kerne.

ISOMORFISÆTNING FOR GRUPPER. Lad $f: (G,\cdot) \to (H,\cdot)$ være en gruppehomomorfi. Da er billedet $f(G)$ en undergruppe i $(H,\cdot)$ og kernen $f^{-1}(e_H)$ er en normal undergruppe i $(G,\cdot)$. Den inducerede homomorfi er en isomorfi $\bar{f}: (G/f^{-1}(e_H),\cdot) \xrightarrow{\approx} (f(G),\cdot)$ af kvotientgruppen på billedet.

BEVIS. Vi har $e_H = f(e_G)$ og $f(x)^{-1} = f(x^{-1})$. Heraf følger let, at den stabile delmængde $f(G)$ er en undergruppe i H. For den til f hørende relation $\tilde{f}$ har vi nu

$$e_G \mathrel{\widetilde{f}} z \iff f(e_G) = f(z) \iff z \in f^{-1}(e_H)$$

Da $\widetilde{f}$ er en kongruensrelation, er $f^{-1}(e_H)$ derfor en normal undergruppe (dette kan naturligvis også let vises direkte) og $\widetilde{f}$ er relationen "kongruens modulo $f^{-1}(e_H)$".

Den sidste påstand følger nu af Isomorfisætning 6.4 ▨

BEMÆRKNING. Homomorfien f er således en sammensætning $f = \iota \circ \bar{f} \circ O$

$$\begin{array}{ccc} (G,\cdot) & \xrightarrow{\ f\ } & (H,\cdot) \\ O\downarrow & & \uparrow\iota \\ (G/f^{-1}(e),\cdot) & \xrightarrow[\approx]{\bar{f}} & (f(G),\cdot) \end{array}$$

af en surjektiv homomorfi O, en isomorfi $\bar{f}$ og en injektiv homomorfi ι.

OBSERVATION. En gruppehomomorfi $f : (G,\cdot) \to (H,\cdot)$ er injektiv, hvis og kun hvis kernen $f^{-1}(e_H)$ kun består af det neutrale element fra G, thi vi har

$$f(x) = f(y) \iff x^{-1}y \in f^{-1}(e_H).$$

NOTATION. Vi fremhæver, at i en kommutativ (additivt skrevet) gruppe $(G,+)$ er alle undergrupper normale. Enhver kongruensrelation i $(G,+)$ har formen

$$x \underset{N}{\equiv} y \overset{DEF}{\iff} y - x \in N,$$

med en undergruppe $N \subseteq G$. Sideklasserne er her delmængderne af formen

$$x + N, \quad x \in G$$

6.9. DEFINITION. Lad $(M, \square, *)$ være en mængde med kompositioner $\square$ og $*$. En ækvivalensrelation $\sim$ i M, der harmonerer med begge kompositioner kaldes også en kongruensrelation i $(M, \square, *)$. Kompositionerne $\square$ og $*$ inducerer da i kvotientmængden $M/\sim$ kompositioner betegnet $\tilde{\square}$ og $\tilde{*}$, og den kanoniske afbildning : $x \mapsto \textcircled{x}$ er en surjektiv homomorfi

$$O : (M, \square, *) \longrightarrow (M/\sim\ ,\ \tilde{\square},\ \tilde{*}).$$

Vi får øjensynlig en UDVIDELSESSÆTNING og en ISOMORFISÆTNING for mængder med to kompositioner ved at anvende de tilsvarende sætninger (6.3 og 6.4) på hver af kompositionerne.

6.10. DEFINITION. Lad $(\Lambda, +, \cdot)$ være en ring. Et ideal $\mathfrak{a}$ i Λ er da en undergruppe i den additive gruppe $(\Lambda, +)$, således at $a \cdot \mathfrak{a} \subseteq \mathfrak{a}$ og $\mathfrak{a} \cdot a \subseteq \mathfrak{a}$ for alle $a \in \Lambda$.

SÆTNING. Lad $(\Lambda, +, \cdot)$ være en ring. Kongruensrelationerne i $(\Lambda, +, \cdot)$ er da netop relationerne $\underset{\mathfrak{a}}{\equiv}$ definerede ved

$$x \underset{\mathfrak{a}}{\equiv} y \overset{\text{DEF}}{\iff} y - x \in \mathfrak{a},$$

hvor $\mathfrak{a} \subseteq \Lambda$ er et ideal.

BEVIS. Ganske som beviset for 6.5, idet også betingelse (8) i Tilføjelse 4.2 inddrages $\square$

6.11. DEFINITION. Lad $\mathfrak{a}$ være et ideal i en ring $(\Lambda, +, \cdot)$. Kongruensrelationen $\underset{\mathfrak{a}}{\equiv}$ defineret ovenfor kaldes da "kongruens modulo $\mathfrak{a}$". Da den kanoniske homomorfi $O : (\Lambda, +, \cdot) \longrightarrow (\Lambda/\underset{\mathfrak{a}}{\equiv}, +, \cdot)$ er surjektiv, følger det lut, at kvotienten, med de inducerede kompositioner $+$ og $\cdot$, igen er en ring. Den kaldes kvotientringen

af Λ m.h.t. $\mathfrak{a}$, og betegnes $\Lambda/\mathfrak{a}$.

Elementerne i kvotienten $\Lambda/\mathfrak{a}$ er ækvivalensklasserne ved $\underset{\mathfrak{a}}{\equiv}$, dvs delmængderne i Λ af formen

$$x + \mathfrak{a}, \quad x \in \Lambda.$$

De kaldes også <u>sideklasser modulo $\mathfrak{a}$</u>. Nul-elementet og et-elementet i kvotienten er sideklasserne

$$0 + \mathfrak{a} = \mathfrak{a} \quad \text{og} \quad 1 + \mathfrak{a}.$$

6.12. Idet en ringhomomorfi $f: (\Lambda,+,\cdot) \to (\Gamma,+,\cdot)$ siges at <u>forsvinde</u> på delmængden $\mathfrak{a} \subseteq \Lambda$, hvis

$$f(x) = 0 \quad \text{for } x \in \mathfrak{a},$$

får vi følgende

UDVIDELSESSÆTNING FOR RINGE. Lad $\mathfrak{a}$ være et ideal i en ring $(\Lambda,+,\cdot)$, og lad $0: (\Lambda,+,\cdot) \to (\Lambda/\mathfrak{a},+,\cdot)$ være den kanoniske homomorfi ind i kvotienten. Enhver ringhomomorfi $f: (\Lambda,+,\cdot) \to (\Gamma,+,\cdot)$, der forsvinder på $\mathfrak{a}$, kan da entydigt udvides til en ringhomomorfi $\bar{f}: (\Lambda/\mathfrak{a},+,\cdot) \to (\Gamma,+,\cdot)$ fra kvotienten.

BEVIS. Jfr. Udvidelsessætning for grupper 6.7 □

6.13. DEFINITION. For en ringhomomorfi $f: (\Lambda,+,\cdot) \to (\Gamma,+,\cdot)$ defineres <u>kernen</u> som originalmængden $f^{-1}(0)$.

ISOMORFISÆTNING FOR RINGE. Lad $f: (\Lambda,+,\cdot) \to (\Gamma,+,\cdot)$ være en ringhomomorfi. Da er billedet $f(\Lambda)$ en delring af $(\Gamma,+,\cdot)$ og kernen $f^{-1}(0)$ er et ideal i $(\Lambda,+,\cdot)$. Den inducerede homomorfi er en isomorfi

$$\bar{f}: (\Lambda/f^{-1}(0), +, \cdot) \xrightarrow{\approx} (f(\Lambda), +, \cdot)$$

af kvotienten på billedet.

BEVIS. Jfr. Isomorfisætning for grupper 6.8 □

GRUPPER

1. Gruppebegrebet. 1.1-2: Gruppe. Kommutativ gruppe. 1.3: Homomorfi etc. 1.4: Undergruppe. Undergrupper i $\mathbb{Z}$. 1.5: Venstreækvivalens. Lagrange's indexsætning. 1.6: Normal undergruppe og kvotient. 1.7: Elementorden. Undergruppen $\langle a \rangle$. 1.8: Cykliske grupper.

2. Permutationer. 2.1: Permutation. Den symmetriske gruppe. 2.2: Fixelement. 2.3: p-cykel. Transposition. 2.4: Cykelsætning. 2.5: Formler. Sætning. 2.6: Transpositionstal. Fortegn. 2.7: Lemma. Homomorfien sign. 2.8: Den alternerende gruppe. 2.9: Sætning.

3. Gruppevirkninger. Repræsentationer. 3.1: Virkning. 3.2: Repræsentation. 3.3: Restriktion. Stabil delmængde. 3.4: Baner. Isotropigruppe. Fixpunkt. 3.5: G-invariant afbildning. 3.6: Translation. 3.7: Konjugering. Centralisator. 3.8: Baners længde. 3.9: Tælleformlen. 3.10: Klasseformlen. 3.11: Burnside's formel. Baneformlen. 3.12-13: Cykeltype. Konjugeretklasser i S_n.

4. Oversigt over lineære grupper. 4.1-2: Lineære grupper. 4.3: Endelige grupper. 4.4: Specielle lineære grupper. 4.5: Kommutantgrupper. 4.6: Stabilisatorgrupper. 4.7: Ortogonale og symplektiske grupper. 4.8: Unitære grupper. 4.9: De klassiske grupper.

5. Hexaedergruppen. 5.1-2: Den regulære hexaedergruppe. 5.3-4: Hexaedergruppen. 5.5: Repræsentationer i mængden af hjørner, i mængden af kanter og i mængden af sideflader. 5.6-8: Akserepræsentationer.

6. Appendix: Permutationsproblemer. 6.1-3: En matematisk model. 6.4-5: Mønsterproblemet. 6.6: Farvning af en terning. 6.7-9: Tilladte mønstre. Invarianter for permutationsproblemer. 6.10: Solitaire-spillet. 6.11: 15-spillet. 6.12: Rubik's terning.

GRUPPER

1. Gruppebegrebet.

1.1. DEFINITION. En gruppe $(G,\cdot)$ er en mængde G med en komposition $\cdot : G\times G \to G$, betegnet $(x,y)\mapsto x\cdot y$, der er associativ, har et neutralt element og opfylder, at hvert element i G er invertibelt. Betegnes det neutrale element e, og det til elementet $x\in G$ hørende inverse x^{-1}, kan betingelserne udtrykkes ved ligningerne:

$$\boxed{\begin{aligned}(x\cdot y)\cdot z &= x\cdot(y\cdot z)\\ e\cdot x &= x\cdot e = x\\ x^{-1}\cdot x &= x\cdot x^{-1} = e\end{aligned}} \qquad x,y,z\in G.$$

Elementantallet i en gruppe kaldes også gruppens orden.

1.2. DEFINITION. En gruppe $(G,\cdot)$ kaldes kommutativ eller abelsk, hvis kompositionen er kommutativ, dvs hvis

$$\boxed{x\cdot y = y\cdot z} \quad , \quad x,y\in G.$$

NOTATION. Som betegnelse for en komposition kan anvendes ethvert bekvemt symbol. I overstående definitioner er kompositionen skrevet multiplikativt, dvs at kompositionstegnet er en "$\cdot$", som vi endda oftest udelader i det følgende. Det neutrale element i gruppen G kan betegnes e_G eller blot e eller eventuelt 1. En kommutativ gruppe kan skrives additivt, dvs at kompositionen betegnes $(x,y)\mapsto x+y$. Det neutrale element betegnes i så fald 0, og det inverse til x betegnes $-x$ og kaldes det modsatte til x.

EKSEMPEL. De hele tal udgør en kommutativ gruppe $(\mathbb{Z},+)$.

BEMÆRKNING. I en gruppe $(G,\cdot)$ defineres en modsat komposition $\overset{op}{\cdot}$ ved

$$x\overset{op}{\cdot}y := y\cdot x.$$

Det er let at se, at $(G,\overset{op}{\cdot})$ igen er en gruppe. Den kaldes G's modsatte gruppe og betegnes G^{op}. Hvis G er kommutativ, er $G^{op}=G$.

1.3. DEFINITION. En afbildning $f: H \to G$ mellem grupper $(H,\cdot)$ og $(G,\cdot)$ kaldes en (gruppe-) homomorfi, hvis

$$\boxed{f(xy) = f(x)f(y)} \qquad x, y \in H.$$

Heraf følger let, at der gælder

$$\boxed{f(e_H) = e_G} \quad \text{og} \quad \boxed{f(x^{-1}) = f(x)^{-1}} \qquad x \in H.$$

Ved kernen for en gruppehomomorfi $f: H \to G$ forstås originalmængden $f^{-1}(e_G)$. Det er let at se, at f er injektiv, netop når kernen er $f^{-1}(e_G) = \{e_H\}$.

Det er klart, at sammensætning af homomorfier $f: H \to G$ og $g: K \to H$ er en homomorfi $f \circ g: K \to G$, og at den identiske afbildning $Id_G: x \to x$ er en homomorfi $: G \to G$.

En bijektiv homomorfi $f: H \to G$ kaldes også en isomorfi (og ofte skrives $f: H \xrightarrow{\sim} G$). For en sådan er også den inverse afbildning en isomorfi $f^{-1}: G \xrightarrow{\sim} H$.

En homomorfi $f: G \to G$ kaldes en endomorfi i G, og hvis den er bijektiv også en automorfi.

BEMÆRKNING. En afbildning $f: H \to G$ mellem grupper H og G, kaldes en anti-homomorfi, hvis $f(xy) = f(y)f(x)$. Det ses, at dette gælder, netop når f er en homomorfi $: H \to G^{op}$.

1.4. DEFINITION. Ved en undergruppe i en gruppe G forstås en delmængde $H \subseteq G$, som er stabil og med sin inducerede komposition selv er en gruppe. Det følger, at inklusionsafbildningen $: x \mapsto x$, $x \in H$, så er en homomorfi $: H \hookrightarrow G$.

OBSERVATION. En delmængde $H \subseteq G$ er en undergruppe, netop når

$$\boxed{\begin{array}{l} x, y \in H \Rightarrow xy \in H \\ e \in H \\ x \in H \Rightarrow x^{-1} \in H. \end{array}}$$

De trivielle undergrupper i G er delmængderne $\{e\}$ og G.

For gruppen $(\mathbb{Z},+)$ gælder den såkaldte HOVEDIDEALSÆTNING. Undergrupperne i $(\mathbb{Z},+)$ er netop delmængderne af formen

$$H = \mathbb{Z}n = \{ pn \mid p \in \mathbb{Z} \}, \text{ hvor } n \geqslant 0.$$

Tallet n er entydigt bestemt ved undergruppen H, nemlig som $n = 0$, hvis $H = \{0\}$, og n = mindste positive tal i H, hvis $H \neq \{0\}$ □

1.5. DEFINITION. Lad H være en undergruppe i gruppen G. Den ved

$$x \sim y \overset{\text{DEF}}{\iff} x^{-1}y \in H$$

definerede relation $\sim$ i G ses da let at være en ækvivalensrelation. Den kaldes <u>venstre-ækvivalens modulo H</u>. Ækvivalensklasserne kaldes (<u>venstre</u>-) <u>sideklasser</u> modulo H, og antallet af sideklasser kaldes undergruppens <u>indeks</u> i G og betegnes $|G:H|$. Den tilhørende kvotientmængde, dvs mængden af sideklasser, betegnes G/H. Antallet af elementer i G/H er altså

$$|G/H| = |G:H|.$$

Sideklassen, der indeholder et givet element $x \in G$, er ögensynlig delmængden

$$xH = \{ xz \mid z \in H \}.$$

Da $z \mapsto xz$ definerer en bijektiv afbildning $: H \longrightarrow xH$ (med den inverse $: y \mapsto x^{-1}y$), har alle sideklasser samme elementantal som H. Da sideklasserne udgör en klassedeling af G med $|G:H|$ klasser, får vi derfor umiddelbart:

LAGRANGE'S INDEX-SÆTNING. For en undergruppe H i en gruppe G gælder:

$$|G| = |G:H| \cdot |H|$$

▨

BEMÆRKNING. For en undergruppe H i G kan vi analogt ved

$$x \underset{h}{\sim} y \overset{\text{DEF}}{\iff} yx^{-1} \in H$$

definere <u>højrækvivalens</u> modulo H, og tilsvarende <u>højresideklasser</u> af formen

$$Ha = \{ za \mid z \in H \}, \quad a \in G$$

[Huskeregel: Hø er en Højre-sideklasse]. Mængden af højresideklasser betegnes $H\backslash G$. For en højresideklasse $X \subseteq G$ er mængden $X^{-1} := \{ x^{-1} \mid x \in X \}$ en venstresideklasse. Det følger, at $X \mapsto X^{-1}$ er en bijektiv afbildning: $H\backslash G \xrightarrow{\sim} G/H$. Vi har altså specielt

$$|H\backslash G| = |G/H| = |G:H|.$$

1.6. DEFINITION. Ved en <u>normal undergruppe</u> i en gruppe G forstås en undergruppe $N \subseteq G$, således at der for alle $a \in G$ gælder:

$$\boxed{a^{-1}Na \subseteq N.}$$

OBSERVATION. De trivielle undergrupper er normale. I en kommutativ gruppe er alle undergrupper normale.

Hvis undergruppen $N \subseteq G$ er normal, er det let at se, at venstre- og højrækvivalens er samme ækvivalensrelation. Den kaldes også <u>kongruens modulo</u> N og betegnes $\underset{N}{\equiv}$.
Er dette tilfældet, kan vi i mængden G/N af sideklasser definere en komposition på følgende måde: Lad X og Y være sideklasser, og vælg repræsentanter: $X = \overline{x}$, $Y = \overline{y}$ og sæt

$$X \cdot Y = \overline{x \cdot y}$$

Da ækvivalensklassen på højresiden ikke afhænger af de foretagne valg af repræsentanter, er dette en veldefineret komposition i mængden G/N. Da den <u>kanoniske</u> afbildning: $x \mapsto \overline{x}$ øjensynlig er en homomorfi: $(G, \cdot) \to (G/N, \cdot)$ følger det let, at $(G/N, \cdot)$ er en gruppe. Den kaldes også <u>kvotientgruppen</u> af G m.h.t. den normale undergruppe N.

Følgende sætninger om grupper følger let af de tilsvarende sætninger om mængder:

UDVIDELSESSÆTNING. Lad $N \subset G$ være en normal undergruppe. En gruppehomomorfi $f: G \to K$, der forsvinder på N (dvs opfylder: $x \in N \Rightarrow f(x) = e_K$), kan da entydigt udvides til en homomorfi $\bar{f}: G/N \to K$ fra kvotienten □

Homomorfien $\bar{f}$ siges at være induceret af f.

ISOMORFISÆTNING. Lad $f: G \to K$ være en gruppehomomorfi. Da er kernen $f^{-1}(e_K)$ en normal undergruppe i G, billedet $f(G)$ er en undergruppe i K og f inducerer en isomorfi $\bar{f}: G/f^{-1}(e_K) \xrightarrow{\sim} f(G)$ af kvotienten på billedet □

1.7. Til et element a i en gruppe G kan vi betragte potenserne a^p, $p \in \mathbb{Z}$. Ifølge første potensregel er afbildningen: $p \mapsto a^p$ en gruppehomomorfi: $(\mathbb{Z}, +) \to (G, \cdot)$.

DEFINITION. Billedet ved homomorfien: $p \mapsto a^p$ kaldes undergruppen frembragt af a og betegnes $\langle a \rangle$, altså

$$\langle a \rangle := \{ \dots, a^{-2}, a^{-1}, e, a, a^2, \dots \}.$$

Det er øjensynlig den mindste undergruppe, som indeholder a. Kernen for denne homomorfi er en undergruppe i $\mathbb{Z}$, altså ifølge Sætning 1.4 af formen $\mathbb{Z}n$, hvor $n \geq 0$ er entydigt bestemt.

DEFINITION. Hvis $n > 0$, siges elementet $a \in G$ at have orden n. Hvis $n = 0$, siges elementet $a \in G$ at have uendelig orden.

Af beskrivelsen i Sætning 1.4 fås umiddelbart følgende:

RESULTAT. Elementet $a \in G$ har uendelig orden, netop når

$$a^m \neq e \quad \text{for alle } m \in \mathbb{N}.$$

I bekræftende fald er $p \mapsto a^p$ en injektiv homomorfi, og $\langle a \rangle$ er isomorf med $\mathbb{Z}$. Specielt har $\langle a \rangle$ uendelig orden.

Elementet $a \in G$ har orden n, netop når n er det

mindste naturlige tal, så at $a^n = e$.

I bekræftende fald fås af Isomorfisætning 1.6, at $\langle a \rangle$ er isomorf med kvotientgruppen $\mathbb{Z}/\mathbb{Z}n$. Specielt har $\langle a \rangle$ orden $|\mathbb{Z}/n\mathbb{Z}| = n$, og vi har

$$\langle a \rangle = \{ e, a, a^2, \cdots, a^{n-1} \}.$$

Specielt fås følgende

OBSERVATION. Undergruppen $\langle a \rangle$ har samme orden som elementet a.

KOROLLAR TIL LAGRANGE'S INDEX-SÆTNING. Et element a i en endelig gruppe G har en orden, som er divisor i G's orden, og der gælder: $\boxed{a^{|G|} = e}$.

BEVIS. Er n ordenen af a, har vi $|\langle a \rangle| = n$. Sættes $d = |G : \langle a \rangle|$ har vi derfor $|G| = |G : \langle a \rangle| \cdot |\langle a \rangle| = dn$, så n er divisor i $|G|$. Videre er $a^{|G|} = a^{nd} = (a^n)^d = e^d = e$ ▨

1.8. DEFINITION. En gruppe $(G, \cdot)$ kaldes <u>cyklisk</u>, hvis der findes et element $a \in G$, så at $G = \langle a \rangle$. Et sådant element kaldes også en <u>frembringer</u> for G.

OBSERVATION. En gruppe $(G, \cdot)$ er cyklisk, netop hvis der findes en surjektiv homomorfi : $(\mathbb{Z}, +) \to (G, \cdot)$. De cykliske grupper er altså isomorfe med $\mathbb{Z}$ eller med $\mathbb{Z}/\mathbb{Z}n$, $n \geq 1$. Specielt er de kommutative.

SÆTNING. Lad $(G, \cdot)$ være en cyklisk gruppe. Enhver undergruppe og enhver kvotientgruppe af G er da ligeledes cyklisk.

BEVIS. Lad $f : \mathbb{Z} \to G$ være en surjektiv homomorfi. For en kvotient G/N fås ved sammensætning : $\mathbb{Z} \xrightarrow{f} G \xrightarrow{\circ} G/N$ en surjektiv homomorfi, og så er G/N cyklisk. For en undergruppe H fås ved restriktion en homomorfi $f^{-1}(H) \to H$, der er surjektiv, da f var surjektiv. Her er $f^{-1}(H) \subseteq \mathbb{Z}$ en undergruppe, og dermed af formen $f^{-1}(H) = \mathbb{Z}n$, og så er $p \longmapsto pn \longmapsto f(pn)$ en surjektiv homomorfi: $\mathbb{Z} \to \mathbb{Z}n = f^{-1}(H) \to H$ ▨

2. Permutationer.

2.1. DEFINITION. Lad X være en mængde. En bijektiv afbildning $\sigma : X \to X$, af X ind i sig selv, kaldes en *automorfi* eller en *transformation* eller (især når X er endelig) en *permutation* i X. Med sammensætning som komposition udgør disse bijektive afbildninger en gruppe, kaldet den *fulde automorfi-* (eller *transformations-* eller *permutations-*) *gruppe* for X. Vi vil generelt betegne denne gruppe

$$Aut(X).$$

Det neutrale element i $Aut(X)$ er den identiske afbildning

$$1_X = Id_X : x \mapsto x.$$

For mængden $\{1, \cdots, n\}$ bruges også betegnelsen

$$S_n := Aut(\{1, \cdots, n\}).$$

Denne gruppe kaldes også *den symmetriske gruppe af grad n*. Den har øjensynlig ordenen

$$|S_n| = n!.$$

OBSERVATION. Lad $\varphi : X \to Y$ være en bijektiv afbildning. Den ved $\sigma \longmapsto \varphi \circ \sigma \circ \varphi^{-1}$ definerede afbildning

$$Aut(X) \longrightarrow Aut(Y)$$

er da en bijektiv gruppehomomorfi, altså en isomorfi. Ækvipotente mængder har derfor isomorfe automorfigrupper. Specielt er automorfigruppen for en endelig mængde X isomorf med S_n, hvor $n = |X|$.

2.2. DEFINITION. Lad σ være en permutation i X. Et element $x \in X$ kaldes *fixelement* for σ, hvis $\sigma(x) = x$. Mængden af fixelementer for σ betegnes X^σ. Permutationerne σ og τ i X kaldes *disjunkte*, når $X^\sigma \cup X^\tau = X$, dvs når komplementærmængderne $X \setminus X^\sigma$ og $X \setminus X^\tau$ er disjunkte.

OBSERVATION. Disjunkte permutationer σ og τ kommuterer, dvs opfylder, at $\sigma\tau(x) = \tau\sigma(x)$ for alle $x \in X$.

En nemlig $x \in X \setminus X^\sigma$, fås $\sigma(x) \in X \setminus X^\sigma$ (da σ er injektiv), og da $X \setminus X^\sigma \subseteq X^\tau$ får vi $\sigma\tau(x) = \sigma(x) = \tau\sigma(x)$. Tilsvarende følger påstanden når $x \in X \setminus X^\tau$, og den er helt triviel, når $x \in X^\sigma \cap X^\tau$.

2.3. DEFINITION. En permutation $\tau : X \to X$ kaldes en <u>p-cykel</u> eller en <u>cykel af længde p</u> (hvor $p \geq 2$), hvis der findes p elementer $x_1, \cdots, x_p \in X$, således at

$$\tau(x_1) = x_2, \quad \tau(x_2) = x_3, \quad \cdots, \quad \tau(x_{p-1}) = x_p, \quad \tau(x_p) = x_1$$

og $\tau(x) = x$, når $x \notin \{x_1, \cdots, x_p\}$.

Delmængden $\{x_1, \cdots, x_p\} \subseteq X$ kaldes cyklens <u>bane</u>. Den består netop af de elementer, der ikke er fix-elementer for cyklen.

OBSERVATION. En p-cykel $\tau : X \to X$ har orden p i gruppen $Aut(X)$,
thi $\tau^i(x_1) = x_{1+i}$, $1 \leq i < p$.

NOTATION. Den ovenfor beskrevne p-cykel τ betegnes (hvis misforståelser er udelukket):

$$\tau = (x_1, \cdots, x_p).$$

Bemærk, at ethvert element i banen kan optræde på førstepladsen, idet vi har

$$\tau = (x_1, x_2, \cdots, x_p) = (x_i, x_{i+1}, \cdots, x_p, x_1, \cdots, x_{i-1}).$$

En cykel af længde 2 kaldes også en <u>transposition</u>. En transposition $\tau = (x_1, x_2)$ ombytter altså x_1 og x_2 og "fixer" de øvrige elementer i X.

2.4. CYKELSÆTNING. Enhver permutation σ i en endelig mængde X kan skrives som en sammensætning af disjunkte

cykler, og bortset fra rækkefølgen af faktorerne er fremstillingen entydig.

BEMÆRKNING. Her medregnes fremstillingen af den identiske permutation som et "tomt produkt".

BEVIS. Ved fuldstændig induktion efter elementantallet i mængden $B_\sigma := X \setminus X^\sigma$ vises, at σ kan skrives som et produkt af disjunkte cykler, hvis baner "udgør" B_σ.
Lad $x_1 \in B_\sigma$. Overvej, at der findes $x_2, \cdots, x_p \in B_\sigma$, $p \geq 2$, så at $x_2 = \sigma(x_1), \cdots x_p = \sigma(x_{p-1})$, $x_1 = \sigma(x_p)$. Overvej, at vi med p-cyklen $\tau = (x_1, \cdots, x_p)$ har

$$B_{\tau^{-1}\sigma} = B_\sigma \setminus \{x_1, \cdots, x_p\}.$$

Ifølge induktionsantagelsen kan $\tau^{-1}\sigma$ derfor skrives som et produkt $\tau_1 \cdots \tau_r$ af disjunkte cykler $\tau_1, \cdots, \tau_r$, der specielt også er disjunkte med τ, og så er

$$\sigma = \tau\tau_1 \cdots \tau_r$$

den ønskede fremstilling □

2.5. FORMLER. For disjunkte cykler $(x_1, \cdots, x_p)$, $(y_1, \cdots, y_q)$, og $a \notin \{x_1, x_2\}$ gælder:

(1) $(x_1, \cdots, x_p) = (x_1, x_p)(x_1, x_{p-1}) \cdots (x_1, x_2)$,

(2) $(x_1, x_2) = (a, x_1)(a, x_2)(a, x_1)$.

(3) $(x_1, x_i) = (x_1, x_{i-1})(x_{i-1}, x_i)(x_1, x_{i-1})$, $2 \leq i \leq p$.

(4) $(x_1, x_i)(x_1, \cdots, x_p) = (x_1, \cdots, x_{i-1})(x_i, \cdots, x_p)$ $2 < i < p$.

(5) $(x_1, y_1)(x_1, \cdots, x_p)(y_1, \cdots, y_q) = (x_1, \cdots, x_p, y_1, \cdots, y_q)$.

BEVIS. Sammensæt selv □

BEMÆRKNING. Det er ofte hensigtsmæssigt for et givet element $x_1 \in X$ at lade (x_1) betegne den identiske permutation. I denne forstand er identiteten altså en 1-cykel.
Overvej, at Formel (4) [resp.(5)] bevarer sin gyldighed i "grænsetilfældene" $2 = i$ og $i = p$. [resp. $p = 1$ eller $q = 1$].

SÆTNING. (1) Enhver permutation σ i en endelig mængde X kan fremstilles som en sammensætning af transpositioner.
(2) Er $a \in X$ et givet element, kan der i fremstillingen vælges transpositioner af formen (a,x), $x \in X \setminus \{a\}$.
(3) Er $X = \{x_1, \cdots, x_n\}$ en nummerering af elementerne i X, kan der i fremstillingen vælges transpositioner af formen (x_i, x_{i+1}), $i = 1, \cdots, n-1$ ("ombytning af naboer").
BEVIS. (1): Ifølge Cykelsætning 2.4 er det nok at betragte en cykel, og for en sådan får vi fremstillingen af Formel (1).
(2): Ifølge (1) er det nok at betragte en transposition, og for en sådan får vi fremstillingen af Formel (2).
(3): Ifølge (2) er det nok at betragte en transposition af formen (x_1, x_i), og for en sådan får vi fremstillingen induktivt af Formel (3) ▨

2.6. DEFINITION. Lad σ være en permutation i den endelige mængde X, og lad os for hvert $p \in \mathbb{N}$ med $m_p = m_p(\sigma)$ betegne antallet af p-cykler, der forekommer i fremstillingen af σ som produkt af disjunkte cykler. Tallet

$$Z(\sigma) := \sum m_p (p-1)$$

vil vi kalde <u>transpositionstallet</u> for σ, og tallet

$$\operatorname{sign}(\sigma) := (-1)^{Z(\sigma)} \in \{1, -1\}$$

kaldes <u>fortegnet</u> for σ.

BEMÆRKNING. Af Formel 2.5 (1) fremgår, at en p-cykel kan fremstilles som et produkt af $p-1$ transpositioner. Det følger, at en given permutation σ <u>kan</u> fremstilles som et produkt af $Z(\sigma)$ transpositioner. En sådan fremstilling er imidlertid <u>ikke</u> entydig.

2.7. LEMMA. For en permutation σ og en transposition τ i en endelig mængde X gælder:

$$Z(\tau\sigma) = Z(\sigma) \pm 1.$$

BEVIS. For at bestemme transpositionstallet for $\tau\sigma$ vil vi ud fra fremstillingen af σ som produkt af disjunkte cykler finde den

tilsvarende fremstilling af $\tau\sigma$. I det vi medregner σ's fixpunkter som 1-cykler, udgør banerne for σ's cykler en klassedeling af X. De to elementer, der ombyttes ved transpositionen τ ligger derfor enten i samme bane eller i hver sin bane.

Tilfælde 1°: Vi kan antage, at $\sigma = (x_1, \cdots, x_p)$, $\tau = (x_1, x_i)$, $2 \le i \le p$. Formel 2.5(4) giver da den ønskede fremstilling af $\tau\sigma$. Vi ser, at

$$Z(\tau\sigma) = (i-1-1) + (p-i) = (p-1) - 1 = Z(\sigma) - 1.$$

Tilfælde 2°: Vi kan antage, at $\sigma = (x_1, \cdots, x_p)(y_1, \cdots, y_q)$, $\tau = (x_1, y_1)$. Formel 2.5(5) giver den ønskede fremstilling af $\tau\sigma$. Vi ser, at

$$Z(\tau\sigma) = p + q - 1 = (p-1) + (q-1) + 1 = Z(\sigma) + 1 \quad \blacksquare$$

BEMÆRKNING. Som nævnt i 2.6 kan en permutation σ fremstilles som et produkt af $Z(\sigma)$ transpositioner. Man kan vise, at transpositionstallet $Z(\sigma)$ angiver det minimale antal transpositioner, der er nødvendigt i en sådan fremstilling af σ.

SÆTNING. For en endelig mængde X er fortegnet en gruppehomomorfi

$$\operatorname{sign} : Aut(X) \to (\{\pm 1\}, \cdot).$$

BEVIS. Lad $\sigma, \tau \in Aut(X)$. Hvis τ er en transposition, får vi

$$\operatorname{sign}(\tau\sigma) = (-1)^{Z(\tau\sigma)} = (-1)\cdot(-1)^{Z(\sigma)} = (-1)\cdot\operatorname{sign}(\sigma).$$

I det almindelige tilfælde kan τ skrives som produkt af $z = Z(\tau)$ transpositioner, så gentagen anvendelse af det viste giver

$$\operatorname{sign}(\tau\sigma) = (-1)^z \operatorname{sign}(\sigma) = \operatorname{sign}(\tau)\operatorname{sign}(\sigma) \quad \blacksquare$$

OBSERVATION. En p-cykel har transpositionstal $p-1$ og altså fortegn $(-1)^{p-1}$! Specielt har en transposition fortegnet -1.

2.8. DEFINITION. En permutation σ i den endelige mængde X kaldes <u>lige</u> eller <u>ulige</u> eftersom transpositionstallet $Z(\sigma)$ er

lige eller ulige.

De lige permutationer er bestemt ved at de har fortegnet 1. De udgør derfor kernen for homomorfien $\text{sign}: \text{Aut}(X) \to \{\pm 1\}$, og danner altså specielt en normal undergruppe i $\text{Aut}(X)$. Hvis X har mere end 1 element (således at der findes transpositioner i X), er homomorfien $\text{Aut}(X) \to \{\pm 1\}$ surjektiv. Undergruppen af lige permutationer har derfor index 2 i $\text{Aut}(X)$. Der er altså ligemange lige og ulige permutationer.

Hvis $X = \{1, \dots, n\}$, således at $\text{Aut}(X) = S_n$ er den symmetriske gruppe af grad n, kaldes undergruppen af lige permutationer også den <u>alternerende gruppe af grad n</u>, og den betegnes A_n.

Hvis $n \geq 2$, har vi

$$|S_n : A_n| = 2, \quad S_n/A_n \cong \{\pm 1\}, \quad |A_n| = \tfrac{1}{2} n!$$

Er derimod $n = 1$, har vi $S_1 = A_1 = \{e\}$.

2.9. OBSERVATION. Er en permutation σ fremstillet som en sammensætning af transpositioner, så er den lige eller ulige, efterhånden som antallet af faktorer er lige eller ulige,
thi er a antallet af faktorer, har vi $\text{sign}(\sigma) = (-1)^a$.

SÆTNING. (1) Enhver lige permutation i en endelig mængde X kan fremstilles som sammensætning af 3-cykler.
(2) Er $a, b \in X$ to givne elementer, kan der i fremstillingen vælges 3-cykler af formen (a, b, x), $x \in X \setminus \{a, b\}$.
(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}), $i = 1, \dots, n-2$ ("cykling af 3 naboer").

BEVIS. <u>(1):</u> Det er nok at betragte et produkt $\sigma = (x_1, x_2)(y_1, y_2)$ af 2 transpositioner. Er transpositionerne disjunkte, har vi

$$\sigma = (x_1, x_2)(y_1, y_2) = (x_1, x_2, y_1)(y_1, y_2, x_2).$$

Har de ét eller to elementer fælles, må du selv prøve!

<u>(2) og (3):</u> Prøv selv. Du må gerne bruge Sætning 2.5 □

3. Gruppevirkninger. Representationer.

3.1. DEFINITION. Lad $(G,\cdot)$ være en gruppe med det neutrale element 1, og lad X være en mængde. Ved en virkning af gruppen G på mængden X forstås en afbildning $: G \times X \to X$, betegnet $(g,x) \mapsto g.x$, således at der for alle $g,h \in G$ og $x \in X$ gælder

$$(gh).x = g.(h.x)$$

$$1.x = x.$$

Er der givet en virkning af G på X siges G at virke eller at operere på X.

3.2. Er der givet en virkning af G på X kan vi for hvert element $g \in G$ betragte den ved

$$g_X : x \to g.x$$

definerede afbildning $g_X : X \to X$. Af betingelserne ovenfor følger, at afbildningen g_X er bijektiv, idet afbildningen $x \mapsto g^{-1}.x$ er dens inverse. Vi har altså $g_X \in Aut(X)$. Videre følger det af betingelserne, at den ved $g \mapsto g_X$ bestemte afbildning:

$$G \to Aut(X).$$

er en homomorfi. Med den indførte notation er 1_X = billedet af det neutrale element = den identiske afbildning: $x \mapsto x$.

DEFINITION. Homomorfien $: G \to Aut(X)$ kaldes den til virkningen hørende repræsentation af gruppen G i mængden X. Ved denne "repræsenteres" altså gruppeelementet $g \in G$ ved automorfien $g_X : X \to X$. Hvis homomorfien $: G \to Aut(X)$ er injektiv, siges repræsentationen at være tro.

Har vi omvendt givet en gruppehomomorfi:

$$\rho : G \to Aut(X),$$

ses det let, at der ved

$$g \cdot x := \rho(g)(x)$$

defineres en virkning : $G \times X \to X$. Vi får således en bijektiv forbindelse mellem virkninger af G på X og representationer : $G \to Aut(X)$.

EKSEMPEL. Den trivielle virkning af G på X er bestemt ved

$$g \cdot x := x \quad , \quad g \in G \, , \; x \in X.$$

Den tilhørende representation : $G \to Aut(X)$ er den trivielle homomorfi: $g \mapsto$ identiske afbildning.

For enhver mængde X kan vi lade den fulde automorfigruppe $Aut(X)$ virke på X ved

$$g \cdot x := g(x) \quad , \quad g \in Aut(X), \; x \in X.$$

Den tilhørende representation er den identiske homomorfi:

$$Aut(X) \xrightarrow{=} Aut(X).$$

3.3. DEFINITION. Lad der være givet en virkning : $G \times X \to X$ af G på X. For enhver undergruppe $H \subseteq G$ defineres da ved restriktion en virkning : $H \times X \to X$ af undergruppen H på X.

En delmængde $Y \subseteq X$ siges at være stabil (eller invariant) under virkningen, hvis der for alle $g \in G$ gælder

$$y \in Y \implies g \cdot y \in Y.$$

For en stabil delmængde $Y \subseteq X$ defineres ved restriktion en virkning : $G \times Y \to Y$ af G på delmængden Y.

3.4. DEFINITION. Lad der være givet en virkning af G på X.

Det er let at se, at der ved

$$x' \underset{G}{\sim} x \overset{DEF}{\iff} \exists g \in G : x' = g.x$$

defineres en ækvivalensrelation $\underset{G}{\sim}$ i mængden X. Ækvivalensklasserne herved kaldes baner. Banen, der indeholder x, er delmængden

$$G.x := \{ g.x \mid g \in G \}.$$

En banes elementantal kaldes også dens længde. Mængden af baner, altså kvotientmængden $X/\tilde{}_G$, kaldes banerummet, og betegnes

$$X/G := X/\tilde{}_G. \quad \text{(læses: "X modulo G").}$$

For et element $x \in X$ er det let at se, at delmængden

$$_xG := \{ g \in G \mid g.x = x \}$$

er en undergruppe i G. Den kaldes isotropigruppen for x.

Et element $x \in X$ siges at være fixpunkt for gruppeelementet $g \in G$ eller at være g-invariant, hvis $g.x = x$. Ofte skriver vi

$$X^g := \{ x \in X \mid g.x = x \}.$$

Et element $x \in X$ siges at være G-invariant, eller at være et fixpunkt for G's virkning, hvis

$$g.x = x, \quad \text{for alle } g \in G.$$

Ækvivalent kan dette udtrykkes ved at banen $G.x$ kun består af ét element (d: er en såkaldt ét-punkts-bane), eller ved at isotropigruppen $_xG$ er hele G. Mængden af fixpunkter for virkningen betegnes X^G, altså

$$X^G := \{ x \in X \mid \forall g \in G : g.x = x \}.$$

BEMÆRKNING. Elementerne i banerummet er delmængder af X af formen $G.x$, $x \in X$. Under visse omstændigheder er det mest naturligt at betegne banerummet $G\backslash X$ (læses: "X modulo G til venstre"). Det må imidlertid understreges, at ved alle de indførte betegnelser er det underforstået hvilken virkning, der er givet.

3,5. DEFINITION. Lad der være givet en virkning af G på mængden X, og lad Y være endnu en mængde. En afbildning $f: X \to Y$ kaldes G-invariant, hvis

$$f(g.x) = f(x), \quad x \in X, \ g \in G.$$

Dette gælder øjensynlig netop når afbildningen $f: X \to Y$ respekterer ækvivalensrelationen $\tilde{}_G$ i X. Af Udvidelsessætning for mængder fås derfor følgende:

UDVIDELSESSÆTNING. En G-invariant afbildning $f: X \to Y$ kan entydigt udvides til en afbildning $\bar{f}: X/G \to Y$ fra banerummet. ▨

BEMÆRKNING. Ved $(g.f)(x) = f(g^{-1}x)$ defineres en virkning $(g,f) \mapsto g.f$ af gruppen G på mængden $Afb(X,Y)$. Det er klart, at de G-invariante afbildninger $f: X \to Y$ netop er de elementer $f \in Afb(X,Y)$, der er fixelementer under denne virkning.

3.6. TRANSLATION. For enhver gruppe $(G,\cdot)$ kan vi definere en virkning $: G \times G \to G$ af G på sig selv ved

$$g \cdot x := gx \quad , \quad g, x \in G.$$

Denne virkning kaldes <u>venstre-translation</u>. Der er kun én bane, og for hvert element $x \in G$ er isotropigruppen triviel. Den tilhørende repræsentation er $\tau: G \to Aut(G)$.

Er $H \subseteq G$ en undergruppe, får vi ved restriktion en virkning $: H \times G \to G$. Banerne er her delmængderne

$$Hx = \{hx \mid h \in H\}, \quad x \in G,$$

altså netop højre-sideklasserne modulo H, og betegnelsen $H\backslash G$ for banerummet, jfr. Bemærkning 3.4, harmonerer således med den tidligere indførte betegnelse for mængden af højre-sideklasser.

3.7. KONJUGERING. For enhver gruppe $(G,\cdot)$ kan vi definere en virkning $: G \times G \to G$ af G på sig selv betegnet

$$(g,x) \longmapsto {}^g x := gxg^{-1}$$

Denne virkning kaldes <u>konjugering</u>. Den til virkningen hørende ækvivalensrelation $\sim$ (jfr. Definition 3.4) er bestemt ved

$$x' \sim x \overset{DEF}{\iff} \exists\, g \in G : x' = gxg^{-1}$$

Den kaldes også "<u>konjugeret med</u>". Banerne kaldes <u>konjugeret-klasser</u> eller blot <u>klasser</u> i G. Bemærk, at automorfismen $: x \mapsto {}^g x$ her er gruppeautomorfi af G.

Klassen, der indeholder $x \in G$ er altså delmængden

$$\{ gxg^{-1} \mid g \in G \} \subseteq G.$$

Isotropigruppen for $x \in G$ kaldes her <u>centralisatoren for x</u> og betegnes $C(x)$. Det er altså undergruppen

$$C(x) := \{ g \in G \mid gxg^{-1} = x \} = \{ g \in G \mid gx = xg \}.$$

Et element $x \in G$ er fixpunkt under denne virkning, hvis $gxg^{-1} = x$ for alle $g \in G$, altså hvis

$$gx = xg \quad , \quad g \in G.$$

Et sådant element kaldes også <u>centralt</u>, og mængden af centrale elementer kaldes gruppens <u>centrum</u> og betegnes $Z(G)$. Det er let at se, at centret $Z(G)$ er en undergruppe i G.

3.8. SÆTNING. *Lad der være givet en virkning af gruppen G på mængden X, og et element $x \in X$. Den ved $g \mapsto g.x$ bestemte afbildning $: G \to X$ inducerer da en bijektiv afbildning:*

$$G/_x G \xrightarrow{\sim} G.x$$

af venstresideklasserne modulo isotropigruppen ${}_xG$ på banen $G.x$.

BEVIS. Vi anvender Isomorfisætning for mængder på afbildningen $g \mapsto g.x$. Billedmængden er øjensynlig netop $G.x$. Endvidere er:

$$g'.x = g.x \iff g^{-1}g'.x = x \iff g^{-1}g' \in {}_xG,$$

så den til afbildningen hørende ækvivalensrelation i G er venstreækvivalens modulo ${}_xG$. Heraf følger påstanden. ▨

KOROLLAR. *Længden af en bane $B \subseteq X$ er bestemt ved*

$$\boxed{|B| = |G : {}_xG|, \quad x \in B,}$$

altså ved indeks af isotropigruppen for et element x i banen.

BEVIS. Når $x \in B$, er $|B| = |G.x| = |G/_x G| = |G : {}_xG|$ ▨

Når gruppen G er endelig, har altså specielt hver bane B en længde, der er divisor i gruppens orden.

3.9. TÆLLEFORMLEN. Lad der være givet en virkning af gruppen G på mængden X. Da gælder:

$$\boxed{|X| = |X^G| + \sum_j |G : x_j G|},$$

hvor $|X^G|$ er antallet af fixpunkter, og hvor der i summationen er valgt ét element x_j fra hver bane, der ikke er en ét-punkts bane.

BEVIS. Da banerne udgør en klassedeling af X, kan elementantallet $|X|$ bestemmes som summen af banernes længder. Ét-punkts-banerne bidrager her med $|X^G|$ 1-taller, og hver af de øvrige baner B_j bidrager med $|B_j| = |G : x_j G|$, $x_j \in B_j$ ▨

EKSEMPEL. Tælleformlens vigtighed beror på, at tallene i $\sum_j$ er divisorer i G's orden, og > 1.

Er der f.eks. givet en gruppe G, hvis orden er en primtalspotens:

$$|G| = p^r, \quad p \text{ primtal},$$

og en virkning af G på en endelig mængde X, så er de enkelte led i Σ_j potenser af p, og > 1, og altså specielt $\equiv 0 \mod p$. Følgelig er

$$|X| \equiv |X^G| \pmod p$$

i dette tilfælde.

3.10. For den ved konjugering (jfr. 3.7.) bestemte virkning af gruppen G på sig selv er banerne konjugeretklasserne.

Længden af en klasse $K \subseteq G$ kan derfor bestemmes ved:

$$|K| = |G : C(x)|, \quad x \in K,$$

altså som indeks af centralisatoren af et element $x \in K$. Indsættelse i Tælleformlen 3.9 giver følgende ligning, der sædvanligvis kaldes

KLASSEFORMLEN. For en gruppe G gælder:

$$\boxed{|G| = |Z(G)| + \sum_j |G : C(x_j)|},$$

hvor $|Z(G)|$ er centrets orden, og hvor der i summa-

tionen er valgt ét element x_j fra hver klasse udover centret. ▨

EKSEMPEL. En endelig gruppe G, hvis orden er en primtalspotens $|G| = p^r$, har et ikke-trivielt centrum, dvs centret indeholder mere end det neutrale element e, thi vi har: $|Z(G)| \equiv |G| \equiv 0 \pmod p$, jfr. Eksempel 3.9, og da $e \in Z(G)$, må der således være mindst p elementer i $Z(G)$.

3.11. BURNSIDE'S FORMEL. Lad der være givet en virkning af en endelig gruppe G på en mængde X. Da er antallet af baner bestemt ved

$$\boxed{|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|},$$

hvor $X^g = \{x \in X \mid g.x = x\}$, $g \in G$.

BEVIS. Lad $I \subseteq G \times X$ betegne delmængden

$$I = \{(g,x) \mid g.x = x\}.$$

Projektionerne $p: (g,x) \to g$ og $q: (g,x) \to x$ definerer da afbildninger $p: I \to G$ og $q: I \to X$, så elementantallet i I kan bestemmes som

$$\sum_{g \in G} |p^{-1}(g)| = |I| = \sum_{x \in X} |q^{-1}(x)|$$

For hvert $g \in G$ har vi $p^{-1}(g) = \{(g,x) \mid g.x = x\} \approx X^g$, og altså

$$(1): \quad |I| = \sum_{g \in G} |X^g|.$$

For hvert $x \in X$ har vi $q^{-1}(x) = \{(g,x) \mid g.x = x\} \approx {}_xG$, og altså

$$(2): \quad |I| = \sum_{x \in X} |{}_xG|.$$

Her er funktionen $x \mapsto |{}_xG|$ konstant på hver bane B, thi når $x \in B$, har vi (jfr. Korollar 3.8)

$$|{}_xG| = \frac{|G|}{|G : {}_xG|} = \frac{|G|}{|B|}.$$

Ligningen (2) kan derfor skrives

$$|I| = \sum_B \sum_{x \in B} |{}_xG| = \sum_B |B| \frac{|G|}{|B|} = |X/G| \cdot |G|,$$

og sammenligning med (1) giver det ønskede ▨

I Burnsides formel er funktionen $g \mapsto |X^g|$ konstant på hver konjugerthklasse $K \subseteq G$, thi er $g_1, g_2 \in K$, $g_2 = {}^h g_1 = hg_1h^{-1}$, definerer $x \mapsto h.x$ en bijektiv afbildning: $X^{g_1} \xrightarrow{\approx} X^{g_2}$. Er $g_0 \in K$, har vi derfor $\sum_{g \in K} |X^g| = |K| \cdot |X^{g_0}| = |G : C(g_0)| \cdot |X^{g_0}| = |G| \frac{|X^{g_0}|}{|C(g_0)|}$.

Indsættelse i Burnside's formel giver:

BANEFORMLEN. Antallet af baner er bestemt ved

$$|X/G| = \sum_i \frac{|X^{g_i}|}{|C(g_i)|},$$

hvor der i $\sum_i$ er valgt ét element g_i fra hver konjugerthklasse i G.

3.12. Lad X være en endelig mængde. Den fulde permutationsgruppe $\mathrm{Aut}(X)$ virker da på X (jfr. Eksempel 3.2), og for en permutation $\sigma \in \mathrm{Aut}(X)$ fås ved restriktion en virkning af den cykliske undergruppe $\langle \sigma \rangle$. Banerne for denne virkning af $\langle \sigma \rangle$ er delmængderne af X af formen

$$\{\sigma^i(x) \mid i \in \mathbb{Z}\}, \quad x \in X.$$

De kaldes også <u>banerne for permutationen σ</u>. Det ses, at banerne netop svarer til fremstillingen af σ som produkt af disjunkte cykler, idet fixpunkterne for σ medregnes som 1-cykler.

Betegnes for $p \in \mathbb{N}$ med $m_p = m_p(\sigma)$ antallet af baner af længde p for permutationen σ, får vi en følge

$$m_1, m_2, m_3, \cdots$$

af tal ≥ 0, der kaldes <u>cykeltypen</u> for permutationen σ. Bemærk, at $m_p = 0$, når $p > |X|$, og at

$$\sum_p p\, m_p = |X|.$$

En given cykeltype anskueliggøres ofte ved et <u>billede</u>

$$\overbrace{(*)\cdots(*)}^{m_1} \quad \overbrace{(*,*)\cdots(*,*)}^{m_2} \quad \cdots \quad \overbrace{(*,\cdots,*)\cdots}^{m_p} \quad \cdots$$

hvor der er m_1 symboler af formen $(*)$ (svarende til "1-cyklerne", dvs fixpunkterne), m_2 symboler af formen $(*,*)$ o.s.v.

For en given endelig mængde X er antallet af cykeltyper bestemt som antallet af løsninger $m_p \geq 0$ til ligningen

$$\sum_{p=1}^{\infty} p\, m_p = |X|.$$

SÆTNING. Lad X være en endelig mængde. To permutationer er da konjugerede i $\mathrm{Aut}(X)$, hvis og kun hvis de har samme cykeltype.

BEVIS. "kun hvis": Cykeltypen af σ er bestemt ved fremstillingen af σ som et produkt af disjunkte cykler. For en p-cykel $(x_1, \ldots, x_p)$ og en permutation τ har vi

$$\tau\,(x_1, \ldots, x_p)\,\tau^{-1} = (\tau(x_1), \ldots, \tau(x_p)).$$

Konjugering afbilder altså en p-cykel på en p-cykel, og da "disjunkthed" bevares, følger påstanden.

"hvis": Vælg en fremstilling af den ene permutation som produkt af disjunkte cykler (medregn fixelementerne som 1-cykler), og opskriv fremstillingen, så at den først kommer alle 1-cykler, dernæst alle 2-cykler osv. Opskriv umiddelbart herunder en tilsvarende fremstilling af den anden permutation. Da de to permutationer har samme type, står der i de to rækker en p-cykel under en p-cykel. Den permutation $: X \to X$, der bestemmes ved at et element $x \in X$ afbildes over i det element, som står umiddelbart under x i den nederste række, vil da konjugere den første permutation over i den anden således som det fremgår af udregningen under "kun hvis" ▨

3.13 For en endelig mængde X svarer konjugeretklasser K i $\mathrm{Aut}(X)$ altså til cykeltyper $(m_1, m_2, \ldots)$ med

$$\sum p\, m_p = |X|,$$

og det er således et kombinatorisk problem at bestemme antallet. Det er ligeledes et kombinatorisk problem

at bestemme, hvor mange permutationer, der har en given cykeltype, dvs at bestemme antallet af elementer i en given konjugeretklasse $K \subseteq Aut(X)$. Det sidste svarer i øvrigt til for et givet $\sigma \in K$ at bestemme hvor mange permutationer, der kommuterer med σ, idet vi har

$$|K| = |Aut(X) : C(\sigma)|$$

jfr. 3.10, hvor $C(\sigma)$ er centralisatoren for σ.

EKSEMPEL. For $|X| = 4$, hvor altså $Aut(X) \simeq S_4$ har ordn 24, får vi følgende tabel, hvor vi ud for hver type har skrevet antallet af elementer af denne type, og ordenen af centralisatoren for et element af denne type. Bemærk, at det er de sidste tal, der indgår i Banes formel 3.11.

	Type	$\lvert K_g \rvert$	$\lvert C(g) \rvert$
I	(*)(*)(*)(*)	1	24
II	(*)(*)(*,*)	6	4
III	(*)(*,*,*)	8	3
IV	(*,*)(*,*)	3	8
V	(*,*,*,*)	6	4

Der er altså 5 konjugeretklasser i S_4. Det ses, at elementer af typerne I, III og V er karakteriseret ved deres orden (som er 1, 3 og 4). Elementer af både type II og IV har orden 2. Men de kendes fra hinanden ved antallet af fixpunkter (som er 2 og 0).

Banes formel er her identiteten:

$$1 = \frac{4}{24} + \frac{2}{4} + \frac{1}{3} + \frac{0}{8} + \frac{0}{4}$$

4. Oversigt over lineære grupper.

I det følgende betegner L et legeme, og V betegner et endelig dimensionalt vektorrum over L. Med $GL(V) = Aut_L(V)$ betegnes mængden af lineære automorfier i V, dvs mængden af bijektive, lineære afbildninger $: V \to V$. Dc udgør undergruppen, kaldt den generelle lineære gruppe

$$GL(V) = Aut_L(V) \subseteq Aut(V),$$

af den fulde transformationsgruppe for mængden V.

Efter et valg af en basis i V kan endomorfierne i V beskrives ved matricer. Herved fås som bekendt en gruppeisomorfi:

$$GL(V) \cong GL_n(L), \quad \text{hvor } n = \dim V.$$

For vektorrummet $V = L^n$ vil vi altid identificere

$$GL(L^n) = GL_n(L).$$

4.1. DEFINITION. Lad G være en gruppe. Ved en lineær repræsentation af G forstås en gruppehomomorfi:

$$G \to GL(V).$$

En lineær repræsentation af G svarer altså til en virkning af G på V, hvor gruppeelementet $g \in G$ repræsenteres ved en lineær automorfi $g_V : V \to V$.

4.2. DEFINITION. Ved en lineær gruppe forstås en gruppe G, der er undergruppe i $GL(V)$ [for et passende vektorrum V].

En lineær gruppe G er således via inklusionsafbildningen $G \hookrightarrow GL(V)$ "født" med en lineær repræsentation. Det må imidlertid fremhæves, at der i studiet af en given lineær gruppe sædvanligvis vil være lineære repræsentationer udover den kanoniske, der spiller en rolle.

Hvis der til en given gruppe G findes en tro lineær repræsentation, kan vi opfatte G som en lineær

gruppe.

4.3. ENDELIGE GRUPPER. Idet vi for $n \in \mathbb{N}$ lader den symmetriske gruppe S_n virke på vektorrummet L^n ved permutation af basisvektorerne (i den kanoniske basis), får vi en tro representation

$$S_n \hookrightarrow GL_n(L).$$

Det følger, at enhver endelig gruppe kan opfattes som en lineær gruppe.

4.4. SPECIELLE LINEÆRE GRUPPER. Som bekendt er determinanten en gruppehomomorfi $\det : GL(V) \to L^*$, og dens kerne

$$SL(V) := \{\sigma \in GL(V) \mid \det(\sigma) = 1\}$$

er følgelig en lineær gruppe, kaldet <u>den specielle lineære gruppe</u>. I almindelighed sættes for en lineær gruppe G

$$SG := G \cap SL(V).$$

Specielt skrives $SL_n(L)$ for gruppen af $n \times n$-matricer med determinant 1.

EKSEMPEL. Af samme type som $SL_n(\mathbb{R})$ er gruppen $GL_n^+(\mathbb{R})$ af matricer med determinant i $\mathbb{R}_+^*$.

4.5. KOMMUTANTGRUPPER. For en endomorfi $\alpha : V \to V$ er mængden

$$GL(V, \alpha) := \{\sigma \in GL(V) \mid \sigma \circ \alpha = \alpha \circ \sigma\},$$

dvs mængden af automorfier σ, der <u>kommuterer</u> med α, åbenbart en lineær gruppe. Er $V = L^n$ således at endomorfien er givet ved en matrix $\alpha \in Mat_n(L)$ bruges betegnelsen $GL_n(L, \alpha)$. Mere generelt kan vi for en hel mængde A af endomorfier i V betragte <u>kommutanten</u>

$$GL(V, A)$$

bestående af de automorfier i V, der kommuterer med alle endomorfier $\alpha \in A$.

EKSEMPEL. Det komplekse talrum $\mathbb{C}^n$ med kanonisk basis $(e_1,\dots,e_n)$ kan også opfattes som vektorrum over $\mathbb{R}$. Via basen $(e_1,\dots,e_n,ie_1,\dots,ie_n)$ kan vi (som vektorrum over $\mathbb{R}$) identificere

$$\mathbb{C}^n = \mathbb{R}^{2n}.$$

En $\mathbb{R}$-lineær automorfi $\sigma : \mathbb{C}^n \to \mathbb{C}^n$ er ögensynlig $\mathbb{C}$-lineær, netop når $\sigma(ix) = i\sigma(x)$, $x \in V$, altså netop når σ kommuterer med homotetien $i_{\mathbb{C}^n}$. I gruppen $Aut_{\mathbb{R}}(\mathbb{C}^n)$ er altså $Aut_{\mathbb{C}}(\mathbb{C}^n)$ netop kommutantgruppen for $i_{\mathbb{C}^n}$. I basen ovenfor svarer homotetien $i_{\mathbb{C}^n}$ som $\mathbb{R}$-lineær automorfi til blokmatricen

$$J = J_n = \begin{pmatrix} 0 & -1_n \\ 1_n & 0 \end{pmatrix} \in Mat_{2n}(\mathbb{R}).$$

Den generelle lineære gruppe $GL_n(\mathbb{C})$ er altså kommutanten

$$GL_n(\mathbb{C}) = GL_{2n}(\mathbb{R}, J) = \{\sigma \in GL_{2n}(\mathbb{R}) \mid \sigma J = J\sigma\}.$$

4.6. STABILISATORGRUPPER. Lad $X \subseteq V$ være en delmængde. Mængden

$$GL(V,X) := \{\sigma \in GL(V) \mid \sigma(X) = X\}$$

af automorfier i V, som <u>stabiliserer</u> X, er da en lineær gruppe, kaldet <u>stabilisatorgruppen</u> for X.

Bemærk, at stabilisatorgruppen $GL(V,X)$ er "født" med en virkning på mængden X.

EKSEMPEL 1. Lad $S^{n-1} := \{x \in \mathbb{R}^n \mid \|x\| = 1\}$ betegne <u>enhedskuglen</u> i det euklidiske vektorrum $\mathbb{R}^n$. Stabilisator-gruppen består ögensynlig netop af de automorfier $\sigma : \mathbb{R}^n \to \mathbb{R}^n$, som opfylder:

$$\|x\| = 1 \Rightarrow \|\sigma(x)\| = 1,$$

og det gælder som bekendt netop for de ortogonale automorfier. Stabilisatorgruppen er altså den ortogonale gruppe:

$$GL_n(\mathbb{R}, S^{n-1}) = O_n(\mathbb{R})$$

og den virker på S^{n-1}!

Betragtes på en gang et helt system $F = \{X_i\}$ af delmængder $X_i \subseteq V$, kan vi betragte gruppen $GL(V, (X_i))$ af automorfier, som stabiliserer hver af mængderne X_i.

EKSEMPEL 2. Er V en direkte sum $V = V_1 \oplus V_2$ finder vi let

$$GL(V, \{V_1, V_2\}) = GL(V_1) \times GL(V_2)$$

[tænk på blokmatricer $\begin{pmatrix} \square & 0 \\ 0 & \square \end{pmatrix}$.]

EKSEMPEL 3. Er $F = \{V_i\}$ et <u>flag</u> i V, dvs en kæde

$$F: \quad V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_r$$

af underrum, kaldes stabilisatorgruppen for den tilhørende <u>flaggruppe</u>. For <u>standardflaget</u> i L^n:

$$0 \subset L \subset L^2 \subset \cdots \subset L^{n-1} \subset L^n$$

kan flaggruppen identificeres med undergruppen

$$T_n(L)^* \subseteq GL_n(L)$$

af invertible øvre trekantsmatricer. [$\begin{pmatrix} \square & \square \\ 0 & \square \end{pmatrix}$]

4.7. ORTOGONALE OG SYMPLEKTISKE GRUPPER. For en given bilinearform $\beta: V \times V \to L$ er mængden

$$O(V, \beta) := \{\sigma \in GL(V) \mid \forall x, y \in V: \beta(\sigma x, \sigma y) = \beta(x, y)\}$$

af automorfier, der <u>lader bilinearformen invariant</u>, en linear gruppe. Er $V = L^n$, og er bilinearformen givet ved en matrix $\beta \in Mat_n(L)$ bruges betegnelsen $O_n(L, \beta)$. Vi har altså

$$O_n(L, \beta) := \{\sigma \in GL_n(L) \mid \sigma^t \beta \sigma = \beta\}.$$

Hvis bilinearformen er <u>symmetrisk</u>, kaldes $O(V, \beta)$ den tilhørende <u>ortogonale gruppe</u>, og elementerne i $O(V, \beta)$ kaldes <u>ortogonale</u> m.h.t. β. Hvis legemet L har karakteristik $\neq 2$, kan en symmetrisk bilinearform udtrykkes ved den tilhørende <u>kvadratiske form</u>: $x \mapsto \beta(x, x)$, og en automorfi σ er ortogonal, når blot den lader den kvadratiske form invariant. Gruppen $SO(V, \beta)$ er den <u>specielle ortogonale gruppe</u>.

Standardeksemplet på en symmetrisk matrix er enhedsmatricen 1_n med den tilhørende kvadratiske form på L^n:

$$x \mapsto x_1^2 + \cdots + x_n^2$$

Den tilhørende ortogonale gruppe betegnes $O_n(L)$, og består af:

$$O_n(L) := \{ \sigma \in GL_n(L) \mid \sigma^t \sigma = 1_n \}$$

Mere generelt kan vi for $p+q=n$ betragte diagonalmatricen $\begin{pmatrix} 1_p & 0 \\ 0 & -1_q \end{pmatrix}$, med den tilhørende kvadratiske form

$$x \mapsto x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2$$

Den tilhørende ortogonale gruppe betegnes $O_{p,q}(L)$.

EKSEMPEL 1. Vi har velkendte geometriske beskrivelser af grupperne $O_2(\mathbb{R})$, $SO_2(\mathbb{R})$, $O_3(\mathbb{R})$, $SO_3(\mathbb{R})$. Gruppen $O_{1,3}(\mathbb{R})$ (og dens undergrupper) spiller en vigtig rolle i relativitetsteori og i ikke-euklidisk geometri.

Hvis bilinearformen β er <u>antisymmetrisk</u>, skrives oftest

$$Sp(V,\beta) := \{ \sigma \in GL(V) \mid \forall x,y : \beta(\sigma.x, \sigma.y) = \beta(x,y) \},$$

og denne gruppe kaldes den tilhørende <u>symplektiske gruppe</u>. Dens elementer kaldes <u>symplektiske</u> m.h.t. β. Er $V = L^n$ skrives

$$Sp_n(L,\beta) = \{ \sigma \in GL_n(L) \mid \sigma^t \beta \sigma = \beta \}.$$

Standardeksemplet på en antisymmetrisk matrix er matricen $J_n = \begin{pmatrix} 0 & -1_n \\ 1_n & 0 \end{pmatrix} \in Mat_{2n}(L)$. For den tilhørende symplektiske gruppe skrives blot

$$Sp_{2n}(L) := \{ \sigma \in GL_{2n}(L) \mid \sigma^t J_n \sigma = J_n \}.$$

BEMÆRKNING. Af en matrixligning $\sigma^t \beta \sigma = \beta$ får vi øjensynlig $(\det\beta)(\det\sigma)^2 = \det(\beta)$. Af $\sigma \in O(V,\beta)$, hvor bilinearformen er <u>regulær</u>, dvs svarende til en matrix med determinant $\neq 0$, følger derfor $\det(\sigma) = \pm 1$. Hvis bilinearformen er regulær og antisymmetrisk, <u>kan man vise</u>, at der altid gælder $\det(\sigma) = 1$. Specielt er altså

$$Sp_{2n}(L) \subseteq SL_{2n}(L),$$

(og for $n=1$ gælder faktisk $Sp_2(L) = SL_2(L)$).

EKSEMPEL 2. Bemærk ligheden og forskellen i definitionen af $GL_{2n}(\mathbb{R}, J_n)$ (jfr. Eksempel 4.5) og $Sp_{2n}(\mathbb{R})$. Hvis $\sigma \in O_{2n}(\mathbb{R})$ har vi $\sigma^t \sigma = 1$, og altså

$$\sigma J = J\sigma \iff \sigma^t J \sigma = J.$$

Vi har derfor i gruppen $GL_{2n}(\mathbb{R})$, jfr. Eksempel 4.5, at

$$GL_n(\mathbb{C}) \cap O_{2n}(\mathbb{R}) = GL_{2n}(\mathbb{R}, J) \cap O_{2n}(\mathbb{R}) = Sp_{2n}(\mathbb{R}) \cap O_{2n}(\mathbb{R}).$$

Denne gruppe består af de $\mathbb{C}$-lineære automorfier i $\mathbb{C}^n$, der er afstandsbevarende, dvs netop af de unitære automorfier i $\mathbb{C}^n$, og disse kan altså karakteriseres som de automorfier i $\mathbb{R}^{2n}$ der er både symplektiske og ortogonale.

4.8. UNITÆRE GRUPPER. Uden at gå i detaljer fremhæver vi, at en del af de foregående definitioner umiddelbart kan overføres til skævlegemer. De efterfølgende definitioner, som har klassiske anvendelser på kvaternionskævlegemet $\mathbb{H}$, vil vi formulere således at de umiddelbart kan anvendes også i en ikke-kommutativ situation.

Antag at der i L er givet en konjugering, dvs en afbildning $\lambda \mapsto \bar{\lambda}$ af L ind i sig selv, som opfylder

$$\overline{\lambda+\mu} = \bar{\lambda}+\bar{\mu}, \quad \overline{\lambda\mu} = \bar{\mu}\bar{\lambda}, \quad \bar{1} = 1, \quad \bar{\bar{\lambda}} = \lambda.$$

[Eksempler: I ethvert legeme L (specielt i $\mathbb{R}$): identiteten, i $\mathbb{C}$: komplekse konjugering, i $\mathbb{H}$: kvaternionkonjugering]

En hermite'sk form h på et vektorrum V over L er da en afbildning $h: V \times V \to L$, som opfylder

$$h(x+y,z) = h(x,z)+h(y,z), \quad h(\lambda x,z) = \lambda h(x,z), \quad \overline{h(x,z)} = h(z,x).$$

For en given hermite'sk form h er mængden

$$U(V,h) := \{\sigma \in GL(V) \mid \forall x,z \in V: h(\sigma x, \sigma z) = h(x,z)\}$$

en lineær gruppe, kaldet den til h hørende unitære gruppe. Dens elementer kaldes unitære m.h.t. h. Er $V = L^n$, og er formen givet ved en hermite'sk matrix h (dvs $h^* = h$) skrives

$$U_n(L,h) := \{\sigma \in GL_n(L) \mid \sigma^* h \bar{\sigma} = h\}.$$

Standardeksemplet på en hermite'sk matrix er enhedsmatricen 1_n svarende til formen

$$(x,y) \mapsto x_1\bar{y}_1 + \cdots + x_n\bar{y}_n.$$

Den tilhørende unitære gruppe betegnes $U_n(L)$ og består af:

$$U_n(L) := \{\sigma \in GL_n(L) \mid \sigma^* \sigma = 1\}.$$

4.9. DE KLASSISKE GRUPPER er de unitære grupper $U_n(L)$ for de "klassiske" legemer $\mathbb{R}, \mathbb{C}, \mathbb{H}$.

For $L = \mathbb{R}$ fås gruppen

$$O(n) := U_n(\mathbb{R}) = O_n(\mathbb{R}),$$ den ortogonale gruppe.

For $L = \mathbb{C}$ fås gruppen

$$U(n) := U_n(\mathbb{C}),$$ den unitære gruppe.

For $L = \mathbb{H}$ fås gruppen

$$Sp(n) := U_n(\mathbb{H}),$$ den symplektiske gruppe.

For $n = 1$ er

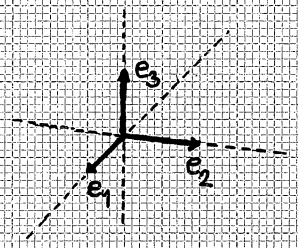
$O(1) = \{\pm 1\}$ de to reelle "enheder", og

$U(1) = \{z \in \mathbb{C}^* \mid |z| = 1\}$ er de komplekse "enheder", og

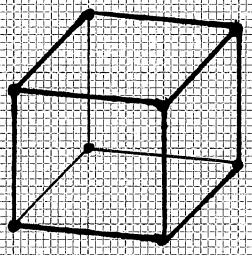
$Sp(1) = \{z \in \mathbb{H}^* \mid z\bar{z} = 1\}$ er "kvaternionenhederne".

BEMÆRKNING. Den tilsyneladende sproglige uoverensstemmelse mellem navnene på $Sp(n)$ og gruppern $Sp(V, \beta)$ er ikke så alvorlig, idet man kan opfatte $Sp(n)$ som en undergruppe i $GL(\mathbb{R}^{4n})$ bestående af automorfier som på én gang er ortogonale og symplektiske med hensyn til 3 forskellige symplektiske strukturer på $\mathbb{R}^{4n}$, jfr. Eksempel 4.7.2.

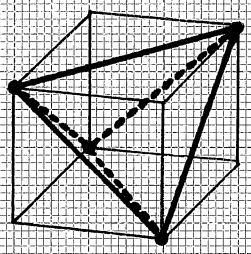
HEXAEDERGRUPPEN



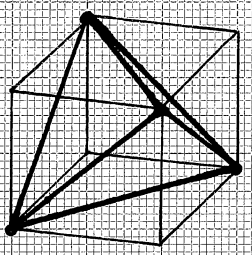
Den ortonormale basis



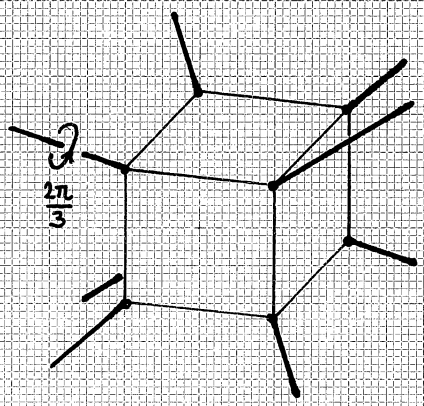
Hexaederet X



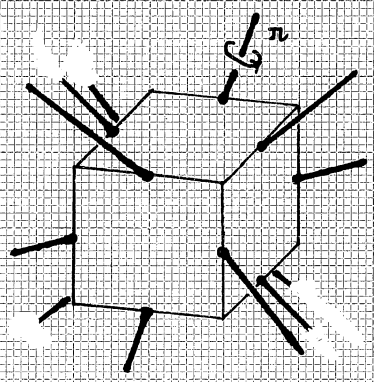
Tetraederet Δ



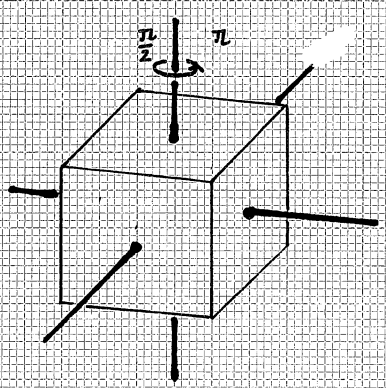
-og det modsatte -Δ



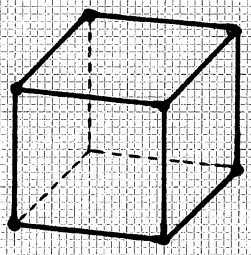
4 hjørneakser Y_0



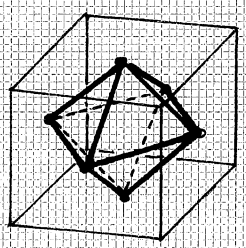
6 kantakser Y_1



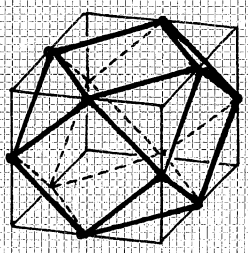
3 fladeakser Y_2



X : Hexaederet



X_2 : Oktaederet



X_1 : "Hexaoktaederet"

5. Hexaedergruppen $= S_4$.

5.1. I det sædvanlige euklidiske talrum $\mathbb{R}^3$ med den kanoniske basis (e_1, e_2, e_3) betragtes delmængden X bestående af de 8 vektorer af formen

$$X = \{ \pm e_1 \pm e_2 \pm e_3 \},$$

og den tilhørende stabilisatorgruppe betegnet

$$\tilde{H} := \{ \sigma \in GL_3(\mathbb{R}) \mid \sigma(X) = X \}.$$

De 8 vektorer i X kan opfattes som hjørnerne i et hexaeder (= terning), og $\tilde{H}$ kaldes den uegentlige hexaedergruppe.

Blandt de 8 hjørner i hexaederet kan vi udtage et såkaldt tetraeder, dvs en delmængde $\Delta \subseteq X$ bestående af (a) 4 vektorer $\Delta = \{ v_0, v_1, v_2, v_3 \}$, (b) som frembringer $\mathbb{R}^3$ og (c) opfylder $v_0 + v_1 + v_2 + v_3 = 0$. Stabilisatorgruppen for Δ, betegnet

$$\tilde{T} := \{ \sigma \in GL_3(\mathbb{R}) \mid \sigma(\Delta) = \Delta \},$$

kaldes den uegentlige tetraedergruppe.

OBSERVATION. Blandt hjørnerne i X kan vi udtage præcis 2 tetraedre, nemlig med Δ også $-\Delta := \{ -v_0, -v_1, -v_2, -v_3 \}$. Gruppen $\tilde{T} \subseteq GL_3(\mathbb{R})$ afhænger således ikke af hvilke af de 2 tetraedre $\subseteq X$ vi har valgt.

BEMÆRKNING. En lineær automorfi respekterer betingelserne (a), (b) og (c), og afbilder altså tetraeder på tetraeder.

5.2. DEN UEGENTLIGE HEXAEDERGRUPPE $\tilde{H}$ har ordnen 48. Den indeholder den uegentlige tetraedergruppe $\tilde{T}$ som en normal undergruppe af ordnen 24. Gruppehomomorfien $: \tilde{T} \to Aut(\Delta)$, som til en tetraedervautomorfi knytter den tilsvarende permutation af tetraederets 4 hjørner, er en isomorfi:

$$\tilde{T} \xrightarrow{\simeq} Aut(\Delta) \simeq S_4.$$

BEVIS. Udfra en basis (v_1, v_2, v_3) for $\mathbb{R}^3$ er en (lineær) automorfi σ i $\mathbb{R}^3$ helt bestemt ved de tre (lineært uafhængige) billedvektorer (w_1, w_2, w_3). Vælg nu som basis 3 af vektorerne i et tetraeder $\Delta \subseteq X$. Da er σ en hexaedervautomorfi, hvis og kun hvis billedvektorerne (w_1, w_2, w_3) alle tilhører

et tetraeder $\Delta' \subseteq X$. Der er således 8 muligheder for w_1 (nemlig $w_1 \in X$), for hver af dem er der 3 muligheder for w_2 ($w_2 \in$ samme tetraeder som w_1), og for hver af dem er der 2 muligheder for w_3 ($w_3 \in$ samme tetraeder som w_1, w_2). I alt er der altså $8 \cdot 3 \cdot 2 = 48$ muligheder for (w_1, w_2, w_3), og dermed 48 elementer i $\tilde{H}$.

Gruppen $\tilde{H} \cap \tilde{T}$ består af de hexaederautomorfier, der stabiliserer Δ. Da enhver hexaederautomorfi enten stabiliserer Δ (og $-\Delta$) eller ombytter Δ og $-\Delta$, må $\tilde{H} \cap \tilde{T}$ være en normal undergruppe i $\tilde{H}$ af index 1 eller 2. Specielt er altså $$|\tilde{T}| \geqslant |\tilde{H} \cap \tilde{T}| \geqslant \tfrac{1}{2}|\tilde{H}| = 24.$$

På den anden side er er den angivne homomorfi: $\tilde{T} \to S_4$ øjensynlig injektiv, hvoraf $$|\tilde{T}| \leqslant |S_4| = 24.$$

Følgelig gælder "=" 'ene, og dét er netop påstandene □

OBSERVATION. Hexaederautomorfierne er ortogonale transformationer. Dette følger måske nemmest ved at bemærke, at vinklen θ mellem to vektorer fra X, der ligger i samme tetraeder, er konstant (og bestemt ved $\cos\theta = -\frac{1}{3}$), og at hexaederautomorfierne bevarer tetraedre.

5.3. De hexaederautomorfier, som er egentlige ortogonale transformationer, udgør undergruppen $$H := \tilde{H} \cap SO_3(\mathbb{R}),$$ der kaldes den (egentlige) <u>hexaedergruppe</u>. Tilsvarende defineres den (egentlige) <u>tetraedergruppe</u> $$T := \tilde{T} \cap SO_3(\mathbb{R}).$$

OBSERVATION. Da hexaederautomorfierne som nævnt er ortogonale, og altså har $\det = \pm 1$, er hexaedergruppen kerne for homomorfien $$\det : \tilde{H} \to \{\pm 1\},$$ og da $-1 \in \tilde{H}$ har $\det(-1) = -1$, er denne homomorfi surjek-

tiv. Følgelig er $H \subseteq \tilde{H}$ en normal undergruppe af index 2. Specielt har den ordnen

$$|H| = 24.$$

5.4. Vi minder om, at enhver egentlig ortogonal transformation $\neq 1$ i $\mathbb{R}^3$ er en drejning om en akse (dvs et 1-dimensionalt underrum bestående af fix-vektorer). Af sådanne mulige akser har hexaederet følgende symmetriakser:

4 hjørneakser, dvs akser gennem 0 og et hjørne,
6 kantakser, dvs akser gennem 0 og midtpunktet af en kant, og
3 fladeakser, dvs akser gennem 0 og midtpunktet af en sideflade.

Fladeakserne er ligesynlig de 3 koordinatakser.

HEXAEDERGRUPPEN H har ordnen 24. Den består af drejningerne i følgende 5 klasser:

Klasse I:	1	identitet
Klasse II:	6	$\frac{1}{2}$-drejninger (d: med vinkel $\frac{2\pi}{2}$) om en kantakse.
Klasse III:	8	$\frac{1}{3}$-drejninger (d: med vinkler $\pm\frac{2\pi}{3}$) om en hjørneakse
Klasse IV	3	$\frac{1}{2}$-drejninger om en fladeakse
Klasse V	6	$\frac{1}{4}$-drejninger (d: med vinkel $\frac{2\pi}{4}$) om en fladeakse.

Tetraedergruppen T er en normal undergruppe af ordnen 12 bestående af drejningerne i klasserne I, III og V.

BEVIS. De anførte 24 drejninger tilhører ligesynlig H, og da $|H| = 24$, udgør de hele H. Da $\tilde{T} \subseteq \tilde{H}$, har vi $T = H \cap \tilde{T}$, og da T er kerne for homomorfien $\det : \tilde{T} \to \{\pm 1\}$, har vi $|T| = 12$ eller $|T| = 24$. Det er let at udelukke den sidste mulighed. Mere præcist er det let at indse, at drejningerne i klasserne II og V ikke tilhører T (find blot et hjørne i Δ, som afbildes over i et hjørne, der ikke ligger i Δ), og så må de resterende 12 drejninger udgøre T ▨

BEMÆRKNING. De 24 automorfier af formen $-\sigma = (-1)\circ\sigma$, $\sigma \in H$, tilhører $\tilde{H}$ og har $\det = -1$. De må derfor udgøre $\tilde{H} \setminus H$, så

$$\tilde{H} = H \cup (-1)H.$$

Da de 12 automorfier af formen σ, $\sigma \in H \setminus T$ vil ombytte Δ og $-\Delta$, vil automorfierne $-\sigma = (-1)\sigma$, $\sigma \in H \setminus T$ tilsvarende udgøre $\tilde{T} \setminus T$.

5.5. Den uegentlige hexaedergruppe $\tilde{H}$ er "født" med en virkning på mængden X af hexaedrets 8 hjørner, svarende til repræsentationen:

$$\tilde{H} \longrightarrow Aut(X) = S_8,$$

som åbenbart er injektiv.

Tilsvarende vil en hexaedervautomorfi permutere mængden X_1 bestående af (midtpunkterne af) hexaederets 12 kanter. Herved fås en repræsentation:

$$\tilde{H} \longrightarrow Aut(X_1) = S_{12},$$

som let ses at være injektiv.

Endelig vil en hexaedervautomorfi permutere mængden X_2 bestående af (midtpunkterne af) hexaederets 6 sideflader. Herved fås en repræsentation:

$$\tilde{H} \longrightarrow Aut(X_2) = S_6,$$

som også ses at være injektiv.

BEMÆRKNING. De 6 vektorer i X_2 er netop vektorerne

$$\pm e_1, \pm e_2, \pm e_3,$$

og de 48 hexaedervautomorfier stabiliserer altså denne mængde. Omvendt ses, at stabilisatorgruppen for X_2 har orden $6 \cdot 4 \cdot 2 = 48$ [(jfr. udregningen i 5.2): For billedet u_1 af e_1 er der 6 muligheder (nemlig $u_1 \in X_2$), for hver af dem er der 4 muligheder for billedet u_2 af e_2 (nemlig $u_2 \in X_2 \setminus \{\pm u_1\}$), og for hver af dem er der 2 muligheder for billedet af e_3].

De 6 vektorer $\pm e_1, \pm e_2, \pm e_3$ udgør hjørnerne i et <u>oktaeder</u>. Da den uegentlige hexaedergruppe ifølge det foregående netop er stabilisatorgruppen herfor, kaldes den også den <u>uegentlige oktaedergruppe</u>, og hexaedergruppen H kaldes også <u>oktaedergruppen</u>.

5.6. En hexaedervautomorfi vil også permutere hexaederets symmetriakser. Betegner vi således med Y_0 mængden, hvis 4 elementer er de 4 hjørneakser, får vi herved en representation: $\tilde{H} \to Aut(Y_0) = S_4$. Herom gælder:

"HJØRNEAKSEREPRÆSENTATIONEN": $\tilde{H} \to Aut(Y_0) = S_4$ er surjektiv med kerne $= \{\pm 1\}$. Dens restriktion til hexaedergruppen H er en isomorfi:

$$H \xrightarrow{\approx} S_4,$$

og herunder svarer tetraedergruppen $T \subseteq H$ til den alternerende gruppe $A_4 \subseteq S_4$. De 5 klasser i H (jfr. 5.4) svarer herved netop til konjugeretklasserne i S_4, efter følgende skema

	Drejningstype	Cykeltype	Antal
I	Identiteten $(=1)$	$(*)(*)(*)(*)$	1
II	$\frac{1}{2}$-drejning om kantakse	$(*)(*)(*,*)$	6
III	$\frac{1}{3}$-drejning om hjørneakse	$(*)(*,*,*)$	8
IV	$\frac{1}{2}$-drejning om fladeakse	$(*,*)(*,*)$	3
V	$\frac{1}{4}$-drejning om fladeakse	$(*,*,*,*)$	6

BEVIS. At en hexaedervautomorfi σ tilhører kernen for $\tilde{H} \to Aut(Y_0)$ betyder, at hvert af de 4 1-dimensionale underrum, som Y_0 består af, er invariante, og dermed egenvektorer for σ. Da σ er ortogonal, og da disse 1-dimensionale underrum <u>ikke</u> er ortogonale (jfr. Observation 5.2) betyder dette, at $\sigma = \pm 1$.

Da kernen således har orden 2, har billedgruppen orden $\frac{1}{2} \cdot 48 = 24$, og den må derfor være hele $Aut(Y_0) = S_4$.

Restriktionen til H må være injektiv, da $-1 \notin H$, og følgelig bijektiv, da $|H| = 24 = |S_4|$.

Påstanden om konjugeringsklasserne ses enten direkte, eller ved at se på ordenerne af de 24 drejninger. Heraf følger også at T svarer til A_4, thi T består af drejningerne i klasserne I, <u>III</u> og <u>V</u> (jfr. 5.4) og de svarer ifølge skemaet netop til de lige permutationer i S_4 □

5.7. Betegner vi tilsvarende med Y_2 mængden, hvis 3 elementer er de 3 fladeaksen (d: koordinatakserne), får vi en repræsentation : $\tilde{H} \to Aut(Y_2) = S_3$, og ved restriktion en repræsentation: $H \to Aut(Y_2) = S_3$. Herom gælder:

"FLADEAKSEREPRÆSENTATIONEN" : $H \to Aut(Y_2) = S_3$ er surjektiv, og dens kerne V er en normal undergruppe i H, bestående af identiteten og de 3 $\frac{1}{2}$-drejninger fra klasse IV.

BEVIS. Repræsentationen er surjektiv, thi er $\tau \in S_3$ en permutation, defineres ved: $(e_1, e_2, e_3) \mapsto (e_{\tau(1)}, e_{\tau(2)}, e_{\tau(3)})$ og $(e_1, e_2, e_3) \mapsto (-e_{\tau(1)}, -e_{\tau(2)}, -e_{\tau(3)})$ 2 hexaedervantomorfier, hvoraf 1 må være en drejning, som begge afbilder over i τ. Kernen V er følgelig en normal undergruppe af orden $|V| = |H| : |S_3| = 24 : 6 = 4$. Da V er normal, vil V med et element σ også indeholde alle elementer konjugerede med σ, og derfor en hel konjugeretklasse. Da $|V| = 4$, er det kun muligt for klasse IV. □

BEMÆRKNINGER. Gruppen V kaldes <u>Klein's fire-gruppe</u> [Tysk: Vier = fire]. Vi har $V \subseteq T \subseteq H$. Via isomorfien : $H \xrightarrow{\approx} S_4$ svarer V til undergruppen (også betegnet V) i S_4 bestående af identiteten og de 3 <u>"dobbelt-transpositioner"</u> af type $(*,*)(*,*)$. Denne undergruppe er altså normal i S_4, og af det ovenstående får vi en isomorfi:

$$S_4 / V \xrightarrow{\approx} S_3.$$

5.8. SIDEBEMÆRKNING. Betegner vi endelig med Y_1 mængden, hvis 3 elementer er de 6 kantakser, fås tilsvarende en injektiv "kantakserepræsentation" : $H \to Aut(Y_1) = S_6$. Man kan vise, at den er "forskellig" fra repræsentationen : $H \to Aut(X_2) = S_6$ defineret i 5.5.

6. Appendix: Permutationsproblemer.

6.1. Når man til daglig taler om permutationer, tænker man sædvanligvis på, at der er givet en "placering" af nogle "genstande" (brikker, hatte, farvede kugler, mennesker, atomkerner, tal, stjerner) på en samling "pladser" (felter, knager, skåle, værelser, koordinater i $\mathbb{R}^4$, konti, retninger). Ved en "permutation" (omflytning, ombytning, rokering, omordning) flyttes så (nogle af) disse genstande hen på andre pladser, hvorved der fremkommer en ny placering.

6.2. EN MATEMATISK MODEL af denne situation får vi ved at tænke på genstandene som en mængde F, på pladserne som en mængde P og ved at fortolke placeringer som afbildninger

$$x : P \to F,$$

idet vi for hver plads $p \in P$ fortolker afbildningens værdi $x(p) \in F$ som den genstand, der er placeret på pladsen p.

En permutation fortolkes så som en bijektiv afbildning

$$\sigma : P \to P, \quad \text{idet} \quad p \longmapsto \sigma(p)$$

fortæller, at genstanden på pladsen p skal flyttes hen på pladsen $\sigma(p)$.

I denne beskrivelse forudsættes ikke nødvendigvis, at afbildningen $x : P \to F$ er injektiv. Den "samme" genstand kan således være placeret på flere forskellige pladser (svarende til at genstandene kunne være farvede kugler). Vi vil i overensstemmelse hermed tænke på elementerne i F som farver, på elementerne i P som pladser og placeringerne $x : P \to F$, altså elementerne i $\mathrm{Afb}(P,F)$, vil vi kalde mønstre. En permutation er således en permutation af pladserne, dvs element i gruppen $\mathrm{Aut}(P)$.

Læg vel mærke til at vi ved at udføre permutationen $\sigma : P \to P$ på mønsteret $x : P \to F$ får mønsteret

$$x \circ \sigma^{-1} : P \to F.$$

OBSERVATION. Ved fastsættelsen

$$\sigma . x = x \circ \sigma^{-1} : P \to F$$

defineres en <u>virkning</u> af gruppen $Aut(P)$ af permutationer på mængden $Afb(P,F)$ af mønstre.

<u>Isotropigruppen</u> for et mønster x består af de permutationer, hvis virkning ikke kan ses på x, og <u>banen</u> for et mønster x består af de mønstre, som x kan forandres til under brug af alle permutationer.

6.3. BEMÆRKNINGER (1). I daglig tale kan man tillade sig at betragte placeringer, hvor nogle af pladserne er "tomme". Dette kan vi beskrive i modellen ved til farverne F at <u>tilføje</u> en "farvelös" farve.

(2) Man kan også - således som man gør i visse spil - tillade sig at fjerne nogle af genstandene fra en given placering. Dette beskrives i modellen ved til pladserne at <u>tilføje</u> en række "afsætningspladser". At fjerne en genstand svarer så til at ombytte en genstand på en af de oprindelige pladser med en "farvelös" genstand fra en af afsætningspladserne.

6.4. MØNSTERPROBLEMET. Et klassisk problem består i at tælle antallet af forskellige mønstre. Forudsætter vi, at P og F er endelige mængder, så er naturligvis også mængden

$$X := Afb(P,F)$$

af mønstre endelig, med

$$|X| = |F|^{|P|}$$

elementer. Ofte vil man imidlertid betragte 2 mønstre x', x som det samme mønster, hvis x' fremgår af x ved at anvende en permutation σ, altså hvis

$$x' = \sigma . x , \quad \sigma \in Aut(P).$$

Dette betyder netop, at x' og x tilhører samme bane ved den ovenfor definerede virkning af $Aut(P)$ på X,

og mønsterproblemet svarer således til at tælle antallet af baner. For hertil at anvende Burnside's formel 3.11, skal vi betragte mønstre, der er invariante ved en given permutation $\sigma \in Aut(P)$.

SÆTNING. Lad $\sigma \in Aut(P)$ være en permutation. Et mønster $x : P \to F$ er da σ-invariant, netop når (afbildningen) x er konstant på hver af σ's baner.

BEVIS. At mønsteret x er σ-invariant betyder, at $\sigma . x = x$, altså at

$$x(\sigma^{-1}(p)) = x(p) \quad \text{for alle } p \in P.$$

Dette gælder netop når afbildningen $x : P \to F$ er konstant på delmængderne af formen $\{\sigma^i(p) \mid i \in \mathbb{Z}\}$, og disse delmængder er jo netop σ's baner, jfr. 3.12 ▨

KOROLLAR. Antallet af mønstre $x : P \to F$, der er σ-invariante er

$$|F|^{m_1 + m_2 + \cdots},$$

hvor $(m_1, m_2, \ldots)$ er cykeltypen for σ.

BEVIS. Antallet af baner for σ er $m_1 + m_2 + \cdots$ ▨

6.5. Ofte betragtes i mønsterproblemet i stedet for alle permutationer af pladserne en virkning af en given gruppe G på mængden P af pladser. Ved definitionen

$$g . x = x \circ g_P^{-1}, \quad g \in G, \quad x \in Afb(P, F)$$

fås en virkning af G på mængden $X = Afb(P, F)$ af mønstre, og mønstre betragtes som ens, hvis de er ækvivalente under denne virkning.

SÆTNING. Antallet af mønstre m.h.t. G's virkning er:

$$\boxed{|X/G| = \frac{1}{|G|} \sum_{g \in G} |F|^{m(g)}},$$

hvor $m(g) = m_1 + m_2 + \cdots$ og $(m_1, m_2, \ldots)$ er cykeltypen for permutationen $g_P \in Aut(P)$.

BEVIS. Følger umiddelbart af Burnside's formel 3.11 ▨

BEMÆRKNING. Ofte kan optællingen ovenfor systematiseres. Kender vi konjugeretklasserne i G behøver vi jo kun at beregne $|X^g|$ for ét element g fra hver konjugeretklasse, jfr. Banеformlen 3.11. En tilsvarende reduktion opnås, hvis vi for hver af de mulige cykeltyper $(m_1, m_2, \dots)$ kender antallet af gruppeelementer $g \in G$, for hvilke permutationen g_P har denne type.

6.6. EKSEMPEL. FARVNINGER AF EN TERNING. De 6 sider på en terning må farves med N givne farver. Bestem antallet $a(N)$ af forskellige mønstre, der kan fremkomme.

SVAR. Der er 6 pladser, så på en fast terning har mængden X af mønstre N^6 elementer. Her er det nemeligt at regne to mønstre for det samme, hvis det ene fremkommer af det andet ved at "trille" med terningen. Vi skal derfor betragte den velkendte virkning af Hexaedergruppen H på terningens 6 sider, og vi skal for hver hexaederdrejning $g \in H$ undersøge den tilsvarende permutation g_P af terningens 6 sideflader.

Hexaederdrejn. g	Cykeltype for g_P	$m_1+m_2+\dots$	$\lvert C(g)\rvert$
Identiteten	$(*)(*)(*)(*)(*)(*) \leftrightarrow (6,0,0,0,\dots)$	6	24
$\frac{1}{2}$-drejning om kant	$(*,*)(*,*)(*,*) \leftrightarrow (0,3,0,0,\dots)$	3	4
$\frac{1}{3}$-drejning om hjørne	$(*,*,*)(*,*,*) \leftrightarrow (0,0,2,0,\dots)$	2	3
$\frac{1}{2}$-drejning om side	$(*)(*)(*,*)(*,*) \leftrightarrow (2,2,0,0,\dots)$	4	8
$\frac{1}{4}$-drejning om side	$(*)(*)(*,*,*,*) \leftrightarrow (2,0,0,1,\dots)$	3	4

hvor sidste søjle er ordenen af centralisatoren for g i H. Af banеformlen følger nu:

$$a(N) = \frac{N^6}{24} + \frac{N^3}{4} + \frac{N^2}{3} + \frac{N^4}{8} + \frac{N^3}{4}$$

6.7. Ofte møder man i forbindelse med permutationer følgende mere kompliceret situation: Svarende til en given mængde P af pladser og en given mængde F af farver betragtes ikke alle mønstre, men kun en delmængde

$$M \subseteq Aff(P,F),$$

som vi vil kalde de <u>tilladte mønstre</u>. Endvidere betragtes kun visse <u>tilladte permutationer</u>, og her kan det yderligere være tilfældet, at "tilladeligheden" af en permutation afhænger af hvilket mønster, den skal anvendes på. I almindelighed vil der således for hvert tilladt mønster $x \in M$ være givet en delmængde

$$R(x) \subseteq Aut(P),$$

af permutationer, som det er tilladt at anvende på x. Vi vil altid forudsætte, at der gælder

$$(*) \quad x \in M \wedge \sigma \in R(x) \Rightarrow \sigma.x \in M.$$

I denne situation sætter vi:

$$\tilde{R}(x) := \{\sigma_n \circ \cdots \circ \sigma_1 \mid n \in \mathbb{N} \wedge \sigma_1 \in R(x) \wedge \sigma_2 \in R(\sigma_1.x) \wedge \cdots \wedge \sigma_n \in R(\sigma_{n-1} \cdots \sigma_1.x)\}$$

og for tilladte mønstre $x, x' \in M$ skriver vi:

$$x \to x' \overset{DEF}{\iff} \exists \tau \in \tilde{R}(x) : \tau.x = x'.$$

Delmængden $\tilde{R}(x) \subseteq Aut(P)$ består således af permutationer, der kan sammensættes af tilladte permutationer, og relationen $x \to x'$ udtrykker, at man kan komme fra x til x' ved successivt at anvende tilladte permutationer.

I denne situation har vi følgende

PERMUTATIONSPROBLEMER. (I) Bestem for hvert tilladt mønster x mængden $\tilde{R}(x) \subseteq Aut(P)$.

(II) Bestem relationen $\to$ i mængden M.

BEMÆRKNING. Det skal understreges, at de to problemer er praktiske problemer, idet mængden $\tilde{R}(x)$ og relationen $\to$ naturligvis er "bestemt" ved deres definitioner. At "løse" problemerne betyder altså for en given situation at finde praktisk anvendelige (f.eks. numeriske) kriterier til at afgøre, om der for et givet $\sigma \in Aut(P)$ (resp. for givne $x, x' \in M$) gælder $\sigma \in \tilde{R}(x)$ eller $\sigma \notin R(x)$ (resp. $x \to x'$ eller $x \not\to x'$).
Naturligvis kan der i praksis være tilsvarende problemer med at afgrænse de tilladte mønstre og de tilladte permutationer.

6.8. I den i 6.7 beskrevne situation kan vi også direkte betragte den ved

$$x \mapsto x' \overset{\text{DEF}}{\iff} \exists\, \sigma \in R(x) : \sigma.x = x'$$

bestemte relation $\mapsto$. Forudsætninger om den givne situation vil således spejle sig i egenskaber ved denne relation. Bemærk imidlertid, at relationen $\to$ i M altid er transitiv.

Hvis "tilladeligheden" af en permutation ikke afhænger af hvilket af de tilladte mønstre, den skal anvendes på, består de tilladte permutationer blot af en delmængde

$$R \subseteq Aut(P),$$

og delmængden

$$\tilde{R} := \{ \sigma_m \cdots \sigma_1 \mid m \in \mathbb{N},\ \sigma_1, \ldots, \sigma_m \in R \} \subseteq Aut(P)$$

er øjensynlig en stabil delmængde. Hvis P er en endelig mængde, således at gruppen $Aut(P)$ er endelig, og $R \neq \emptyset$, følger det let, at $\tilde{R} \subseteq Aut(P)$ er en undergruppe. Af 6.7 (*) følger nu, at gruppen $\tilde{R}$ virker på mængden M af tilladte mønstre, og relationen $\to$ i M er netop den tilhørende ækvivalensrelation. Den er altså i dette tilfælde også refleksiv og symmetrisk.

6.9. De angivne Permutationsproblemer 6.7 søges ofte løst ved at finde såkaldte <u>invarianter</u> for den givne situation.

Hermed menes – uden at vi nærmere vil præcisere dette – afbildninger fra den givne situation over i en simplere situation, som respekterer (dele af) den givne struktur.

Vi kan f.eks. søge afbildninger $f: M \to Y$, hvor Y er en mængde med en relation S, således at

$$\sigma \in R(x) \Rightarrow f(x)\ S\ f(\sigma x).$$

Hvis relationen S i Y er transitiv, følger heraf, at

$$x \longrightarrow x' \Rightarrow f(x)\ S\ f(x').$$

At $f(x)\ S\ f(x')$ er således en nødvendig betingelse for at $x \longrightarrow x'$.

Det forekommer ofte, at de tilladelige permutationer er elementer i en gruppe G, der virker på M. I denne situation kan der med fordel søges invarianter i form af en mængde Y hvorpå G virker, og en afbildning $f: M \to Y$, som opfylder:

$$\sigma \in R(x) \Rightarrow \sigma.f(x) = f(\sigma.x).$$

Heraf følger, at

$$\tau \in \tilde{R}(x) \Rightarrow \tau.f(x) = f(\tau.x).$$

At $\tau.f(x) = f(\tau.x)$ er således en nødvendig betingelse for at $\tau \in \tilde{R}(x)$.

Er der fundet en eller flere invarianter, er det ofte nyttigt at undersøge, om de også giver tilstrækkelige betingelser.

6.10 EKSEMPEL. SOLITAIRE-SPILLET. I dette velkendte éu-mands-spil er en gruppe pinde placeret i en række huller på et bræt. Et tilladt træk består i at springe med en pind over en nabopind ned i et tilstødende tomt hul, og fjerne den pind man sprang over. Kan man ende med kun at have 1 pind tilbage på brættet?

SVAR. I modellen (jfr Bemærkning 6.3) består P af brættets huller (vi kan tænke på dem som en endelig delmængde $B \subseteq \mathbb{Z} \times \mathbb{Z}$) samt af en række afsætningspladser, F består af farverne: "pind" og "ikke-pind", og alle "mønstre" $x: P \to F$ er tilladte. De tilladte permutationer svarer til de tilladte træk, og afhænger således af det givne mønster.

En oplagt invariant fås ved til hvert mønster x at knytte antallet ($=: a(x)$) af prikker i B fra mønstret x. Hvis $\sigma \in R(x)$, har vi øjensynlig $a(\sigma.x) = a(x) - 1$, og følgelig

$$x \longrightarrow x' \quad \Rightarrow \quad a(x) > a(x')$$

[men det kan vist ikke imponere nogen].

En mere spændende invariant fås på følgende måde: I $Y = \mathbb{Z}^4$ betragtes undergruppen bestående af $(y_0, y_1, y_2, y) \in \mathbb{Z}^4$ med $y - y_0 \in 2\mathbb{Z}$, $y - y_1 \in 2\mathbb{Z}$, $y - y_2 \in 2\mathbb{Z}$, og med $\equiv$ betegnes den tilsvarende kongruensrelation. Del nu mængden $B \subseteq \mathbb{Z} \times \mathbb{Z}$ i de tre delmængder B_0, B_1, B_2, hvor $B_\nu = \{(i,j) \in B \mid i+j \equiv \nu \pmod 3\}$, og knyt til mønstret x

$$f(x) = \big(a_0(x), a_1(x), a_2(x), a(x)\big) \in Y,$$

hvor $a_\nu(x) :=$ antal prikker i B_ν fra mønstret x. Ved en tilladt permutation $\sigma \in R(x)$ ændres hvert af de 4 tal a_0, a_1, a_2, a med ± 1 (!), og vi har derfor $f(x) \equiv f(\sigma.x)$. Det følger, at

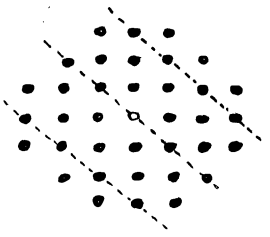
$$x \longrightarrow x' \quad \Rightarrow \quad f(x) \equiv f(x').$$

For et mønster x', med 1 prik, f.eks. i B_0, har vi $f(x') = (1,0,0,1)$. Af $x \longrightarrow x'$ følger derfor

$f(x) =$ (ulige, lige, lige, ulige) eller $f(x) =$ (lige, ulige, ulige, lige).

SPECIELT: Følgende bræt

B



har 37 huller. På figuren har vi antydet B_0. For mønsteret z med en prik i alle huller finder vi $f(z) = (13, 12, 12, 37)$, men her er naturligvis $R(z) = \emptyset$. For en stilling x med prikker i alle huller på nær i det midterste har vi $f(x) = (12, 12, 12, 36)$. Følgelig er det fra dette mønster umuligt at komme til et mønster, der kun har 1 prik.

6.11. EKSEMPEL. 15-SPILLET. I dette velkendte én-mands-spil er 15 kvadratiske brikker placeret på et kvadratisk bræt med $4 \times 4 = 16$ felter, således at ét felt er tomt. Et tilladt

trick består i at skubbe en brik hen på et nabofelt, hvis dette er tomt. Hvilke placeringer kan man komme til?
SVAR. I modellen består P af brættets 16 felter [Vi kan tænke på P som delmængden $P=\{(i,j)\in\mathbb{N}\times\mathbb{N} \mid 1\leqslant i\leqslant 4,\ 1\leqslant j\leqslant 4\}$], F består af de 15 brikker samt en tom brik 0, og de tilladte mønstre er de bijektive afbildninger $x: P\to F$. De tilladte permutationer svarer til de tilladte træk, og afhænger således af mønsteret. Mere præcist: Betegner vi for et tilladt mønster x med $p=x^{-1}(0)$ det felt, hvorpå den tomme brik findes, så består $R(x)$ af de transpositioner, der ombytter p med et af dets nabofelter.

Bemærk, at hele gruppen $G=\mathrm{Aut}(P)=S_{16}$ virker på de tilladte mønstre. Der er kun 1 bane, og for givne mønstre $x,x'\in M$ er der netop en permutation $\sigma\in\mathrm{Aut}(P)$, med $\sigma.x=x'$. Vi betegner den $\sigma=\frac{x'}{x}$.

For at bestemme en invariant betragter vi $Y=\{\pm 1\}$, og vi lader $G=\mathrm{Aut}(P)$ virke på Y via fortegnet, dvs ved

$$\sigma.\varepsilon = \mathrm{sign}(\sigma)\,\varepsilon \in \{\pm 1\},\quad \sigma\in\mathrm{Aut}(P),\ \varepsilon=\pm 1,$$

og vi definerer $f: M\to Y$ ved

$$f(x)=\begin{cases} 1 & \text{hvis } x^{-1}(0) \text{ har koordinater } (i,j) \text{ med } i+j\in 2\mathbb{Z} \\ -1 & \text{hvis } x^{-1}(0) \text{ har koordinater } (i,j) \text{ med } i+j\in 1+2\mathbb{Z}\end{cases}$$

Nu gælder for en tilladt permutation $\sigma\in R(x)$, at

$$f(\sigma.x)=\sigma.f(x)=\mathrm{sign}(\sigma)\cdot f(x),$$

thi da hver tilladt permutation er en transposition, udtrykker dette blot at $f(\sigma.x)$ og $f(x)$ har modsat fortegn, og det er jo klart! Vi har følgelig en nødvendig betingelse:

$$\tau\in\tilde{R}(x) \Longrightarrow f(\tau.x)=\mathrm{sign}(\tau)\,f(x),$$

som også kan udtrykkes

$$x\longrightarrow x' \Longrightarrow \frac{f(x')}{f(x)}=\mathrm{sign}\left(\frac{x'}{x}\right).$$

SPECIELT ses for to mønstre $x,x'\in M$, der har den tomme brik placeret på <u>samme</u> felt (f.eks. på (4,1)), at

$$x \longrightarrow x' \quad \Longrightarrow \quad \operatorname{sign}\left(\frac{x'}{x}\right) = 1.$$

De to mønstre vil altså "afvige" med en lige permutation.
BEMÆRKNING. Det er ikke svært at vise, at den anførte invariant giver en tilstrækkelig betingelse. [Prøv! - det er smart, at udnytte Sætning 2.9 (2).]

6.12 EKSEMPEL. RUBIK'S TERNING. På denne velkendte terning er hver af de 6 sider delt i $3 \times 3 = 9$ (farvede) felter. Hvilke mønstre kan vi få frem ved de velkendte drejninger af terningens sideflader? Vi ser her bort fra hvad der sker med de 6 midterfelter.
SVAR. I modellen består P altså af $8 \times 3 = 24$ hjørnefelter og $12 \times 2 = 24$ kantfelter, altså $|P| = 48$. Sædvanligvis bruges 6 farver, så der er 6^{48} mulige elementer i $X = \mathrm{Afb}(P, F)$. De tilladte permutationer svarer til $\frac{1}{4}$-drejningerne af sidefladerne. De udgør en delmængde $R \subseteq \mathrm{Aut}(P)$ [hvis element er produkter af 5 disjunkte 4-cykler, nemlig 3 cykler i hjørnefelterne og 2 cykler i kantfelterne], og det første problem er at afgrænse undergruppen $\tilde{R} \subseteq \mathrm{Aut}(P)$.

Fysisk kan vi betragte de permutationer af P, der består i at skille terningen ad og samle den igen. De udgør en undergruppe $G \subseteq \mathrm{Aut}(P)$, som matematisk kan beskrives på følgende måde: Mængden P har, svarende til den fysiske situation, en "struktur" der består i at den er inddelt i kantfelter og hjørnefelter, kantfelterne er delt i 12 delmængder med 2 elementer i hver, kaldet <u>kanter</u>, og hjørnefelterne er delt i 8 delmængder med 3 elementer i hver, kaldet <u>hjørner</u>. Endvidere har for hvert hjørne H de 3 elementer i H en naturlig rækkefølge: Der er 6 mulige nummereringer $\varphi: \{1,2,3\} \xrightarrow{\sim} H$. Af dem er de 3 <u>positive</u>, dvs opfylder, at $\varphi_1, \varphi_2, \varphi_3$ "svarer til den positive omløbsretning, når man kigger på terningen". Gruppen G består nu af de

permutationer $\sigma \in Aut(P)$, som bevarer denne struktur, dvs som opfylder: Hvis $K \subseteq P$ er en kant, så er $\sigma(K)$ en kant. Hvis $H \subseteq P$ er et hjørne, så er $\sigma(H)$ et hjørne, og hvis $H = \{h_1, h_2, h_3\}$ er en positiv numerering af H, så er $\sigma(H) = \{\sigma(h_1), \sigma(h_2), \sigma(h_3)\}$ en positiv nummerering af $\sigma(H)$.

Det er klart, at gruppen G har ordn

$$|G| = 12! \cdot 2^{12} \cdot 8! \cdot 3^8,$$

og at $\tilde{R}$ er en undergruppe i G.

Gruppen G permuterer kanterne og hjørnerne, og virker altså på mængden $\mathcal{K}$ bestående af de 12 kanter, og på mængden $\mathcal{H}$ bestående af de 8 hjørne, og dermed også på foreningsmængden $\mathcal{K} \cup \mathcal{H}$. Vi har således repræsentationer

$$G \to Aut(\mathcal{K}) = S_{12}\ ,\quad G \to Aut(\mathcal{H}) = S_8\ ,\quad G \to Aut(\mathcal{K} \cup \mathcal{H}) = S_{20}$$

De 2 første homomorfier er surjektive, og billedet ved den sidste er med en oplagt betegnelse undergruppen $S_8 \times S_{12} \subseteq S_{20}$. Kernen for den sidste homomorfi er den normale undergruppe $G_0 \subseteq G$ bestående af permutationer, som fixer kanter og hjørner (men som eventuelt permuterer felter hørende til samme kant eller hjørne). Fortegnet for permutationen $\sigma_{\mathcal{K} \cup \mathcal{H}}$ definerer en homomorfi, som vi (også) betegner

$$\text{Sign} : G \longrightarrow \{\pm 1\}. \approx \mathbb{Z}/2\mathbb{Z}$$

Vi har øjensynlig $\text{sign}(\sigma) = \text{sign}(\sigma_{\mathcal{K}})\,\text{sign}(\sigma_{\mathcal{H}})$. Endvidere er denne homomorfi en invariant, i den forstand, at

$$(*) \qquad \sigma \in \tilde{R} \implies \text{Sign}(\sigma) = 0 \in \mathbb{Z}/2\mathbb{Z}.$$

Det er nemlig nok at betragte en tilladt $\frac{1}{4}$-drejning $\sigma \in R$, og her er $\sigma_{\mathcal{K} \cup \mathcal{H}} = \sigma_{\mathcal{K}} \circ \sigma_{\mathcal{H}}$ et produkt af 2 4-cykler, og har altså fortegnet (additivt skrevet) $3 \cdot 1 + 3 \cdot 1 = 6 \equiv 0$.

Gruppen G virker også på delmængden $L \subseteq P$ bestående af de 24 kantfelter. Vi får således en repræsentation: $G \to Aut(L) = S_{24}$, og ved sammensætning med fortegnet $\text{sign}: S_{24} \longrightarrow \{\pm 1\} \approx \mathbb{Z}/2\mathbb{Z}$ fås en homomorfi, som vi betegner

$$\text{Flip} : G \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

idet den i en vis forstand måler, hvor mange kanter, der "flippes".

Også Flip er en invariant:

$$(**)\quad \sigma \in \tilde{R} \Rightarrow \mathrm{Flip}(\sigma) = 0 \in \mathbb{Z}/2\mathbb{Z}$$

idet en tilladt $\frac{1}{4}$-drejning på kantfeltene er et produkt af 2 4-cykler.

Endelig defineres for $\sigma \in G$ "rotationen" $\mathrm{Rot}(\sigma) \in \mathbb{Z}/3\mathbb{Z}$ på følgende måde: Hvis $\varphi, \psi : \{1,2,3\} \xrightarrow{\sim} H$ er positive nummereringer af det samme hjørne H, så er $\psi^{-1} \circ \varphi$ en lige permutation i $\{1,2,3\}$, altså element i gruppen A_3. Vælg nu for hvert hjørne H en positiv nummerering $\varphi_H : \{1,2,3\} \xrightarrow{\sim} H$, og sæt

$$\mathrm{Rot}_{H,\varphi}(\sigma) = \varphi_{\sigma H}^{-1} \circ \sigma \circ \varphi_H \in A_3$$

Er også $\tau \in G$ finder vi let $\mathrm{Rot}_{H,\varphi}(\sigma\tau) = \mathrm{Rot}_{\tau(H)}(\sigma) \circ \mathrm{Rot}_H(\tau)$.

Idet vi identificerer $A_3 = \mathbb{Z}/3\mathbb{Z}$, og opfatter $\mathrm{Rot}_{H,\varphi}(\sigma) \in \mathbb{Z}/3\mathbb{Z}$, sættes

$$\mathrm{Rot}(\sigma) = \sum_H \mathrm{Rot}_{H,\varphi}(\sigma) \in \mathbb{Z}/3\mathbb{Z}.$$

Det er let at se, at dette faktisk er uafhængigt af de valgte nummereringer, og at der herved defineres en homomorfi

$$\mathrm{Rot} : G \to \mathbb{Z}/3\mathbb{Z}.$$

Dette er den tredie invariant:

$$(***)\quad \sigma \in \tilde{R} \Rightarrow \mathrm{Rot}(\sigma) = 0 \in \mathbb{Z}/3\mathbb{Z}.$$

SPECIELT: Følgende kan ikke udføres på terningen ($\sigma \notin \tilde{R}$): Ombytning af 2 kanter, ombytning af 2 hjørner, flip af en kant, rotation af et hjørne – uden at røre resten.

BEMÆRKNING. De anførte invarianter er faktisk tilstrækkelige: Antag altså, at $\sigma \in G$ har $\mathrm{sign}(\sigma) = 0$, $\mathrm{Flip}(\sigma) = 0$, $\mathrm{Rot}(\sigma) = 0$. Sammensættes σ eventuelt med en $\frac{1}{4}$-drejning, kan vi antage, at både σ_K og $\sigma_{\mathcal{H}}$ er lige permutationer. I $\tilde{R}$ findes (!) elementer, der 3-cykler kanterne, og elementer, der 3-cykler hjørnerne. Sammensættes eventuelt σ med et passende antal sådanne, kan vi antage, at $\sigma \in G_0$. I $\tilde{R}$ findes elementer, der er et "dobbeltflip" af 2 kanter, og elementer, der er en dobbeltrotation af 2 hjørner. Sammensættes σ eventuelt med et passende antal sådanne, kan vi antage, at σ kun flipper 1 kant og roterer 1 hjørne. Af $\mathrm{Flip}(\sigma) = 0$ og $\mathrm{Rot}(\sigma) = 0$ følger så, at $\sigma = 1$. Og så er jo $\sigma \in \tilde{R}$.

Specielt: $|\tilde{R}| = |G| / |\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}| = 2^{10} \cdot 3^7 \cdot 8! \cdot 12!$

RINGE

1. Ringbegrebet. 1.1: Ring. 1.2: Kommutativ ring. 1.3: Ringhomomorfi. 1.4: Delring. 1.5: Ideal. Idealer i $\mathbb{Z}$. 1.6: Ideal og kvotientring. 1.7: Karakteristik og primring. 1.8: Regulært og invertibelt element. 1.9: Integritetsområde og (skæv-)legeme. 1.10: Legemerne $\mathbb{F}_p$. 1.11: Primlegeme. 1.12: Kommutation. Centrum. 1.13: Involutorisk. Idempotent. Nilpotent.

2. Polynomiumsringen $R[x]$ i én variabel over en kommutativ ring R. 2.1: Beskrivelse. 2.2: Konstant. Normeret polynomium. Grad. 2.3: Grad af sum og produkt. 2.4: Nulreglen. 2.5: Divisionssætning. 2.6: Indsættelse. Rod. 2.7: Sætning om rødder. 2.8: Afledet polynomium. 2.9: Strukturssætning for polynomiumskvotient. 2.10: Hovedidealsætning.

3. Nogle ringkonstruktioner. 3.1: Produktring. 3.2: Funktionsring. 3.3: Matrixring. 3.4: Endomorfiring. 3.5: Polynomiumsringen $\Lambda[x]$. 3.6: Potensrækkeringen $\Lambda[[x]]$. 3.7: Polynomiumsringen $\Lambda[x_1, \ldots, x_n]$. 3.8: Foldningsringen $\Lambda[M]$. 3.9: Foldningsrækkeringen $\Lambda[[M]]$

4. Algebraer. 4.1: R-algebra. 4.2: Lie-algebra. Jordan-algebra. Alternativ algebra. Associativ algebra. 4.3: Strukturhomomorfi. 4.4: Eksempler. 4.5: Homomorfi. 4.6: Del-algebra. Ideal. Kvotientalgebra. 4.7: Delalgebraen $R[\alpha]$. 4.8: Indsættelse. Rod. 4.9: Algebraisk og transcendent. 4.10: Minimalt polynomium. Grad af et element. 4.11: Sætning.

RINGE

1. Ringbegrebet.

1.1. DEFINITION. En ring $(\Lambda;+,\cdot)$ er en mængde Λ forsynet med to kompositioner, en addition $+ : \Lambda\times\Lambda \to \Lambda$ betegnet $(\lambda,\mu) \mapsto \lambda+\mu$ og en multiplikation $\cdot : \Lambda\times\Lambda \to \Lambda$ betegnet $(\lambda,\mu) \mapsto \lambda\mu$ således at følgende er opfyldt:

(a) Med hensyn til addition er Λ en kommutativ gruppe.

(m) Med hensyn til multiplikation er Λ et monoid.

(d) Multiplikation er distributiv m.h.t. addition.

Den kommutative gruppe $(\Lambda,+)$ kaldes ringens additive gruppe, og betegnes ofte Λ^+. Dens neutrale element kaldes ringens nul-element og betegnes 0_Λ (eller blot: 0)

Det inverse m.h.t. addition af et element $\lambda\in\Lambda$ kaldes ofte det modsatte til λ og betegnes $-\lambda$.

Monoidet $(\Lambda,\cdot)$ kaldes ringens multiplikative monoid, og betegnes ofte $\Lambda^\times$. Dets neutrale element kaldes ringens et-element og betegnes 1_Λ (eller blot: 1).

Betingelserne kan udtrykkes ved ligningerne:

$$\text{(a)}\quad \begin{cases} \lambda+\mu = \mu+\lambda \\ (\lambda+\mu)+\nu = \lambda+(\mu+\nu) \\ \lambda+0 = \lambda \\ \lambda+(-\lambda) = 0 \end{cases}$$

$$\text{(m)}\quad \begin{cases} (\lambda\mu)\nu = \lambda(\mu\nu) \\ 1\lambda = \lambda = \lambda 1 \end{cases}$$

$$\text{(d)}\quad \lambda(\mu+\nu) = \lambda\mu+\lambda\nu,\quad (\lambda+\mu)\nu = \lambda\nu+\mu\nu$$

OBSERVATION. For alle $\lambda\in\Lambda$ gælder

$$0\lambda = 0 = \lambda 0 \quad\text{og}\quad (-1)\lambda = -\lambda = \lambda(-1),$$

thi den første ligning følger for eksempel af at

$$0\lambda + 0\lambda = (0+0)\lambda = 0\lambda$$

og den sidste af at

$$\lambda + \lambda(-1) = \lambda 1 + \lambda(-1) = \lambda[1+(-1)] = \lambda 0 = 0.$$

BEMÆRKNING. Det forudsættes ikke, at $0_\Lambda \neq 1_\Lambda$. Er imidlertid $0_\Lambda = 1_\Lambda$, finder vi $\lambda = 1\lambda = 0\lambda = 0$ for alle $\lambda \in \Lambda$, så Λ indeholder i så fald kun ét element. Denne ring kaldes nulringen og betegnes (også) 0. I alle andre ringe er altså $0 \neq 1$.

1.2. DEFINITION. Ringen Λ kaldes kommutativ, hvis den for alle $\lambda, \mu \in \Lambda$ gælder

$$\lambda\mu = \mu\lambda.$$

EKSEMPEL. De hele tal udgør en kommutativ ring $(\mathbb{Z}, +, \cdot)$.

BEMÆRKNING. I enhver ring Λ kan en modsat multiplikation defineres ved

$$\lambda \overset{\text{op}}{\cdot} \mu := \mu\lambda.$$

Det er let at se, at $(\Lambda, +, \overset{\text{op}}{\cdot})$ er en ring; den kaldes Λ's modsatte ring og betegnes Λ^{op}. Hvis Λ er kommutativ, er $\Lambda = \Lambda^{\text{op}}$.

1.3. DEFINITION. En afbildning $\varphi : \Gamma \to \Lambda$ mellem ringe Γ og Λ kaldes en (ring-) homomorfi, hvis den respekterer strukturen i den forstand, at

$$\begin{aligned} \varphi(\gamma+\mu) &= \varphi(\gamma) + \varphi(\mu) \\ \varphi(\gamma\mu) &= \varphi(\gamma)\varphi(\mu) \qquad \gamma, \mu \in \Gamma. \\ \varphi(1_\Gamma) &= 1_\Lambda. \end{aligned}$$

Ved kernen for homomorfien $\varphi: \Gamma \to \Lambda$ forstås originalmængden $\varphi^{-1}(0_\Lambda)$. Det er let at se, at φ er injektiv, netop når kernen er $\varphi^{-1}(0_\Lambda) = \{0_\Gamma\}$.

Det er klart, at sammensætning af homomorfier $\varphi: \Gamma \to \Lambda$ og $\psi: \Delta \to \Gamma$ er en homomorfi $\varphi\circ\psi: \Delta \to \Lambda$. Endvidere er den identiske afbildning $Id_\Lambda: \lambda \mapsto \lambda$ en homomorfi $Id_\Lambda: \Lambda \to \Lambda$.

En bijektiv homomorfi $\varphi: \Gamma \to \Lambda$ kaldes også en (ring-) isomorfi. For en sådan er også den inverse afbildning en isomorfi $\varphi^{-1}: \Lambda \to \Gamma$.

En homomorfi $\varphi: \Lambda \to \Lambda$ af ringen Λ ind i sig selv kaldes også en endomorfi, og hvis den er bijektiv også en automorfi.

BEMÆRKNING. En ringhomomorfi $\varphi: \Gamma \to \Lambda^{op}$ kaldes også en anti-homomorfi $\varphi: \Gamma \to \Lambda$.

1.4. DEFINITION. Ved en delring af en ring Λ forstås en delmængde $\Gamma \subseteq \Lambda$, som er stabil under addition og multiplikation, og som med sine inducerede kompositioner selv er en ring med samme et-element som Λ. Den sidste betingelse sikrer, at inklusionsafbildningen: $\gamma \mapsto \gamma$ er en ringhomomorfi: $\Gamma \hookrightarrow \Lambda$.

OBSERVATION. En stabil delmængde $\Gamma \subseteq \Lambda$ er en delring, når blot $-1_\Lambda \in \Gamma$,

thi i så fald finder vi først $1 = -(-1) = (-1)(-1) \in \Gamma$, dernæst $0 = 1 + (-1) \in \Gamma$ og endelig $-\gamma = (-1)\gamma \in \Gamma$, når $\gamma \in \Gamma$.

1.5. DEFINITION. Ved et ideal i en ring Λ forstås en delmængde $\mathfrak{a} \subseteq \Lambda$, som opfylder:

(a) $\mathfrak{a}$ er en undergruppe i den additive gruppe $(\Lambda,+)$.
(m) $\mathfrak{a}$ er stabil over for multiplikation med et vilkårligt element fra Λ, d.v.s. opfylder

$$\alpha \in \mathfrak{a} \wedge \lambda \in \Lambda \Rightarrow \alpha\lambda \in \mathfrak{a} \wedge \lambda\alpha \in \mathfrak{a}.$$

De trivielle idealer i Λ er delmængderne $\{0\}$ (også betegnet (0)) og hele Λ.

HOVEDIDEALSÆTNING. Idealerne i ringen $\mathbb{Z}$ er netop delmængderne af formen

$$\mathfrak{a} = \mathbb{Z}n = \{ pn \mid p \in \mathbb{Z} \}, \quad n \geqslant 0.$$

Tallet n er entydigt bestemt ved idealet $\mathfrak{a}$, nemlig som $n = 0$, hvis $\mathfrak{a} = (0)$, og n = mindste positive tal i $\mathfrak{a}$, hvis $\mathfrak{a} \neq (0)$.
BEVIS. De anførte delmængder er som bekendt samtlige undergrupper i $(\mathbb{Z},+)$, og da de ógensynlig er idealer, følger påstanden ▨

1.6. Som bekendt er der en entydig forbindelse mellem idealer $\mathfrak{a}$ i ringen Λ og kongruensrelationer i Λ. Den til idealet $\mathfrak{a}$ hørende kongruensrelation er $\underset{\mathfrak{a}}{\equiv}$ ("kongruens modulo $\mathfrak{a}$") defineret ved

$$\lambda' \underset{\mathfrak{a}}{\equiv} \lambda \overset{\text{DEF}}{\Leftrightarrow} \lambda' - \lambda \in \mathfrak{a}.$$

Ækvivalensklassen, der indeholder λ er altså delmængden

$$\lambda + \mathfrak{a} = \{ \lambda + \alpha \mid \alpha \in \mathfrak{a} \}.$$

Den tilhørende kvotientring betegnes $\Lambda/\mathfrak{a}$, og $\lambda \mapsto \overline{\lambda}$ betegner den kanoniske homomorfi $\Lambda \to \Lambda/\mathfrak{a}$.
Med hensyn til denne gælder som bekendt
UDVIDELSESSÆTNINGEN. En ringhomomorfi $\varphi: \Lambda \to \Gamma$, som forsvinder på idealet $\mathfrak{a} \subseteq \Lambda$,

kan entydigt udvides til en ringhomomorfi fra kvotienten $\bar{\varphi}: \Lambda/\alpha \to \Gamma$.

$$\begin{array}{ccc} \Lambda & \xrightarrow{\pi} & \Lambda/\alpha \\ {\scriptstyle\varphi}\downarrow & \swarrow_{\bar{\varphi}} & \\ \Gamma & & \end{array}$$ ▨

Homomorfien $\bar{\varphi}$ er den <u>inducerede</u> homomorfi.

Viden gælder som bekendt

ISOMORFISÆTNINGEN. Lad $\varphi: \Lambda \to \Gamma$ være en ringhomomorfi. Da er kernen $\varphi^{-1}(0)$ et ideal i Λ, billedmængden $\varphi(\Lambda)$ er en delring af Γ, og φ inducerer en isomorfi $\bar{\varphi}: \Lambda/\varphi^{-1}(0) \xrightarrow{\approx} \varphi(\Lambda)$ af kvotienten på billedet.

$$\begin{array}{ccc} \Lambda & \xrightarrow{\varphi} & \Gamma \\ \downarrow & & \uparrow \\ \Lambda/\varphi^{-1}(0) & \xrightarrow[\bar{\varphi}]{\approx} & \varphi(\Lambda). \end{array}$$

EKSEMPEL. Kvotientringen $\mathbb{Z}/\mathbb{Z}n$ hørende til idealet $\mathbb{Z}n$, $n \geq 1$, er restklasseringen modulo n. Den betegnes også $\mathbb{Z}/n$.

1.7. KARAKTERISTIK OG PRIMRING. Som bekendt findes for enhver ring Λ en og kun én ringhomomorfi: $\mathbb{Z} \to \Lambda$, nemlig den <u>kanoniske ringhomomorfi</u>:

$$q \longmapsto q1_\Lambda, \qquad q \in \mathbb{Z}.$$

Kernen for den kanoniske ringhomomorfi $\mathbb{Z} \to \Lambda$ er et ideal i $\mathbb{Z}$, og altså af formen $\mathbb{Z}n$, hvor $n \geq 0$ er entydigt bestemt (**Hovedidealsætning 1.5**).

DEFINITION. Tallet $n \geq 0$ kaldes <u>karakteristikken</u> af ringen Λ, og billedet ved den kanoniske ringhomomorfi $\mathbb{Z} \to \Lambda$ kaldes <u>primringen</u> i Λ.

Karakteristikken af Λ kan betegnes $\mathrm{char}(\Lambda)$.

Primringen i Λ er delmængden

$$\{ q1_\Lambda \mid q \in \mathbb{Z} \}.$$

Det er øjensynlig den mindste delring af Λ.

Af beskrivelsen i Sætning 1.5 fremgår følgende:

RESULTAT. Ringen Λ har karakteristik 0, netop når

$$\overbrace{1_\Lambda + \cdots + 1_\Lambda}^{m} \neq 0_\Lambda$$

for alle $m \in \mathbb{N}$. I dette tilfælde er den kanoniske ringhomomorfi : $\mathbb{Z} \to \Lambda$ injektiv, og primringen i Λ er (isomorf med) $\mathbb{Z}$.

Ringen Λ har karakteristik $n \geqslant 1$, netop når n er det mindste naturlige tal således at

$$\overbrace{1_\Lambda + \cdots + 1_\Lambda}^{n} = 0_\Lambda.$$

I dette tilfælde får vi af Isomorfisætningen en isomorfi af restklasseringen $\mathbb{Z}/n$ på primringen i Λ. Bemærk, at der her gælder $\overbrace{\lambda + \cdots + \lambda}^{n} = 0_\Lambda$ for alle $\lambda \in \Lambda$, idet jo $\overbrace{\lambda + \cdots + \lambda}^{n} = \overbrace{1 + \cdots + 1}^{n} \cdot \lambda = 0 \cdot \lambda = 0$.

EKSEMPLER. Ringen $\mathbb{Z}$ har karakteristik 0. Restklasseringen $\mathbb{Z}/n$, $n \geqslant 1$, har karakteristik n (hvorfor?). En endelig ring har karakteristik >0 (hvorfor?).

1.8. REGULÆRT OG INVERTIBELT ELEMENT.

DEFINITION. Lad Λ være en ring. Et element $\lambda \in \Lambda$ kaldes <u>regulært</u>, hvis der for alle $\xi \in \Lambda$ gælder

$$\lambda\xi = 0 \Rightarrow \xi = 0 \quad \text{og} \quad \xi\lambda = 0 \Rightarrow \xi = 0.$$

Mængden af regulære elementer i Λ kan betegnes Λ^{reg}.

Et element $\lambda \in \Lambda$ kaldes <u>invertibelt</u> (eller en <u>enhed</u>), hvis der findes et element $\lambda' \in \Lambda$, således at

$$\lambda\lambda' = 1 = \lambda'\lambda.$$

I bekræftende fald er elementet λ' entydigt bestemt. Det kaldes det <u>inverse</u> til λ og betegnes λ^{-1}. Mængden af invertible elementer i Λ betegnes Λ^*.

OBSERVATIONER. (1) Ethvert invertibelt element $\lambda \in \Lambda$ er regulært,
thi af $\lambda \xi = 0$ følger $0 = \lambda^{-1} 0 = \lambda^{-1} \lambda \xi = 1 \xi = \xi$, og analogt hvis $\xi \lambda = 0$.
(2) Delmængden Λ^{reg} er stabil under multiplikation og indeholder et-elementet 1. Vi kan altså opfatte Λ^{reg} som et monoid.
(3) Delmængden Λ^* er stabil under multiplikation, indeholder et-elementet og med et element λ tillige det inverse λ^{-1}! Vi kan altså opfatte Λ^* som en gruppe (med multiplikation som komposition og et-elementet som neutralt element).

EKSEMPEL. For ringen $\mathbb{Z}$ har vi

$$\mathbb{Z}^{reg} = \mathbb{Z} \setminus \{0\}, \qquad \mathbb{Z}^* = \{\pm 1\}.$$

1.9. INTEGRITETSOMRÅDE OG (SKÆV-)LEGEME.

DEFINITION. I ringen Λ siges <u>nul-reglen</u> at gælde, hvis vi for alle elementer $\lambda, \mu \in \Lambda$ har

$$\lambda \mu = 0 \quad \Rightarrow \quad \lambda = 0 \ \vee \ \mu = 0.$$

Ringen Λ kaldes et <u>integritetsområde</u> (eller blot et <u>område</u>), hvis

$$\Lambda^{reg} = \Lambda \setminus \{0\},$$

og et <u>skævlegeme</u>, hvis

$$\Lambda^* = \Lambda \setminus \{0\}.$$

Et <u>legeme</u> er et kommutativt skævlegeme. Ved et <u>dellegeme</u> af et legeme forstås en delring, som selv er et legeme.

BEMÆRKNINGER. Nul-reglen udsiger, at alle elementer $\neq 0$ er regulære, altså at

$$\Lambda \setminus \{0\} \subseteq \Lambda^{reg}$$

Dette gælder formelt for nul-ringen.

I nul-ringen er nul-elementet regulært, så nul-ringen er <u>ikke</u> et integritetsområde. Det følger, at en ring $\Lambda \neq 0$ er et integritetsområde, netop når nul-reglen gælder.
Tilsvarende ses, at nul-ringen <u>ikke</u> er et skælegeme, og at en ring $\Lambda \neq 0$ er et skælegeme, netop når ethvert element $\neq 0$ i Λ er invertibelt.

EKSEMPEL. De hele tals ring $\mathbb{Z}$ er et kommutativt integritetsområde, men ikke et legeme. De rationale tal udgør legemet $\mathbb{Q}$.

SÆTNING. For et integritetsområde (og specielt for et legeme) Λ er karakteristikken n enten 0 eller et primtal.
BEVIS. (Indirekte). Vi har $n \neq 1$ (idet kun nul-ringen har karakteristik 1), og hvis n var et sammensat tal, $n = ad$, $1 < a < n$, $1 < d < n$, ville

$$a1_\Lambda \neq 0_\Lambda \quad , \quad d1_\Lambda \neq 0_\Lambda \quad , \quad (a1_\Lambda)(d1_\Lambda) = n1_\Lambda = 0_\Lambda$$

(jfr. 1.7) være i modstrid med nulreglen ▨

1.10. LEGEMERNE $\mathbb{F}_p$. SÆTNING. Enhver endelig ring Λ, hvis elementantal p er et primtal, er et legeme, isomorft med restklasseringen $\mathbb{Z}/p$.
BEVIS. Da $|\Lambda| = p > 1$, er Λ ikke nul-ringen. For at vise, at hvert element $\lambda \neq 0$ i Λ er invertibelt, betragtes i den additive gruppe $(\Lambda, +)$ undergruppen

$$\mathbb{Z}\lambda = \{ q\lambda \mid q \in \mathbb{Z} \}$$

bestående af (additive) potenser af λ. Denne undergruppes orden er > 1 (idet den indeholder både 0 og λ). I følge Lagrange's sætning er ordenen $|\mathbb{Z}\lambda|$ divisor i $|\Lambda| = p$, som er et primtal, og vi har følgelig $|\mathbb{Z}\lambda| = |\Lambda|$ og dermed $\mathbb{Z}\lambda = \Lambda$.

Specielt findes et helt tal $q \in \mathbb{Z}$, således at $q\lambda = 1_\Lambda$. Af

$$(q1_\Lambda)\lambda = \lambda(q1_\Lambda) = q\lambda = 1$$

fremgår, at λ er invertibel (med den inverse $\lambda^{-1} = q1_\Lambda$). Følgelig er Λ et skævlegeme.

Anvendes ovenstående på elementet $\lambda = 1_\Lambda \in \Lambda$, ses at

$$\mathbb{Z}1_\Lambda = \{q1_\Lambda \mid q \in \mathbb{Z}\} = \Lambda.$$

Den kanoniske homomorfi: $\mathbb{Z} \to \Lambda$ er altså surjektiv, og inducerer derfor en isomorfi:

$$\mathbb{Z}/n \xrightarrow{\approx} \Lambda,$$

hvor n er karakteristikken af Λ. Specielt er Λ kommutativ, da $\mathbb{Z}/n$ er kommutativ. Endelig er

$$n = |\mathbb{Z}/n| = |\Lambda| = p \quad \square$$

KOROLLAR. Restklasseringen $\mathbb{Z}/p$, hvor p er et primtal, er et (endeligt) legeme $\square$

NOTATION. For et primtal p betegnes legemet $\mathbb{Z}/p$ også $\mathbb{F}_p$.

BEMÆRKNING. Det fremgår af Sætning 1.9, at restklasseringene $\mathbb{Z}/n$, hvor $n \geq 1$ ikke er et primtal, ikke er integritetsområder.

1.11. PRIMLEGEME. Lad L være et legeme, og lad

$$R = \{q1_L \mid q \in \mathbb{Z}\}$$

betegne primringen i L. Som delring af L er R et kommutativt integritetsområde, så vi kan i L betragte brøklegemet for R:

$$\{(a1_L)(s1_L)^{-1} \mid a, s \in \mathbb{Z},\ s1_L \neq 0_L\}.$$

DEFINITION. Dette brøklegeme kaldes primlegemet i legemet L.

Blandt dellegemerne af L er primlegemet øjensynlig det mindste.
Hvis legemet L har karakteristik 0, er primringen isomorf med $\mathbb{Z}$, og primlegemet følgelig isomorft med $\mathbb{Q}$.
Hvis legemet L har karakteristik $p > 0$, så er p et primtal (Sætning 1.9), og primringen $\mathbb{Z}/p$ er selv et legeme. Primlegemet er altså $\mathbb{F}_p$.

1.12. KOMMUTATION. DEFINITION. I ringen Λ siges elementer $\lambda, \mu \in \Lambda$ at <u>kommutere</u>, hvis

$$\lambda\mu = \mu\lambda.$$

Elementet $\lambda \in \Lambda$ kaldes <u>centralt</u>, hvis det kommuterer med alle elementer $\mu \in \Lambda$. Delmængden bestående af centrale elementer i Λ kaldes <u>centrum</u> i Λ. Den betegnes ofte $\mathrm{Cent}(\Lambda)$. En ringhomomorfi $\varphi: \Gamma \to \Lambda$ kaldes <u>central</u>, hvis $\varphi(\gamma)$ er centralt i Λ for alle $\gamma \in \Gamma$.

OBSERVATION. Centret i en ring Λ er en (kommutativ) delring.

1.13. DEFINITIONER. Et element λ i ringen Λ kaldes <u>involutorisk</u>, hvis

$$\lambda^2 = 1,$$

<u>idempotent</u>, hvis

$$\lambda^2 = \lambda,$$

og <u>nilpotent</u>, hvis der findes et $N \in \mathbb{N}$, så at

$$\lambda^N = 0.$$

OBSERVATION. Hvis nul-reglen gælder, så er 1 og -1 de eneste involutioner, 0 og 1 er de eneste idempotenter, og 0 er det eneste nilpotente element,
thi ligningerne ovenfor kan skrives

$$(\lambda - 1)(\lambda + 1) = 0, \quad \lambda(\lambda - 1) = 0, \quad \lambda \cdots \lambda = 0.$$

2. Polynomiumsringen $R[X]$ i én variabel over en kommutativ ring R.

I det følgende betegner R en kommutativ ring.

2.1. BESKRIVELSE. Til den givne ring R kan man konstruere en større kommutativ ring $R[X]$ kaldet polynomiumsringen over R. Den indeholder R som delring og yderligere et bestemt element betegnet X, og opfylder, at ethvert element $p \in R[X]$ kan skrives

$$p = p_0 + p_1 X + \cdots + p_n X^n, \quad n \geq 0, \quad p_i \in R, \; i = 0, \ldots, n$$

og at denne fremstilling er entydig bortset fra eventuel tilføjelse/fjernelse af led af formen $0X^i$.

Elementerne $p \in R[X]$ kaldes polynomier (med koefficienter i R), og elementerne $p_i \in R$, $i = 0, 1, 2, \ldots$ kaldes koefficienterne i polynomiet p.

OBSERVATION. Kompositionerne i ringen $R[X]$ er helt bestemt ved beskrivelsen, thi for givne polynomier

$$p = p_0 + p_1 X + \cdots + p_n X^n$$
$$q = q_0 + q_1 X + \cdots + q_m X^m \qquad \text{(hvor f.eks. } m \geq n\text{)}$$

finder vi blot ved brug af regnereglerne, at

$$p+q = (p_0+q_0) + (p_1+q_1)X + \cdots + (p_n+q_n)X^n + q_{n+1}X^{n+1} + \cdots + q_m X^m$$

$$pq = (p_0 q_0) + (p_0 q_1 + p_1 q_0)X + (p_0 q_2 + p_1 q_1 + p_2 q_0)X^2 + \cdots + p_n q_m X^{n+m}.$$

BEMÆRKNING. Af entydigheden af fremstillingen

$$p = p_0 + p_1 X + \cdots + p_n X^n, \quad p_i \in R$$

følger, at polynomiet $p \in R[X]$ helt bestemmer sine koefficienter $p_i \in R$. Koefficienterne p_i er definerede for alle $i = 0, 1, 2, \ldots$, og de er $= 0$, når i er tilstrækkelig stor. Polynomier kan derfor defineres som værende sådanne følger af koefficienter. Af de fundne udtryk for sum og produkt af polynomier ses hvordan sum og produkt af sådanne koefficientfølger så må defineres.

2.2. Opfattet som polynomier kaldes elementerne i R også <u>konstanter</u>. De er karakteriseret ved at koefficienterne er $p_i = 0$, når $i > 0$. <u>Nulpolynomiet</u> er konstanten 0, hvis koefficienter er $p_i = 0$ for alle i. For alle polynomier $p \neq 0$ findes en koefficient $p_i \neq 0$.

DEFINITION. Lad $p \in R[X]$ være et polynomium $\neq 0$. Det største tal $n \geq 0$ så at $p_n \neq 0$ kaldes da <u>graden</u> af polynomiet p og betegnes $\operatorname{grad}(p)$ og elementet $p_n \in R$, $n = \operatorname{grad}(p)$, kaldes den <u>ledende koefficient</u> i p. Hvis den ledende koefficient er $1 \in R$, siges p at være et <u>normeret</u> polynomium.

Polynomierne af grad n er altså polynomierne af formen

$$p = p_0 + \cdots + p_n X^n, \quad p_i \in R, i = 0, \cdots, n, \quad p_n \neq 0,$$

og heraf har de normerede formen

$$p = X^n + p_{n-1} X^{n-1} + \cdots + p_0, \quad p_i \in R, \ i = 0, \cdots, n-1.$$

TILFØJELSE. Vi har ikke ovenfor tillagt nulpolynomiet nogen grad, og nulpolynomiet har således <u>ingen</u> ledende koefficient og det er specielt <u>ikke</u> normeret. Det er ofte hensigtsmæssigt at tillægge nulpolynomiet en grad,

der er $<$ alle andre graden (dvs. <0). I det følgende tillægger vi nulpolynomiet graden $-\infty$ [med oplagte konventioner for regning med $-\infty$].

Polynomier $p \in R[X]$ af grad $\leqslant n$ har altså formen

$$p = aX^n + \dots \quad , \quad a \in R,$$

hvor "..." står for et polynomium af grad $< n$. Hvis $\operatorname{grad}(p) = n$, dvs hvis $a \neq 0$, så er a den ledende koefficient.

2.3. OBSERVATION. Af de fundne udtryk for sum og produkt fremgår umiddelbart, at vi for polynomier $p, q \in R[X]$ har

$$\boxed{\begin{aligned} &(1) \quad \operatorname{grad}(p+q) \leqslant \max\{\operatorname{grad}(p), \operatorname{grad}(q)\} \\ &(2) \quad \operatorname{grad}(pq) \leqslant \operatorname{grad}(p) + \operatorname{grad}(q), \end{aligned}}$$

og at der gælder "$<$" i (1), netop når p og q har samme grad $\geqslant 0$ og modsatte ledende koefficienter. Videre ses, at der i (2) gælder "$=$", når $p, q \neq 0$ og produktet af de ledende koefficienter er $\neq 0$. Specielt fremhæves, at "$=$" gælder i (2), når et af polynomierne er normeret.

Lidt mere specielt fremhæves følgende

2.4. SÆTNING. *Lad R være et integritetsområde. Da er*

$$\boxed{\operatorname{grad}(pq) = \operatorname{grad}(p) + \operatorname{grad}(q)}, \quad p, q \in R[X].$$

Polynomiumringen $R[X]$ er også et integritetsområde, og de invertible polynomier er netop de konstanter, der er invertible i R.

BEVIS. Ligningen følger af det observerede, og heraf følger også nulreglen. Da $R \subseteq R[X]$, har vi $R^* \subseteq (R[X])^*$. For at vise "$\supseteq$" betragtes $p \in (R[X])^*$. Der findes altså $q \in R[X]$, så at $1 = pq$. Heraf fås $0 = \operatorname{grad}(1) = \operatorname{grad}(pq)$ $= \operatorname{grad}(p) + \operatorname{grad}(q)$, hvoraf $0 = \operatorname{grad}(p) = \operatorname{grad}(q)$.

Altså er $p, q \in R$, og af $1 = pq$ følger $p \in R^*$ ▨

2.5. DIVISIONSSÆTNING. Lad $d \in R[X]$ være et normeret polynomium. Til hvert polynomium $p \in R[X]$ findes da entydigt bestemte polynomier $q, r \in R[X]$, så at

$$p = qd + r \quad , \quad \text{med } \operatorname{grad}(r) < \operatorname{grad}(d).$$

BEVIS. Sæt $n = \operatorname{grad}(d) \geqslant 0$.

Eksistens: Hvis polynomiet p har grad $< n$ har vi fremstillingen $p = 0 \cdot d + p$, hvor $q = 0$ og $r = p$ har grad $< n$.

Antag derfor, at p har grad $m \geqslant n$ og ledende koefficient p_m, dvs at p har formen

$$p = p_m X^m + \cdots \quad , \quad \text{hvor } p_m \neq 0.$$

Da polynomiet d er normeret, har $p_m X^{m-n} d$ også denne form, og polynomiet $p - p_m X^{m-n} d$ har derfor grad $< m$. Induktivt har vi derfor en fremstilling

$$p - p_m X^{m-n} d = \tilde{q} d + r \quad , \quad \operatorname{grad}(r) < \operatorname{grad}(d),$$

og så er

$$p = (p_m X^{m-n} + \tilde{q}) d + r$$

en ønsket fremstilling af p.

Entydighed: Det er nok at betragte en fremstilling

$$0 = qd + r \quad , \quad \operatorname{grad}(r) < \operatorname{grad}(d).$$

Da d er normeret, fås heraf (Observation 2.3), at

$$\operatorname{grad}(r) = \operatorname{grad}(-qd) = \operatorname{grad}(q) + \operatorname{grad}(d).$$

Var $q \neq 0$ og dermed $\operatorname{grad}(q) \geqslant 0$, ville vi få modstriden $\operatorname{grad}(r) \geqslant \operatorname{grad}(d)$. Altså er $q = 0$ og dermed også $r = 0$ ▨

BEMÆRKNING. Hvis det om $d \in R[X]$, $d \neq 0$, blot forudsættes, at den ledende koefficient u er invertibel i R fås et tilsvarende resultat ved at anvende sætningen på det normerede polynomium $u^{-1} d$.

Hvis ringen R er et legeme, kan Divisionssætningen altså anvendes med et vilkårligt polynomium $d \neq 0$.

2.6 DEFINITION. Lad der være givet et polynomium

$$p = p_0 + p_1 X + \cdots + p_n X^n \in R[X]$$

og et element $a \in R$. Elementet $p_0 + p_1 a + \cdots + p_n a^n \in R$ betegnes da $p(a)$, altså

$$p(a) = p_0 + p_1 a + \cdots + p_n a^n \in R,$$

og det siges at fremkomme ved at indsætte elementet a i polynomiet p. Hvis $p(a) = 0$, siges a at være rod i polynomiet p.

OBSERVATION. For et fast element $a \in R$ er afbildningen

$$p \mapsto p(a)$$

en surjektiv ringhomomorfi : $R[X] \to R$. Dens kerne består af de polynomier, der har a som rod. De udgør altså et ideal i $R[X]$.

BEMÆRKNING. For et givet polynomium $p = p_0 + p_1 X + \cdots + p_n X^n \in R[X]$ vil udtrykket

$$p_0 + p_1 \alpha + \cdots + p_n \alpha^n$$

have mening, når blot α er et element i en ring Λ, der indeholder R som delring. Også i denne generelle situation skrives

$$p(\alpha) = p_0 + p_1 \alpha + \cdots + p_n \alpha^n.$$

Da $R[X] \supseteq R$, kan vi altså specielt skrive

$$p = p(X).$$

2.7. SÆTNING. Polynomiet $p \in R[X]$ har elementet $a \in R$ som rod, hvis og kun hvis det kan skrives

$$p = q \cdot (X - a),$$

med et polynomium $q \in R[X]$.

BEVIS. Anvendes Divisionssætningen 2.5 med 1^{ste}-gradspolynomiet $d = X - a$ fås en entydig fremstilling

$$p = q \cdot (X-a) + r, \quad \deg(r) < 1.$$

Polynomiet $r \in R[X]$ har altså grad ≤ 0, og er derfor konstant. Indsættelse af a giver

$$p(a) = q(a) \cdot 0 + r = r \in R.$$

Vi har altså $p(a) = 0$, hvis og kun hvis $r = 0$ ▨

KOROLLAR. Hvert polynomium $p \neq 0$ af grad n i $R[X]$ har en fremstilling

$$p = \tilde{p} \cdot (X-a_1) \cdots (X-a_k), \quad k \leq n, \quad a_i \in R,$$

hvor polynomiet $\tilde{p} \in R[X]$ ikke har rødder i R.
Hvis R er et integritetsområde, er fremstillingen entydig (bortset fra permutation af 1^{ste}-gradsfaktorerne), og

$$\{a_1, \ldots, a_k\} = \{a \in R \mid p(a) = 0\}.$$

Specielt er i dette tilfælde antallet af rødder i $p \leq \deg(p)$.

BEVIS. Hvis p ikke har rødder i R, får vi den ønskede fremstilling med $p = \tilde{p}$ og $k = 0$. Hvis p har en rod a_1, kan vi skrive $p = p_1 \cdot (X-a_1)$, og da $X - a_1$ er normeret er $\deg(p_1) = \deg(p) - 1 = n - 1$. Fortsættes nu med polynomiet p_1, får vi efter højst n skridt den ønskede fremstilling.
Antag nu, at R er et integritetsområde. Ud fra en fremstilling

$$p = \tilde{p} \cdot (X-a_1) \cdots (X-a_k), \ \tilde{p} \text{ uden rødder},$$

aflæser vi, at

$$\{a_1, \ldots, a_k\} = \{a \in R \mid p(a) = 0\},$$

thi "$\subseteq$" er oplagt, og er omvendt $p(a) = 0$, så er

$$0 = \tilde{p}(a)\,(a-a_1) \cdots (a-a_k);$$

da $\tilde{p}(a) \neq 0$, og da nul-reglen gælder, må en af de øvrige faktorer være 0.
Vi viser nu entydigheden ved induktion efter graden n. Entydigheden er klar, hvis $n = 0$, da p så er konstant.

Er $n > 0$, og har vi endnu en fremstilling

$$p = \tilde{q} \cdot (X-b_1)\cdots(X-b_\ell), \quad \tilde{q} \text{ uden rødder},$$

så er b_ℓ rod i p, altså ifølge det viste $b_\ell \in \{a_1, \dots, a_k\}$. Vi kan antage, at $b_\ell = a_k$. Af

$$p = \tilde{p} \cdot (X-a_1)\cdots(X-a_k) = \tilde{q} \cdot (X-b_1)\cdots(X-b_{\ell-1})(X-a_k)$$

følger imidlertid (da nul-reglen gælder i $R[X]$), at

$$\tilde{p} \cdot (X-a_1)\cdots(X-a_{k-1}) = \tilde{q} \cdot (X-b_1)\cdots(X-b_{\ell-1}).$$

Dette er fremstillinger af et polynomium af grad $n-1$, og induktionsforudsætningen giver derfor: $\tilde{p} = \tilde{q}$, $k-1 = \ell-1$ og (eventuelt efter permutation) $a_1 = b_1, \dots, a_{k-1} = b_{k-1}$. ▨

BEMÆRKNING. Lad $\nu \in \mathbb{N}$. Et element $a \in R$ siges da at være <u>ν-dobbelt rod</u> eller at være en <u>rod af multiplicitet ν</u> i polynomiet $p \in R[X]$, hvis p kan skrives

$$p = q \cdot (X-a)^\nu, \qquad q(a) \neq 0.$$

Hvis R er et integritetsområde, ses at antallet af rødder i p, "talt med multiplicitet", er $\leq \deg(p)$.

2.8. DEFINITION. For et polynomium

$$p = p_0 + p_1 X + \cdots + p_n X^n \in R[X]$$

er det <u>afledede</u> polynomium p' bestemt ved

$$p' = p_1 + 2p_2 X + \cdots + n p_n X^{n-1}$$

[hvor $i p_i = \overbrace{p_i + \cdots + p_i}^{i} \in R$]. Det er let at eftervise de sædvanlige regneregler:

$$(p+q)' = p' + q', \quad (pq)' = p'q + pq'.$$

SÆTNING. Lad R være et integritetsområde, og lad $a \in R$ være rod i polynomiet $p \in R[X]$. Da er a en rod af multiplicitet ≥ 2, netop når a også er rod i det afledede polynomium p'.

BEVIS. Prøv selv! □

2.9. Lad $d = X^n + d_{n-1}X^{n-1} + \cdots + d_1X + d_0 \in R[X]$ være et normeret polynomium af grad $n \geq 1$. Sættes

$$(d) := \{ qd \mid q \in R[X] \},$$

er (d) åbenbart et ideal i $R[X]$, og vi kan betragte kvotientringen $\Lambda := R[X]/(d)$ og den kanoniske homomorfi

$$\Theta : R[X] \to \Lambda.$$

Den sammensatte homomorfi $: a \mapsto \textcircled{a}$, der til et element $a \in R$ knytter ækvivalensklassen, der indeholder det konstante polynomium a, er da en injektiv homomorfi $: R \to \Lambda$, thi $\textcircled{a} = 0_\Lambda$ betyder, at $a \in (d)$, og da polynomierne $\neq 0$ i (d) har grad $\geq n \geq 1$, kan dette kun være opfyldt, når konstanten a er $= 0$. Idet vi identificerer elementerne $a \in R$ med deres billeder i Λ, kan vi opfatte R som en delring: $R \subseteq \Lambda$.

Herom gælder følgende

STRUKTURSÆTNING FOR POLYNOMIUMSKVOTIENTER.

Lad

$$d = X^n + d_{n-1}X^{n-1} + \cdots + d_1X + d_0 \quad , \quad n \geq 1,$$

være et normeret polynomium i $R[X]$. Kvotientringen $\Lambda := R[X]/(d)$ er da en kommutativ ring, som indeholder R, og sættes

$$\xi := \textcircled{X} \in \Lambda,$$

kan hvert element $\lambda \in \Lambda$ entydigt skrives

$$\lambda = r_0 + r_1\xi + \cdots + r_{n-1}\xi^{n-1}, \text{ med } r_0, r_1, \ldots, r_{n-1} \in R.$$

Endvidere gælder i Λ ligningen

$$(*) \quad \xi^n = -d_0 - d_1\xi - \cdots - d_{n-1}\xi^{n-1}.$$

BEVIS. Da $R[X]$ er kommutativ, er også kvotientringen Λ kommutativ. Lad $r_0, r_1, \ldots, r_{n-1}$ være elementer i R. Med de indførte identifikationer har vi

$$r_0 + r_1\xi + \cdots + r_{n-1}\xi^{n-1} = r_0 + r_1\textcircled{X} + \cdots + r_{n-1}\textcircled{X}^{n-1}$$

$$= \textcircled{r_0} + \textcircled{r_1}\textcircled{X} + \cdots + \textcircled{r_{n-1}}\textcircled{X}^{n-1} = \textcircled{r_0 + r_1X + \cdots + r_{n-1}X^{n-1}}$$

Ethvert element λ i kvotienten Λ har formen $\textcircled{p}$, hvor $p \in R[X]$. Vi har altså

$$\textcircled{p} = r_0 + r_1 \xi + \cdots + r_{n-1} \xi^{n-1},$$

netop når $\textcircled{p} = \overline{r_0 + r_1 X + \cdots + r_{n-1} X^{n-1}}$, dvs netop når p kan skrives

$$p = qd + r_0 + r_1 X + \cdots + r_{n-1} X^{n-1}, \quad q \in R[X].$$

Da Divisionssætningen udsiger, at ethvert polynomium p har en sådan entydig fremstilling, følger det, at ethvert $\lambda \in \Lambda$ entydigt kan skrives $\lambda = r_0 + r_1 \xi + \cdots + r_{n-1} \xi^{n-1}$, $r_0, r_1, \ldots, r_{n-1} \in R$.

Endelig har vi i Λ:

$$0_\Lambda = \textcircled{0} = \textcircled{d} = \overline{d_0 + d_1 X + \cdots + d_{n-1} X^{n-1} + X^n}$$

$$= d_0 + d_1 \xi + \cdots + d_{n-1} \xi^{n-1} + \xi^n,$$

og det er netop den anførte ligning ▨

BEMÆRKNINGER. (1) Hvis ringen $R = L$ er et legeme, ser vi at $1, \xi, \ldots, \xi^{n-1}$ er en basis for Λ som vektorrum over L. Dimensionen er netop graden n af det givne polynomium d.

(2) Multiplikationen i ringen Λ er bestemt af den anførte ligning (*), thi vi har

$$\xi^{n+1} = \xi^n \xi = -d_0 \xi - d_1 \xi^2 - \cdots - d_{n-2} \xi^{n-1} - d_{n-1} \xi^n$$

og v.hj.a. (*) kan $-d_{n-1} \xi^n$ skrives som "linearkombination" af $1, \xi, \ldots, \xi^{n-1}$. Induktivt får vi alle potenser $\xi^{n+1}, \xi^{n+2}, \ldots$ skrevet som "linearkombinationer" af $1, \xi, \ldots, \xi^{n-1}$.

(3). Opfattes det givne polynomium d som et polynomium med koefficienter i den større ring $\Lambda = R[X]/(d) \supseteq R$:

$$d \in R[X] \subseteq \Lambda[X],$$

ser vi, at det givne polynomium d i Λ har roden ξ, thi ligningen (*) kan skrives

$$d(\xi) = 0.$$

2.10. Strukturssætningen behandler kun kvotienter $R[x]/\mathfrak{a}$, hvor idealet $\mathfrak{a} \subseteq R[x]$ er af typen

$$\mathfrak{a} = (d) = \{ qd \mid q \in R[x] \}$$

med et normeret polynomium d af grad ≥ 1, og vi vil ikke her beskæftige os med idealer af andre typer. Hvis ringen R er et legeme er der essentielt ikke andre typer idealer. Dette er indholdet i følgende:

HOVEDIDEALSÆTNING. Lad L være et legeme. For hvert ideal $\mathfrak{a}$ i polynomiumsringen $L[x]$ findes et polynomium $d \in L[x]$, så at

$$\mathfrak{a} = \{ qd \mid q \in L[x] \}.$$

BEVIS. Hvis $\mathfrak{a} = \{0\}$, kan vi øjensynlig tage $d = 0$. Antag derfor at $\mathfrak{a} \neq \{0\}$. Vælg et polynomium $d \in \mathfrak{a} \setminus \{0\}$ hvis grad er mindst blandt alle graderne af polynomierne i $\mathfrak{a} \setminus \{0\}$. Det påstås, at

$$\mathfrak{a} = \{ qd \mid q \in L[x] \} = (d)$$

Her er "$\supseteq$" klart, thi da $d \in \mathfrak{a}$, og $\mathfrak{a}$ er et ideal, er også $qd \in \mathfrak{a}$, $q \in L[x]$.

Lad omvendt $p \in \mathfrak{a}$. Ifølge divisionssætningen kan vi skrive

$$p = qd + r, \qquad \deg(r) < \deg(d).$$

Da $\mathfrak{a}$ er et ideal, og $p, d \in \mathfrak{a}$, vil $r = p - qd \in \mathfrak{a}$. Hvis $r \neq 0$, ville

$$r \in \mathfrak{a} \setminus \{0\} \quad \text{og} \quad \deg(r) < \deg(d)$$

og det er i modstrid med valget af d. Følgelig er $r = 0$, og altså $p = qd \in (d)$ ▨

3. Nogle ring-konstruktioner.

3.1. PRODUKTRINGEN $\Lambda_1 \times \cdots \times \Lambda_r$. Er $\Lambda_1, \ldots, \Lambda_r$ ringe, kan vi i produktmængden

$$\Lambda := \Lambda_1 \times \cdots \times \Lambda_r$$

definere kompositioner koordinatvis: Addition er defineret ved

$$(\lambda_1, \ldots, \lambda_r) + (\mu_1, \ldots, \mu_r) := (\lambda_1 + \mu_1, \ldots, \lambda_r + \mu_r),$$

og multiplikation ved

$$(\lambda_1, \ldots, \lambda_r) \cdot (\mu_1, \ldots, \mu_r) := (\lambda_1 \mu_1, \ldots, \lambda_r \mu_r).$$

Med disse kompositioner er Λ en ring, kaldet <u>produktringen</u>. Nul-elementet og et-elementet i Λ er

$$0_\Lambda = (0, \ldots, 0) \quad \text{og} \quad 1_\Lambda = (1, \ldots, 1).$$

Bemærk, at den i'te koordinatprojektion

$$(\lambda_1, \ldots, \lambda_r) \longmapsto \lambda_i$$

er en surjektiv ringhomomorfi: $\Lambda_1 \times \cdots \times \Lambda_r \longrightarrow \Lambda_i$.

Et element $(\lambda_1, \ldots, \lambda_r) \in \Lambda$ er ógensynlig invertibelt (resp. regulært), netop når hvert λ_i er invertibelt (resp. regulært) i Λ_i. Specielt kan gruppen Λ^* af invertible elementer opfattes som produktet

$$\Lambda^* = \Lambda_1^* \times \cdots \times \Lambda_r^*.$$

BEMÆRKNING. Ovenstående kan umiddelbart generaliseres til produkter

$$\prod_{i \in I} \Lambda_i,$$

når Λ_i, $i \in I$ er en familie af ringe, og indexmængden I ikke nødvendigvis er endelig.

3.2. FUNKTIONSRINGEN $\Lambda^T = Afb(T,\Lambda)$. Er Λ en ring, og er T en mængde, kan vi i mængden

$$\Lambda^T = Afb(T,\Lambda)$$

af afbildninger $\varphi : T \to \Lambda$ definere kompositioner argumentvis: Addition er defineret ved

$$\varphi_1 + \varphi_2 : t \longmapsto \varphi_1(t) + \varphi_2(t),$$

og multiplikation ved

$$\varphi_1 \cdot \varphi_2 : t \longmapsto \varphi_1(t)\,\varphi_2(t).$$

Med disse kompositioner er $Afb(T,\Lambda)$ en ring, kaldet <u>funktionsringen</u>. Nul-elementet og et-elementet er de konstante afbildninger

$$0 : t \longmapsto 0 \quad \text{og} \quad 1 : t \longmapsto 1.$$

De konstante afbildninger udgør en delring, isomorf med Λ.

3.3. MATRIX-RINGEN $Mat_n(\Lambda)$. Er Λ en ring (og er $n \in \mathbb{N}$), kan vi i mængden

$$Mat_n(\Lambda)$$

af $n \times n$ - matricer med koefficienter i Λ på sædvanlig måde definere kompositioner: For matricer $\lambda = (\lambda_{ij})$ og $\mu = (\mu_{ij})$ er addition defineret ved

$$(\lambda + \mu)_{ij} = \lambda_{ij} + \mu_{ij}$$

og multiplikation ved

$$(\lambda\mu)_{ij} = \sum_{k=1}^{n} \lambda_{ik}\mu_{kj}.$$

Med disse kompositioner er $Mat_n(\Lambda)$ en ring, kaldet <u>matrixringen med koefficienter i Λ</u>. Nul-elementet og ét-elementet i $Mat_n(\Lambda)$ er diagonalmatricerne

$$0_n = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \quad \text{og} \quad 1_n = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}.$$

<u>Skalar-matricerne</u>, dvs diagonalmatricer af formen $\lambda 1_n = \begin{pmatrix} \lambda & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda \end{pmatrix}$, udgør en delring, isomorf med Λ.

3.4. ENDOMORFIRINGEN $End(M)$. Er $(M,+)$ en kommutativ gruppe, kan vi i mængden

$$End(M)$$

af endomorfier $\varphi : (M,+) \to (M,+)$ definere kompositioner som følger: For endomorfier φ og ψ er addition argumentvis defineret ved

$$\varphi + \psi : x \longmapsto \varphi(x) + \psi(x),$$

og multiplikation er sammensætning

$$\varphi \circ \psi : x \longmapsto \varphi(\psi(x)).$$

Med disse kompositioner er $End(M)$ en ring, kaldet endomorfiringen for gruppen M. Nul-elementet er den konstante afbildning

$$0 : x \longmapsto 0,$$

og et-elementet er den identiske afbildning

$$1 : x \longmapsto x.$$

De invertible elementer i $End(M)$ er automorfierne i M. Vi har altså

$$Aut(M) = End(M)^*.$$

3.5. POLYNOMIUMSRINGEN $\Lambda[X]$. Er Λ en ring, kan vi betragte mængden af de følger:

$$p = (p_0, p_1, p_2, \cdots), \quad p_i \in \Lambda,$$

som opfylder:

$$p_i = 0 \text{ på nær for endelig mange } i \in \tilde{\mathbb{N}}.$$

En sådan følge kaldes et polynomium med koefficienter i Λ. At en følge p er et polynomium, betyder at $p_i = 0$ fra et vist trin, altså at følgen har formen

$$p = (p_0, p_1, \cdots, p_n, 0, 0, 0, \cdots).$$

For polynomier p og q defineres addition koordinatvis ved

$$(p+q)_i = p_i + q_i,$$

og multiplikation er Cauchy-multiplikation defineret ved

$$(pq)_i = \sum_{j=0}^{i} p_j q_{i-j} = \sum_{j+k=i} p_i q_k .$$

Med disse kompositioner udgør polynomierne en ring, kaldet polynomiumsringen med koefficienter i Λ og betegnet $\Lambda[X]$. Nul-elementet og et-elementet er polynomierne

$$0 = (0,0,0,\cdots) \quad \text{og} \quad 1 = (1,0,0,\cdots)$$

Polynomier af formen $(\lambda,0,0,\cdots)$, $\lambda \in \Lambda$, kaldes konstante. De udgør en delring, isomorf med Λ. Vi vil oftist identificere et element $\lambda \in \Lambda$ med det tilsvarende konstante polynomium $(\lambda,0,0,\cdots)$, og altså opfatte Λ som en delring

$$\Lambda \subseteq \Lambda[X].$$

For produktet af en konstant $\lambda = (\lambda,0,0,\cdots)$ med et polynomium $p = (p_0, p_1, p_2, \cdots)$ finder vi

$$\lambda p = (\lambda p_0, \lambda p_1, \lambda p_2, \cdots) \quad \text{og}$$

$$p\lambda = (p_0\lambda, p_1\lambda, p_2\lambda, \cdots).$$

Det specielle polynomium $(0,1,0,0,\cdots)$ betegnes

$$X := (0,1,0,0,\cdots).$$

Vi finder

$$Xp = pX = (0, p_0, p_1, p_2, \cdots)$$

og for potenserne af X har vi derfor

$$X = (0,1,0,0,\cdots)$$
$$X^2 = (0,0,1,0,\cdots)$$
$$\vdots$$
$$X^i = (\underbrace{0,0,\cdots,0}_{i\ 0'er},1,0,\cdots)$$
$$\vdots$$

Er $\lambda_0, \cdots, \lambda_n \in \Lambda$, kan vi i $\Lambda[X]$ betragte elementet $\lambda_0 + \lambda_1 X + \cdots + \lambda_n X^n$. Af det foregående fås:

$$\lambda_0 + \lambda_1 X + \cdots + \lambda_n X^n = (\lambda_0, \lambda_1, \cdots, \lambda_n, 0, 0, \cdots).$$

Polynomiet $p = (p_0, \cdots, p_n, 0, 0, \cdots)$ kan altså skrives

$$p = p_0 + p_1 X + \cdots + p_n X^n.$$

Vi skriver også

$$p = \sum_{i \geq 0} p_i X^i,$$

idet kun endelig mange led i denne sum er $\neq 0$.

3.6. POTENSRÆKKERINGEN $\Lambda[[X]]$. Er Λ en ring, kan vi betragte mængden af alle følger

$$p = (p_0, p_1, p_2, \cdots), \quad p_i \in \Lambda.$$

Med kompositioner defineret ganske som for polynomier (jfr. 3.5) udgør disse følger en ring, kaldet ringen af (formelle) potensrækker med koefficienter i Λ, og betegnet $\Lambda[[X]]$.

Ifølge definitionen udgør polynomierne en delring

$$\Lambda[X] \subseteq \Lambda[[X]].$$

For en potensrække $p = (p_0, p_1, \cdots)$ skrives ofte formelt

$$p = \sum_{i \geq 0} p_i X^i = p_0 + p_1 X + p_2 X^2 + \cdots$$

Dette er en ren formel skrivemåde, der blot udtrykker, at potensrækken p som sin i-te koefficient har det der på højre side står som koefficient til X^i. Skrivemåden impliciter altså ikke nogen udregning (konvergens) af den uendelige sum på højre side.

3.7. POLYNOMIUMSRINGEN $\Lambda[X_1, \cdots, X_r]$. Er Λ en ring, kan vi betragte mængden af de afbildninger:

$$i \mapsto p_i$$

af: $\tilde{\mathbb{N}}^r \to \Lambda$, som opfylder

$$p_i = 0 \text{ på nær for endelig mange } i \in \tilde{\mathbb{N}}^r.$$

En sådan afbildning kaldes et polynomium i r variable med koefficienter i Λ.

[Her betegner $\mathbb{N}^r$ mængden af multi-indices

$$i = (i_1, \cdots, i_r) \quad , \quad i_\nu \in \tilde{\mathbb{N}}.$$

Vi minder om at multi-indices kan adderes: Med kompositionen givet ved

$$(i_1, \cdots, i_r) + (j_1, \cdots, j_r) := (i_1 + j_1, \cdots, i_r + j_r)$$

udgør de et monoid med $0 = (0, \cdots, 0)$ som neutralt element. Idet vi som bekendt for et multi-index $i = (i_1, \cdots, i_r)$ sætter

$$|i| = i_1 + \cdots + i_r \in \tilde{\mathbb{N}}$$

har vi øjensynlig

$$|i + j| = |i| + |j|. \ ]$$

For sådanne polynomier p og q defineres addition argumentvis ved

$$(p+q)_i = p_i + q_i$$

og multiplikation ved <u>Cauchy-multiplikation</u> givet ved

$$(pq)_i = \sum_{j+k=i} p_j q_k$$

[Det skal naturligvis overvejes, at summen her er endelig, og at den således definerede afbildning $\mathbb{N}^r \to \Lambda$ er et polynomium]

Med disse kompositioner udgør polynomierne en ring, kaldt <u>polynomiumsringen i r variable</u> med koefficienter i Λ, og betegnet $\Lambda[X_1, \cdots, X_r]$.

For hvert element $\lambda \in \Lambda$ defineres det tilsvarende <u>konstante</u> polynomium (også betegnet λ) ved

$$\lambda : i \longmapsto \begin{cases} \lambda & , \ i = (0, \cdots, 0) \\ 0 & \ i \neq (0, \cdots, 0). \end{cases}$$

For hvert multi-index j defineres polynomiet X^j ved

$$X^j : i \longmapsto \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases}$$

Med disse betegnelser finder vi for et givet polynomium p, at

$$p = \sum_i p_i X^i$$

Videre finder vi

$$X^i \cdot X^j = X^{i+j}$$

Idet vi indfører de specielle polynomier

$$X_1 := X^{(1,0,0,\cdots,0)}, \; X_2 = X^{(0,1,0,\cdots,0)}, \; \cdots, \; X_r = X^{(0,0,0,\cdots,1)}$$

og bemærker, at vi i $(\tilde{N}^r, +)$ har

$$(j_1, \cdots, j_r) = j_1(1,0,\cdots,0) + \cdots + j_r(0,0,\cdots,1),$$

har vi derfor

$$X^j = X^{(j_1,\cdots,j_r)} = X_1^{j_1} \cdots X_r^{j_r}.$$

Polynomiet p kan således entydigt skrives

$$p = \sum p_{i_1,\cdots,i_r} X_1^{i_1} \cdots X_r^{i_r},$$

hvor summen er endelig (eller rettere sagt: kun indeholder endelig mange led $\neq 0$).

3.8. FOLDNINGSRINGEN $\Lambda[M]$. Lad $(M,\cdot)$ være et multiplikativt skrevet monoid. Er Λ en ring, kan vi betragte mængden af de afbildninger

$$\varphi : M \to \Lambda,$$

som opfylder:

$$\varphi(s) = 0 \text{ på nær for endelig mange } s \in M.$$

For sådanne afbildninger φ og ψ definerer addition argumentvis ved

$$(\varphi + \psi)(s) = \varphi(s) + \psi(s)$$

og multiplikation er <u>foldning</u> $\varphi\psi := \varphi * \psi$ defineret ved

$$(\varphi * \psi)(s) = \sum_{u \cdot v = s} \varphi(u)\psi(v).$$

Med disse to kompositioner udgør de betragtede afbildninger en ring, kaldet foldningsringen over M med koefficienter i Λ, og betegnet $\Lambda[M]$.

For hvert element $\lambda \in \Lambda$ definerer et tilsvarende element i $\Lambda[M]$ (også betegnet λ) ved

$$\lambda(s) = \begin{cases} \lambda & \text{for } s = e_M \\ 0 & \text{for } s \neq e_M. \end{cases}$$

Herved kan vi opfatte Λ som en delring

$$\Lambda \subseteq \Lambda[M].$$

Endvidere kan vi for hvert element $u \in M$ betragte det ved

$$\delta_u(s) = \begin{cases} 1 & \text{når } s = u \\ 0 & \text{når } s \neq u \end{cases}$$

definerede element $\delta_u \in \Lambda[M]$. Vi finder

$$\delta_u \cdot \delta_v = \delta_{uv},$$

(og δ_e er et-elementet i $\Lambda[M]$), så $u \mapsto \delta_u$ er en injektiv monoid-homomorfi:

$$(M, \cdot) \longrightarrow (\Lambda[M], \cdot)$$

Er $u_1, \ldots, u_k$ forskellige elementer i M, og er $\lambda_1, \ldots, \lambda_k$ elementer i Λ, ses dit, at elementet

$$(*) \qquad \varphi = \lambda_1 \delta_{u_1} + \cdots + \lambda_k \delta_{u_k}$$

dannet i ringen $\Lambda[M]$ er afbildningen $\varphi : M \to \Lambda$ bestemt ved

$$\varphi(s) = \begin{cases} \lambda_i & \text{når } s = u_i \\ 0 & \text{når } s \notin \{u_1, \ldots, u_k\}. \end{cases}$$

Det følger, at hvert element $\varphi \in \Lambda[M]$ har en entydig fremstilling af formen $(*)$. Fremstillingen skrives også

$$\varphi = \sum_{u \in M} \lambda_u \delta_u,$$

idet det underforstås, at kun endelig mange koefficienter $\lambda_u = \varphi(u)$ er $\neq 0$.

Hvis misforståelser er udelukkede, identificerer man elementerne $u \in M$ med deres billeder $\delta_u \in \Lambda[M]$, og opfatter altså M som en delmængde

$$M \subseteq \Lambda[M].$$

Elementerne i $\Lambda[M]$ er da endelige summer

$$\varphi = \lambda_1 u_1 + \cdots + \lambda_k u_k, \quad \lambda_1, \ldots, \lambda_k \in \Lambda, \ u_1, \ldots, u_k \in M,$$

der også skrives

$$\varphi = \sum_{u \in M} \lambda_u u.$$

NOTATION. Betragtes et additivt skrevet monoid $(M,+)$ (med neutralt element 0), er det sædvanligt at skrive X^u for δ_u. I foldningsringen $\Lambda[M]$ har vi da

$$X^u X^v = X^{u+v} \quad (\text{og } X^0 = 1 \in \Lambda[M]).$$

Elementerne i $\Lambda[M]$ er da endelige summer

$$\varphi = \lambda_1 X^{u_1} + \cdots + \lambda_k X^{u_k},$$

der også skrives

$$\varphi = \sum_{u \in M} \lambda_u X^u.$$

EKSEMPLER. Foldningsringen over monoidet $(\tilde{\mathbb{N}},+)$ er polynomiumsringen $\Lambda[X]$, jfr. 3.5. Foldningsringen over monoidet $(\tilde{\mathbb{N}}^r,+)$ er polynomiumsringen $\Lambda[X_1,\ldots,X_r]$, jfr. 3.7.

BEMÆRKNING. Hvis det givne monoid er en gruppe, kaldes foldningsringen $\Lambda[G]$ også <u>gruppering</u>. Foldningen kan her defineres ved

$$\varphi * \psi(s) = \sum_{u \in G} \varphi(u)\,\psi(u^{-1}s)$$

3.9. FOLDNINGSRÆKKERINGEN $\Lambda[[M]]$. Hvis et givet monoid $(M,\cdot)$ har den egenskab, at der for hvert $s \in M$ kun findes endelig mange par $(u,v) \in M \times M$ så at $uv = s$, kan kompositionerne definerede i 3.8 umiddelbart udvides til kompositioner defineret i mængden af <u>alle</u> afbildninger

$$\varphi : M \to \Lambda.$$

Med disse kompositioner udgør afbildningerne $\varphi : M \to \Lambda$ en ring, kaldet ringen af (formelle) <u>foldningsrækker</u> og betegnet $\Lambda[[M]]$. Vi har

$$\Lambda[M] \subseteq \Lambda[[M]]$$

(med "$=$", netop når M er endelig).

EKSEMPLER. Monoidet $(\tilde{\mathbb{N}}, +)$ har den anførte egenskab; den tilhørende rekkefølge er ringen af formelle potensrækker $\Lambda[[X]]$, jfr. 3.6. Monoidet $(\tilde{\mathbb{N}}^r, +)$ har den anførte egenskab; den tilsvarende rekkefølge kaldes ringen af (formelle) potensrækker i r variable og betegnes $\Lambda[[X_1, \dots, X_r]]$.
Monoidet $(\mathbb{N}, \cdot)$ har også den anførte egenskab; den tilsvarende rekke-ring kaldes ringen af formelle Dirichlet-rækker.

4. Algebraer.

I det følgende betegner R en kommutativ ring.

4.1. DEFINITION. En *R-algebra* $(A,+,\cdot,R)$ er en mængde A forsynet med tre kompositioner, en (indre) *addition*: $A\times A\to A$ betegnet $(\alpha,\beta)\mapsto \alpha+\beta$, en (indre) *multiplikation*: $A\times A\to A$ betegnet $(\alpha,\beta)\mapsto \alpha\cdot\beta$ og en (ydre) *multiplikation med skalar*: $R\times A\to A$ betegnet $(r,\alpha)\mapsto r\alpha$, således at følgende er opfyldt:

(a) Med hensyn til addition er A en kommutativ gruppe. Der findes altså et *nul-element* $0\in A$ og for hvert element $\alpha\in A$ et *modsat* element $-\alpha$, så at

$$\begin{cases} \alpha+\beta=\beta+\alpha, \\ (\alpha+\beta)+\gamma=\alpha+(\beta+\gamma), \\ \alpha+0=\alpha, \\ \alpha+(-\alpha)=0. \end{cases} \qquad \alpha,\beta,\gamma\in A$$

(s) Multiplikation med skalar er "lineær" i den forstand at

$$\begin{cases} 1\alpha=\alpha, \\ r(\alpha+\beta)=r\alpha+r\beta, \\ (r+s)\alpha=r\alpha+s\alpha \\ (rs)\alpha=r(s\alpha). \end{cases} \qquad r,s\in R,\ \alpha,\beta\in A$$

(d) Multiplikationen er distributiv med hensyn til addition, dvs

$$\begin{cases} \alpha\cdot(\beta+\gamma)=\alpha\cdot\beta+\alpha\cdot\gamma, \\ (\alpha+\beta)\cdot\gamma=\alpha\cdot\gamma+\beta\cdot\gamma. \end{cases} \qquad \alpha,\beta,\gamma\in A$$

(h) Multiplikation og multiplikation med skalar "harmonerer" i den forstand at

$$\begin{cases} (r\alpha)\cdot\beta=r(\alpha\cdot\beta), \\ \alpha\cdot(r\beta)=r(\alpha\cdot\beta). \end{cases} \qquad r\in R,\ \alpha,\beta\in A$$

En R-algebra $(A,+,\cdot,R)$ kaldes også en *algebra over* R.

BEMÆRKNING. For en algebra $(A,+,\cdot,L)$ over et legeme L udsiger betingelserne (a) og (s), at $(A,+,L)$ er et vektorrum over legemet L, og betingelserne (d) og (h) udsiger, at multiplikationen $\cdot : A\times A \to A$ er bilineær.

4.2. Udover de anførte betingelser vil man i almindelighed forudsætte, at algebraens multiplikation opfylder yderligere betingelser. Ved betingelsen:

$$\begin{cases} \alpha\cdot\alpha = 0, \\ \alpha\cdot(\beta\cdot\gamma) + \beta\cdot(\gamma\cdot\alpha) + \gamma\cdot(\alpha\cdot\beta) = 0 \end{cases} \qquad \alpha,\beta,\gamma \in A$$

defineres således en Lie-algebra. Ved betingelsen:

$$\begin{cases} \alpha\cdot\beta = \beta\cdot\alpha \\ (\alpha\cdot\beta)\cdot(\alpha\cdot\alpha) = \alpha\cdot[\beta\cdot(\alpha\cdot\alpha)] \end{cases} \qquad \alpha,\beta \in A$$

defineres en Jordan-algebra. Ved betingelsen:

$$\begin{cases} (\alpha\cdot\alpha)\cdot\beta = \alpha\cdot(\alpha\cdot\beta), \\ \alpha\cdot(\beta\cdot\beta) = (\alpha\cdot\beta)\cdot\beta \end{cases} \qquad \alpha,\beta \in A$$

defineres en alternativ algebra. Endelig defineres ved betingelsen (hvor $1\in A$ er et givet element):

$$\begin{cases} 1\cdot\alpha = \alpha\cdot 1 = \alpha, \\ \alpha\cdot(\beta\cdot\gamma) = (\alpha\cdot\beta)\cdot\gamma \end{cases} \qquad \alpha,\beta,\gamma \in A$$

en såkaldt associativ algebra med et-element. Denne betingelse udtrykker, at $(A,\cdot)$ er et monoid, og sammen med betingelserne 4.1 (a) og (d) udsiger det, at $(A,+,\cdot)$ er en ring.

RESERVATION. Vi vil udelukkende beskæftige os med algebraer af den sidste type, og vi vil reservere benævnelsen "algebra" til denne situation. I en R-algebra $(A,+,\cdot,R)$ vil altså $(A,+,\cdot)$ være en ring, og multiplikation med skalar: $R\times A \to A$ vil opfylde betingelserne 4.1. (s) og (h). Algebraen kaldes kommutativ, hvis multiplikationen er kommutativ.

4.3. Lad $(A,+,\cdot,R)$ være en R-algebra (jfr. Reservation 4.2.),

og lad $1_A \in A$ være ét-elementet i ringen A. Af betingelserne følger let, at vi har

$$r\alpha = (r1_A)\cdot\alpha = \alpha\cdot(r1_A), \quad r\in R,\ \alpha\in A.$$

At multiplicere algebraelementet $\alpha\in A$ med skalaren $r\in R$ er således det samme som at multiplicere α med algebraelementet $r1_A \in A$.

Det følger videre af betingelserne, at den ved

$$\varphi(r) := r1_A$$

bestemte afbildning er en ringhomomorfi $: R \to A$, og at den er central (dvs billederne $\varphi(r) = r1_A$, $r\in R$ kommuterer med elementerne $\alpha\in A$). Denne homomorfi

$$\varphi : R \to A$$

kaldes algebraens <u>strukturhomomorfi</u>. Den bestemmer R-algebrastrukturen på ringen $(A,+,\cdot)$, idet vi jo har

$$r\alpha = \varphi(r)\cdot\alpha.$$

OBSERVATION. Er der omvendt givet en ring A og en central ringhomomorfi $\varphi: R\to A$, så organiseres A ved at <u>definere</u>

$$r\alpha := \varphi(r)\cdot\alpha$$

som multiplikation med skalar til en R-algebra $(A,+,\cdot,R)$. I overensstemmelse hermed kan R-algebraen betegnes (A,φ).

4.4. EKSEMPLER. (1) Enhver ring A kan entydig opfattes som en $\mathbb{Z}$-algebra idet multiplikation med en skalar $m\in\mathbb{Z}$ er

$$m\alpha = m\text{'te additive potens af } \alpha \text{ i } (A,+).$$

Strukturhomomorfien er den kanoniske ringhomomorfi:

$$\mathbb{Z} \to A.$$

(2) Ringen R kan opfattes som en algebra over sig selv, idet multiplikation med skalar $: R\times R \to R$ blot er multiplikation i ringen R. Strukturhomomorfien er

er her den identiske afbildning : $R \xrightarrow{=} R$.

(3) Mere generelt kan vi for en homomorfi $\varphi: R \to A$ mellem kommutative ringe opfatte A som en (kommutativ) R-algebra med φ som strukturhomomorfi.

(4) Enhver ring A kan opfattes som algebra over en delring, der er indeholdt i centrum for A. Specielt kan A opfattes som algebra over sin primring.

(5) Funktionsringen $Afb(T,R)$ kan opfattes som en R-algebra, idet multiplikation af en funktion $t \mapsto \psi(t)$ med en skalar $r \in R$ er bestemt ved

$$(r\psi)(t) := r\,\psi(t), \quad t \in T.$$

Strukturhomomorfien afbilder en skalar $r \in R$ over i den konstante funktion : $t \mapsto r$.

(6). Matrixringen $Mat_n(R)$ kan opfattes som en R-algebra, idet multiplikation af en matrix $\alpha = (\alpha_{ij})$ med en skalar $r \in R$ er bestemt ved

$$r\alpha := (r\alpha_{ij}).$$

Strukturhomomorfien afbilder en skalar $r \in R$ over i skalarmatricen $\begin{pmatrix} r & & 0 \\ & \ddots & \\ 0 & & r \end{pmatrix}$.

(7) Endomorfiringen $End_L(V)$ af lineære endomorfier i et vektorrum V over et legeme L kan opfattes som en L-algebra, idet multiplikation af en endomorfi $f: V \to V$ med en skalar $\lambda \in L$ er bestemt ved

$$(\lambda f)(v) = \lambda f(v) \quad (= f(\lambda v)).$$

Strukturhomomorfien afbilder en skalar $\lambda \in L$ over i homotetien : $v \mapsto \lambda v$.

(8) Polynomiumsringen $R[X]$ kan opfattes som en R-algebra, idet multiplikation af et polynomium $p = p_0 + \cdots + p_n X^n$ med en skalar $r \in R$ er polynomiet

$$rp = rp_0 + \cdots + rp_n X^n.$$

Strukturhomomorfien afbilder en skalar $r \in R$ over i

konstantun (også betegnet) $r \in R[X]$.

4.5. DEFINITION. En afbildning $f: A \to A'$ mellem R-algebraer kaldes en <u>R-algebra-homomorfi</u>, hvis den respekterer strukturen i den forstand, at

$$\begin{aligned} f(\alpha+\beta) &= f(\alpha)+f(\beta), \\ f(\alpha\beta) &= f(\alpha)f(\beta), \\ f(1_A) &= 1_{A'} \\ f(r\alpha) &= r f(\alpha). \end{aligned} \qquad \alpha,\beta \in A,\ r \in R.$$

OBSERVATION. De første 3 betingelser udsiger, at f er en ringhomomorfi $: (A,+,\cdot) \to (A',+,\cdot)$, og den sidste udsiger om strukturhomomorfierne $\varphi: R \to A$ og $\varphi': R \to A'$, at

$$f \circ \varphi = \varphi'.$$

4.6. DEFINITION. Lad $(A,+,\cdot,R)$ være en algebra over R, med strukturhomomorfien $\varphi: R \to A$. Ved en <u>del-algebra</u> af A forstås en delring $B \subseteq A$, som indeholder $\varphi(R)$. Det følger, at vi kan opfatte φ som en ringhomomorfi $\varphi: R \to B$, og med den som strukturhomomorfi bliver B selv en R-algebra, og inklusionsafbildningen

$$B \hookrightarrow A$$

bliver en R-algebrahomomorfi.

Ved et <u>ideal</u> i A forstås et ideal $\mathfrak{a}$ i ringen A. Med den sammensatte homomorfi $: R \to A \to A/\mathfrak{a}$ som strukturhomomorfi bliver kvotientringen $A/\mathfrak{a}$ en R-algebra (kaldet <u>kvotientalgebraen</u>), og den kanoniske afbildning

$$\sigma: A \to A/\mathfrak{a}$$

bliver en R-algebra-homomorfi.

4.7. OBSERVATION. Lad A være en algebra over R, og lad $\alpha \in A$ være et element. Da findes en mindste delalgebra af A, som indeholder elementet α, thi en sådan delalgebra B må indeholde alle elementerne $1_A, \alpha, \alpha^2, \alpha^3, \cdots$, og dermed også alle summer:

$$r_0 1_A + r_1 \alpha + \cdots + r_n \alpha^n, \quad r_0, \cdots, r_n \in R,$$

og da disse summer øjensynlig udgør en delalgebra (som indeholder α), må det være den mindste.

DEFINITION. Den ovenfor beskrevne delalgebra af A kaldes <u>delalgebraen frembragt af α</u>, og betegnes

$$R[\alpha] := \{ r_0 1_A + r_1 \alpha + \cdots + r_n \alpha^n \mid r_0, \cdots, r_n \in R \}.$$

BEMÆRKNING. Er der mere generelt i A givet endelig mange elementer $\alpha_1, \cdots, \alpha_k$, kan man mere generelt beskrive den mindste delalgebra af A, som indeholder elementerne $\alpha_1, \cdots, \alpha_k$. Hvis elementerne <u>kommuterer</u>, dvs hvis $\alpha_i \alpha_j = \alpha_j \alpha_i$, $i, j = 1, \cdots, k$, bliver beskrivelsen simpel: Delalgebraen består af de elementer, der er endelige summer af elementer af formen

$$r \alpha_1^{\nu_1} \cdots \alpha_k^{\nu_k}, \quad r \in R, \quad \nu_1 \geq 0, \cdots, \nu_k \geq 0,$$

og den betegnes i så fald $R[\alpha_1, \cdots, \alpha_k]$.

4.8. DEFINITION. Lad A være en R-algebra, og lad $\alpha \in A$ være et element. For et polynomium $p = p_0 + p_1 X + \cdots + p_n X^n \in R[X]$ siges det ved

$$p(\alpha) := p_0 1_A + p_1 \alpha + \cdots + p_n \alpha^n \in A$$

definerede algebraelement at fremkomme ved at <u>indsætte α i p</u>. Hvis $p(\alpha) = 0$, siges α at <u>være rod</u> i p.

SÆTNING. Lad α være et element i R-algebraen A. Da findes netop én R-algebra-homomorfi $R[X] \to A$, således at $X \mapsto \alpha$, nemlig afbildningen $p \mapsto p(\alpha)$. Dens billede er delalgebraen $R[\alpha] \subseteq A$, og dens kerne består af de polynomier, der har α som rod.

BEVIS. Blot en oversættelse af definitionerne. □

BEMÆRKNING. Af Isomorfisætning for ringe får vi en isomorfi:

$$R[x] / \{p \in R[x] \mid p(\alpha) = 0\} \xrightarrow{\approx} R[\alpha],$$

som åbenbart er en R-algebra-homomorfi.

4.9. DEFINITION. Et element α i R-algebraen A kaldes <u>algebraisk</u> (over R), hvis der findes et $n \in \tilde{N}$, og elementer $r_0, r_1, \ldots, r_n \in R$, som ikke alle er 0, således at

$$r_0 1_A + r_1 \alpha + \cdots + r_n \alpha^n = 0.$$

Et element $\alpha \in A$, som ikke er algebraisk, kaldes <u>transcendent</u> (over R).

OBSERVATION. Et element $\alpha \in A$ er transcendent (resp. algebraisk), netop når $p \mapsto p(\alpha)$ er injektiv (resp. ikke injektiv).

4.10. I det følgende betragtes en algebra A over et <u>legeme</u> L. Vi minder om at A i så fald specielt kan betragtes som vektorrum over L. Det ses, at et element $\alpha \in A$ er algebraisk over L, netop når elementerne $1, \alpha, \alpha^2, \ldots$ er lineært afhængige.

SÆTNING. Lad A være en algebra over et legeme L, og lad $\alpha \in A$ være et algebraisk element. Blandt polynomierne i $L[x]$, der har α som rod, findes da netop ét normeret polynomium f, således at ethvert polynomium p, der har α som rod, kan skrives

$$p = qf, \quad q \in L[x].$$

BEVIS. Anvend Hovedidealsætning 2.10 □

DEFINITION. Det i sætningen nævnte entydige polynomium f kaldes det <u>minimale</u> polynomium for α, og det betegnes $f_{\alpha/L}$. Dets grad kaldes også <u>graden</u> af α, og kan betegnes $\deg(\alpha)$.

4.11. SÆTNING. Lad A være en algebra over legemet L, lad $\alpha \in A$, og betragt den ved $p \mapsto p(\alpha)$ definerede homomorfi:

$$L[X] \longrightarrow A.$$

(t) Elementet α er transcendent, hvis og kun hvis $L[\alpha]$ er uendelig-dimensional som vektorrum over L. I bekræftende fald inducerer homomorfien en isomorfi:

$$L[X] \xrightarrow{\approx} L[\alpha].$$

(a) Elementet α er algebraisk, hvis og kun hvis $L[\alpha]$ er endelig-dimensional som vektorrum over L. I bekræftende fald inducerer homomorfien en isomorfi:

$$L[X]/(f_{\alpha/L}) \xrightarrow{\approx} L[\alpha],$$

og α's grad er

$$\deg(\alpha) = \dim L[\alpha].$$

BEVIS. Hvis α er transcendent, er elementerne $1, \alpha, \alpha^2, \ldots$ lineært uafhængige, så $\dim L[\alpha] = \infty$.
Hvis α er algebraisk, har vi $\{p \in L[X] \mid p(\alpha) = 0\} = (f_{\alpha/L})$ ifølge definitionen af $f_{\alpha/L}$, og homomorfien inducerer derfor den beskrevne isomorfi. Sættes $n = \deg(\alpha) = \deg(f_{\alpha/L})$, følger det af Strukturssetning for polynomiumskvotienter 2.9, at $①, ⓧ, \ldots ⓧ^{n-1}$ er en basis for $L[X]/(f_{\alpha/L})$, og deres billeder $1, \alpha, \ldots, \alpha^{n-1}$ er derfor en basis for $L[\alpha]$. Specielt er $\dim L[\alpha] = n$.
Heraf følger påstandene ▨

KOROLLAR. Hvis algebraen A er endelig-dimensional over legemet L, så er hvert element $\alpha \in A$ algebraisk af grad $\leqslant \dim_L A$. □

BEMÆRKNING. For et legeme L og et givet normeret polynomium $f \in L[X]$ kan vi betragte kvotientalgebraen $A = L[X]/(f)$, og heri elementet $ⓧ$. Det er klart, at $A = L[ⓧ]$, og at den kanoniske homomorfi $\Theta: L[X] \to L[X]/(f)$ er afbildningen $p \mapsto p(ⓧ)$. Det følger, at $ⓧ$ er algebraisk og at f er det minimale polynomium. Specielt er $\deg(ⓧ) = \deg(f)$.

IDEALER I KOMMUTATIVE RINGE.

1. Idealer. Hovedidealer. 1.1: Ideal. Trivielt ideal. 1.2: Idealoperationerne. 1.4: Hovedidealring. $\mathbb{Z}$ og $L[x]$. En numerisk betingelse. 1.5: Den opstigende kædes egenskab.

2. Primideal og maksimalideal. 2.1: Ideal og kongruensrelation. 2.2: Primideal. 2.3: Karakterisering af primideal. 2.4: Maksimalideal. 2.5: Karakterisering af maksimalideal. 2.6: Sætning. 2.7: Legemet $\mathbb{Z}/\mathbb{Z}p$.

3. Faktorielle ringe. 3.1: Definitioner. 3.3: Karakterisering ved hovedidealer. 3.4: Irreducible elementer i et hovedidealområde. 3.5: Opløsninger. 3.6: Primopløsningers entydighed. 3.7: Faktoriel ring. 3.8: Lemma. 3.9: Hovedsætning om hovedidealområder. 3.10: Anvendelse på $\mathbb{Z}$. 3.11: Anvendelse på $L[x]$. 3.12: Repræsentantsystem for primelementer.

4. Største fælles divisor. 4.1: Største fælles divisor. Primisk. 4.2: Karakterisering ved hovedideal. 4.3: Hovedidealområder. 4.4: Euklid's algoritme. 4.5: Faktoriel ring. 4.6: Lemma. 4.7: Den kinesiske restklassesætning. 4.8. Bemærkning.

5. Gauß' sætning. 5.1: Sætning. 5.2. Primitivt polynomium. 5.3: Gauß' lemma. 5.4: Bemærkning. 55: Korollar til Gauß' lemma. 5.7: Gauß' sætning. 5.8: Anvendelse. 5.9: Schönemann-Eisenstein's kriterium. 5.10: Eksempler.

6. Appendix: Kvadratiske talringe. 6.1: Kvadratisk tal. 6.2: Lemma. 6.3: Konjugeret tal. Norm. 6.4: Observation. 6.5: Ringen $\mathbb{Z}[\xi]$. 6.6: Morale. 6.7: Enheder i $\mathbb{Z}[\xi]$. 6.8: Divisorer inden for $\mathbb{Z}[\xi]$. 6.9: Specielle resultater. 6.10: $\mathbb{Z}[\sqrt{-5}]$. 6.11: Forgrening. 6.12: Forgrening i $\mathbb{Z}[i]$. 6.13: Ligningen $x^2+y^2=k$. 6.14: Pythagoræiske tal.

IDEALER I KOMMUTATIVE RINGE

I det følgende betegner R en kommutativ ring.

1. Idealer. Hovedidealer.

1.1. Vi minder om, at et ideal i R er en delmængde $\mathfrak{a} \subseteq R$, som opfylder:

(a1) $a_1, a_2 \in \mathfrak{a} \Rightarrow a_1 + a_2 \in \mathfrak{a}$

(a2) $0 \in \mathfrak{a}$

(a3) $a \in \mathfrak{a} \Rightarrow -a \in \mathfrak{a}$

(m) $a \in \mathfrak{a} \wedge r \in R \Rightarrow ra \in \mathfrak{a}$.

Betingelserne (a1),(a2),(a3) udsiger, at $\mathfrak{a}$ er en undergruppe i ringens additive gruppe $(R,+)$. De trivielle idealer i R er delmængden $\{0\}$ og hele mængden R.

OBSERVATION. (a3) følger af (m), thi $-a = (-1)a$.

IDEALOPERATIONERNE.

1.2. Det er let at se, at en vilkårlig fællesmængde af idealer i R igen er et ideal i R. For endelig mange idealer $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ i R er også delmængden

$$\mathfrak{a}_1 + \cdots + \mathfrak{a}_n := \{a_1 + \cdots + a_n \mid a_1 \in \mathfrak{a}_1 \wedge \cdots \wedge a_n \in \mathfrak{a}_n\}$$

et ideal i R. Det er øjensynlig det mindste ideal i R, der indeholder alle idealerne $\mathfrak{a}_1, \dots, \mathfrak{a}_n$. For et element $a \in R$ er delmængden

$$Ra := \{ra \mid r \in R\}$$

et ideal i R, og det er øjensynlig det mindste ideal i R, som indeholder elementet a. For endelig mange elementer $a_1, \dots, a_n \in R$ finder vi

$$Ra_1 + \cdots + Ra_n = \{r_1 a_1 + \cdots + r_n a_n \mid r_1, \dots, r_n \in R\},$$

og dette ideal er øjensynlig det mindste ideal, der indeholder elementerne $a_1, \dots, a_m \in R$.

DEFINITION. Idealet $\mathfrak{a}_1 + \cdots + \mathfrak{a}_m$ kaldes <u>summen</u> af idealerne $\mathfrak{a}_1, \dots, \mathfrak{a}_m$.
Idealet Ra kaldes <u>idealet frembragt af a</u>, og det betegnes ofte (a). Et ideal $\mathfrak{a} \subseteq R$, der har formen $\mathfrak{a} = Ra$, med $a \in R$, kaldes et <u>hovedideal</u>.
Idealet $Ra_1 + \cdots + Ra_n$ kaldes <u>idealet frembragt af $a_1, \dots, a_n$</u>, og det betegnes ofte $(a_1, \dots, a_n)$. Et ideal $\mathfrak{a} \subseteq R$, der har formen $\mathfrak{a} = Ra_1 + \cdots + Ra_m$, med $a_1, \dots, a_m \in R$, siges at være <u>endeligt frembragt</u>.

OBSERVATION. De trivielle idealer i R kan skrives $\{0\} = (0)$ og $R = (1)$. De er altså hovedidealer.

1.3. En vilkårlig foreningsmængde af idealer i R vil sædvanligvis ikke være et ideal. Herom gælder imidlertid følgende:
SÆTNING. Lad $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$ være en følge af idealer i R. Da er foreningsmængden $\mathfrak{a} := \bigcup_{n \in \mathbb{N}} \mathfrak{a}_n$ et ideal.
BEVIS. Lad $a_1, a_2 \in \mathfrak{a}$. Der findes da $n_1, n_2 \in \mathbb{N}$, så at $a_1 \in \mathfrak{a}_{n_1}$, $a_2 \in \mathfrak{a}_{n_2}$. Er $\mathfrak{a}_m$ det største af idealerne $\mathfrak{a}_{n_1}$ og $\mathfrak{a}_{n_2}$, har vi således $a_1, a_2 \in \mathfrak{a}_m$, og så er

$$a_1 + a_2 \in \mathfrak{a}_m \subseteq \bigcup_n \mathfrak{a}_n = \mathfrak{a}.$$

Delmængden $\mathfrak{a} \subseteq R$ opfylder således betingelsen 1.1 (a1). De øvrige betingelser er trivielt opfyldte □

1.4. DEFINITION. En ring R kaldes en <u>hovedidealring</u>, hvis alle dens idealer er hovedidealer. Er ringen R desuden et integritetsområde, kaldes den et <u>hovedidealområde</u>.

Følgende er et velkendt
RESULTAT. De hele tals ring $\mathbb{Z}$ og enhver polynomiumsring $L[X]$, hvor L er et legeme, er hovedidealområder.

Beviserne (for $\mathbb{Z}$ og for $L[X]$) har fælles træk, der abstrakt kan formuleres som en

NUMERISK BETINGELSE. Antag, at der i ringen R er givet en funktion $\nu : R \to \mathbb{Z}$, som er nedad begrænset og har følgende egenskab: For ethvert $d \neq 0$ i R og ethvert $a \in R$ findes et element $q \in R$, så at

$$\nu(a - qd) < \nu(d).$$

Da er R en hovedidealring.

BEVIS. Lad $\mathfrak{a} \subseteq R$ være et ideal. Vi skal vise, at der findes et element $d \in R$, således at $\mathfrak{a} = Rd$. Hvis $\mathfrak{a} = \{0\}$, kan vi bruge $d = 0$. Hvis $\mathfrak{a} \supset \{0\}$, kan vi betragte det mindste af tallene

$$\nu(r), \quad r \in \mathfrak{a} \setminus \{0\}.$$

[Det findes, da funktionen ν er nedad begrænset]. Det har formen $\nu(d)$, $d \in \mathfrak{a} \setminus \{0\}$. Nu gælder

$$\mathfrak{a} = Rd,$$

thi da $d \in \mathfrak{a}$ har vi trivielt "$\supseteq$", og er omvendt $a \in \mathfrak{a}$ kan vi finde $q \in R$, så at $r := a - qd$ opfylder

$$\nu(r) < \nu(d).$$

Da $a \in \mathfrak{a}$ og $qd \in Rd \subseteq \mathfrak{a}$, 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 altså $a = qd \in Rd$ ∎

BEMÆRKNING. For $R = \mathbb{Z}$ følger det af Divisionssætningen, at funktionen $\nu : p \mapsto |p|$ har ovennævnte egenskab. For $R = L[X]$, hvor L er et legeme, følger det af Divisionssætningen for polynomier, at funktionen $\nu : p \mapsto \deg(p)$ [hvor nul-polynomiet tillægges graden -1] har ovennævnte egenskab.

1.5. DEN OPSTIGENDE KÆDES EGENSKAB. Lad R være en hovedidealring. I enhver voksende følge af idealer

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$$

gælder da "$=$" fra et vist trin [dvs der findes et $N \in \mathbb{N}$

så at $\mathfrak{a}_N = \mathfrak{a}_{N+1} = \cdots$].

BEVIS. Foreningsmængden $\mathfrak{a} := \bigcup_{n\in\mathbb{N}} \mathfrak{a}_n$ er et ideal ifølge Sætning 1.3. Da R er en hovedidealring, har vi $\mathfrak{a} = Ra$, med et $a \in R$. Da $a \in Ra = \mathfrak{a} = \bigcup_{n\in\mathbb{N}} \mathfrak{a}_n$ findes et $N \in \mathbb{N}$ således at $a \in \mathfrak{a}_N$. Men så vil $Ra \subseteq \mathfrak{a}_N$, og af

$$Ra \subseteq \mathfrak{a}_N \subseteq \mathfrak{a}_{N+1} \subseteq \cdots \subseteq \bigcup_{n\in\mathbb{N}} \mathfrak{a}_n = Ra$$

følger $\mathfrak{a}_N = \mathfrak{a}_{N+1} = \cdots$ ▨

2. Primideal og maksimalideal.

2.1. Der er som bekendt en bijektiv forbindelse mellem idealer i ringen R og kongruensrelationer i R. Den til idealet $\mathfrak{a} \subseteq R$ hørende kongruensrelation $\underset{\mathfrak{a}}{\equiv}$ er bestemt ved

$$x' \underset{\mathfrak{a}}{\equiv} x \overset{\text{DEF}}{\iff} x' - x \in \mathfrak{a}.$$

Den tilhørende kvotientring $R/\mathfrak{a}$ består af ækvivalensklasserne, og den kanoniske afbildning $: x \mapsto \overline{x}$, der afbilder et element $x \in R$ over i den ækvivalensklasse, der indeholder x, er en surjektiv ringhomomorfi:

$$R \longrightarrow R/\mathfrak{a}.$$

2.2. DEFINITION. Et ideal $\mathfrak{p}$ i R kaldes et <u>primideal</u>, hvis $\mathfrak{p} \subset R$, og hvis der for alle $x, y \in R$ gælder:

$$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \vee y \in \mathfrak{p}.$$

2.3. BEMÆRKNING. Ifølge definitionen er det trivielle ideal R <u>ikke</u> et primideal i R. Det trivielle ideal (0) kan derimod godt være et primideal, idet der øjensynlig gælder:

Idealet (0) er et primideal i R, hvis og kun hvis R er et integritetsområde.

Mere generelt gælder følgende:

KARAKTERISERING AF PRIMIDEALER.

SÆTNING. Et ideal $\mathfrak{p}$ i R er et primideal, hvis og kun hvis kvotientringen $R/\mathfrak{p}$ er et integritetsområde.

BEVIS. "<u>hvis</u>": Da et integritetsområde ikke er nulringen, har vi $R/\mathfrak{p} \neq 0$, og altså $\mathfrak{p} \subset R$. Antag, at $xy \in \mathfrak{p}$, og at $x \notin \mathfrak{p}$. Da er $xy \equiv 0$ og $x \not\equiv 0$, og i $R/\mathfrak{p}$ har vi derfor:

$$\overline{x}\,\overline{y} = \overline{xy} = \overline{0} \quad \text{og} \quad \overline{x} \neq \overline{0}.$$

Da nul-reglen gælder i $R/\mathfrak{p}$, må vi have $\overline{y} = \overline{0}$, altså $y \in \mathfrak{p}$.

"kun hvis": Da $\mathfrak{p} \subset R$, er $R/\mathfrak{p} \neq 0$, så vi skal blot vise, at nul-reglen gælder i $R/\mathfrak{p}$. Lad altså X, Y være elementer i $R/\mathfrak{p}$ så at

$$XY = \overline{0} \quad \text{og} \quad X \neq \overline{0}.$$

Vælges repræsentanter: $X = \overline{x}$, $Y = \overline{y}$, har vi $\overline{xy} = \overline{x}\,\overline{y} = XY = \overline{0}$, altså $xy \in \mathfrak{p}$, og $\overline{x} = X \neq \overline{0}$, altså $x \notin \mathfrak{p}$. Heraf følger $y \in \mathfrak{p}$, og dermed $Y = \overline{y} = \overline{0}$ ▨

KOROLLAR. Lad $\varphi: R \to R'$ være en ringhomomorfi. Hvis R' er et integritetsområde, så er φ's kerne et primideal.

BEVIS. Lad $\mathfrak{p} := \varphi^{-1}(0)$ være kernen for φ. Ifølge Isomorfisætningen for ringe har vi en isomorfi:

$$R/\mathfrak{p} \xrightarrow{\sim} \varphi(R)$$

Her er billedringen $\varphi(R) \subseteq R'$ en delring af et integritetsområde og dermed selv et integritetsområde. Det følger, at $R/\mathfrak{p}$ er et integritetsområde, og $\mathfrak{p}$ er derfor et primideal. ▨

2.4. Mængden af idealer i R udgør, med inklusion $\subseteq$ som ordning, en (partielt) ordnet mængde.

DEFINITION. Et ideal $\mathfrak{M}$ i R kaldes et <u>maksimalideal</u>, hvis det er maksimalt blandt idealerne $\subset R$.

Idealet $\mathfrak{M}$ er således et maksimalideal, hvis $\mathfrak{M} \subset R$, og hvis der for alle idealer $\mathfrak{a} \subseteq R$ gælder:

$$\mathfrak{M} \subseteq \mathfrak{a} \subset R \Rightarrow \mathfrak{M} = \mathfrak{a}.$$

OBSERVATION. Betingelsen kan udtrykkes således: Af idealer $\mathfrak{a}$ i R, som opfylder

$$\mathfrak{M} \subseteq \mathfrak{a} \subseteq R$$

findes der præcis 2, nemlig $\mathfrak{a} = \mathfrak{M}$ og $\mathfrak{a} = R$.

2.5. BEMÆRKNING. Ifølge definitionen er det trivielle ideal R ikke et maksimalideal. Det trivielle ideal (0) kan derimod godt være et maksimalideal, idet vi ifølge Observationen ovenfor har:
Idealet (0) er et maksimalideal, hvis og kun hvis R har præcis 2 idealer. Denne egenskab karakteriserer legemerne, idet der mere generelt gælder følgende:

KARAKTERISERING AF MAKSIMALIDEALER.
SÆTNING. Et ideal $\mathfrak{m}$ i R er et maksimalideal, hvis og kun hvis kvotientringen $R/\mathfrak{m}$ er et legeme.
BEVIS. "hvis": Da et legeme ikke er nulringen, har vi $R/\mathfrak{m} \neq 0$, og altså $\mathfrak{m} \subset R$. Antag nu, at

$$\mathfrak{m} \subseteq \mathfrak{o} \subseteq R \quad \text{og at} \quad \mathfrak{m} \subset \mathfrak{o}.$$

Vi skal da vise, at $\mathfrak{o} = R$. Vælg et element $a \in \mathfrak{o} \setminus \mathfrak{m}$. Da er $a \neq 0$ modulo $\mathfrak{m}$, og i $R/\mathfrak{m}$ har vi derfor $\textcircled{a} \neq \textcircled{0}$. Da $R/\mathfrak{m}$ er et legeme, er $\textcircled{a}$ derfor invertibel, så der findes et element $X \in R/\mathfrak{m}$, med $X\textcircled{a} = \textcircled{1}$. Vælges en repræsentant: $X = \textcircled{x}$, har vi altså

$$\textcircled{1} = X\textcircled{a} = \textcircled{x}\textcircled{a} = \textcircled{xa}.$$

Følgelig er $1 \equiv xa$, så vi kan skrive

$$1 = xa + m, \quad \text{hvor } m \in \mathfrak{m}.$$

Da $a \in \mathfrak{o}$, og $m \in \mathfrak{m} \subseteq \mathfrak{o}$, slutter vi, at også $1 \in \mathfrak{o}$, men så er for et vilkårligt element $r \in R$ også

$$r = r1 \in \mathfrak{o},$$

og altså $\mathfrak{o} = R$.
"kun hvis": Da $\mathfrak{m} \subset R$, er $R/\mathfrak{m} \neq 0$, så vi skal blot vise, at hvert element $A \neq \textcircled{0}$ i $R/\mathfrak{m}$ er invertibelt. Vælg en repræsentant: $A = \textcircled{a}$. Da $\textcircled{a} = A \neq \textcircled{0}$, er $a \notin \mathfrak{m}$. Dit følger for idealet $\mathfrak{m} + Ra$, at vi har

$$\mathfrak{m} \subset Ra + \mathfrak{m}$$

og heraf følger, at $Ra + \mathfrak{m} = R$. Specielt er $1 \in Ra + \mathfrak{m}$, dvs af formen

$$1 = xa + m, \quad m \in \mathfrak{m}.$$

Nu finder vi

$$\textcircled{1} = \textcircled{xa} = \textcircled{x}\textcircled{a} = \textcircled{x} A,$$

og A er derfor invertibelt (med $\textcircled{x}$ som invers) ▨

2.6. SÆTNING. Ethvert maksimalideal er et primideal.
BEVIS. Da et legeme er et integritetsområde fås dette umiddelbart af karakteriseringerne i Sætningerne 2.3 og 2.5 ▨

2.7. SÆTNING. For et primtal p er restklasseringen $\mathbb{Z}/\mathbb{Z}p$ et legeme.
BEVIS. Ifølge Sætning 2.5 skal vi vise, at idealet $\mathbb{Z}p$ i $\mathbb{Z}$ er et maksimalideal. Det er klart, at $\mathbb{Z}p \subset \mathbb{Z}$. Lad derfor $\mathfrak{a} \subseteq \mathbb{Z}$ være et ideal, således at

$$\mathbb{Z}p \subseteq \mathfrak{a} \subseteq \mathbb{Z}.$$

Ifølge Hovedidealsætningen har idealet $\mathfrak{a}$ formen

$$\mathfrak{a} = \mathbb{Z}d,$$

og vi kan antage $d \geq 0$. Af $p \in \mathbb{Z}p \subseteq \mathbb{Z}d$ følger, at d er divisor i p, og så er enten $d = p$, og altså $\mathfrak{a} = \mathbb{Z}d = \mathbb{Z}p$, eller $d = 1$, og altså $\mathfrak{a} = \mathbb{Z}d = \mathbb{Z}1 = \mathbb{Z}$ ▨

2.8. BEMÆRKNING. V. hj. a. Zorn's lemma kan man vise, at der til hvert ideal $\mathfrak{a} \subset R$ findes et maksimalideal $\mathfrak{m} \supseteq \mathfrak{a}$. Er R en hovedidealring, kan det bevises således: Enten er $\mathfrak{a}$ selv et maksimalideal (og så er vi færdige), eller også er $\mathfrak{a}$ ikke et maksimalideal, og så findes et ideal $\mathfrak{a}_1$ med $\mathfrak{a} \subset \mathfrak{a}_1$, $\mathfrak{a}_1 \subset R$. Her er enten $\mathfrak{a}_1$ et maksimalideal (og så er vi færdige), eller $\mathfrak{a}_1$ er ikke et maksimalideal, og så findes et ideal $\mathfrak{a}_2$ med $\mathfrak{a}_1 \subset \mathfrak{a}_2$, $\mathfrak{a}_2 \subset R$. Her er enten ...
... Af Den opstigende kædes egenskab 1.5 følger, at dette kun kan fortsætte et endeligt antal skridt. Og når det stopper, er vi nået til et maksimalideal.

3. Faktorielle ringe.

Vi vil her forudsætte, at den kommutative ring R er et integritetsområde. Af en ligning $rx = ry$, hvor $r \neq 0$, følger altså, at $x = y$.

3.1. DEFINITIONER. Et element $u \in R$ kaldes en enhed, hvis det er invertibelt.

Et element $a \in R$ kaldes associeret med et element $b \in R$, hvis der findes en enhed $u \in R^*$, så at $a = ub$.

Et element $d \in R$ siges at være divisor i elementet $a \in R$, eller at gå op i a, hvis der findes et element $r \in R$, så at $rd = a$. I så fald skrives

$$d \mid a,$$

og a kaldes et multiplum af d. Bemærk, at $d \mid a \Leftrightarrow a \in Rd$.

De trivielle divisorer i et element a er enhederne og elementerne, der er associerede med a.

Et element $q \in R$ kaldes irreducibelt, hvis $q \neq \{^0_{\text{enhed}}$, og q kun har trivielle divisorer.

Et element $p \in R$ kaldes et primelement, hvis $p \neq \{^0_{\text{enhed}}$, og hvis der for alle $x, y \in R$ gælder

$$p \mid xy \Rightarrow p \mid x \vee p \mid y.$$

3.2. OBSERVATION. Et element $p \neq \{^0_{\text{enhed}}$ er irreducibelt, hvis og kun hvis der af en ligning $p = d_1 d_2$ følger, at d_1 eller d_2 er en enhed.

SÆTNING. Ethvert primelement $p \in R$ er irreducibelt.

BEVIS. Antag, at $p = d_1 d_2$. Vi skal vise, at d_1 eller d_2 er en enhed. Vi har specielt $p \mid d_1 d_2$, så p går op i en af faktorerne, f.eks. i d_2. Vi kan altså skrive $up = d_2$ med $u \in R$, og så får vi $p = d_1 d_2 = d_1 up$. Da $p \neq 0$, får vi $1 = d_1 u$, og d_1 er således en enhed (med $d_1^{-1} = u$) ▨

KARAKTERISERING VED HOVEDIDEALER.

3.3. SÆTNING. *I et integritetsområde R afspejler de indførte begreber sig i relationer mellem hovedidealer, idet der gælder:*

(1) u er en enhed $\Leftrightarrow$ $(u) = R$ $(= (1))$.

(2) a er associeret med b $\Leftrightarrow$ $(a) = (b)$

(3) d er divisor i a $\Leftrightarrow$ $(a) \subseteq (d)$

(4) d er triviel divisor i a $\Leftrightarrow$ $(d) = R$ $\vee$ $(d) = (a)$.

(5) q er irreducibelt $\Leftrightarrow$ $q \neq 0$ og (q) er maksimalt blandt hovedidealer $\subset R$.

(6) p er et primelement $\Leftrightarrow$ $p \neq 0$ og (p) er et primideal.

BEVIS. (1): Hvis u er en enhed, findes $v \in R$ med $vu = 1$, og så gælder for hvert $r \in R$, at $r = r1 = (rv)u \in (u)$. Er omvendt $(u) = R$, så er specielt $1 \in (u)$, og altså $1 = vu$, med $v \in R$.

(2): Hvis a er associeret med b, altså $a = ub$, hvor $u \in R^*$, så er $ra = rub \in (b)$, og altså $(a) \subseteq (b)$, og da vi også har $b = va$ (med $v = u^{-1}$), får vi tilsvarende $(b) \subseteq (a)$. Er omvendt $(a) = (b)$, så har vi $a \in (a) = (b)$, altså $a \in (b)$, og tilsvarende $b \in (a)$, og kan skrive

$$a = ub, \quad b = va, \quad u, v \in R.$$

Hvis $b = 0$, får vi straks $a = 0$. Hvis $b \neq 0$, følger det af $b = va = vub$, at $1 = vu$. Elementet u er derfor en enhed, og a er følgelig associeret med b.

(3): Vi har: $d/a \Leftrightarrow a \in (d) \Leftrightarrow (a) \subseteq (d)$.

(4): Følger umiddelbart af (1) og (2).

(5): Ifølge (3) og (4) svarer divisorerne d i q netop til de hovedidealer (d), som opfylder

$$(q) \subseteq (d) \subseteq R,$$

og d er triviel, hvis og kun hvis der her gælder et af de to mulige "$=$" (altså $(q) = (d)$ eller $(d) = R$). Heraf følger påstanden umiddelbart.

(6): Idet $p/xy \Leftrightarrow xy \in (p)$, $p/x \Leftrightarrow x \in (p)$ og $p/y \Leftrightarrow y \in (p)$, fås påstanden direkte ud fra definitionen på et primideal ▨

3.4. SÆTNING. Lad R være et hovedidealområde. Da er et element $p \in R$ irreducibelt, hvis og kun hvis det er et et primelement. Hovedidealet (p) frembragt af et sådant element er et maximalideal i R.

BEVIS. "hvis": gælder i ethvert integritetsområde (Sætning 3.2.).

"kun hvis": Lad $p \in R$ være irreducibelt. Ifølge Sætning 3.3(5) er idealet (p) maksimalt blandt hovedidealer $\subset R$. Da alle idealer i R er hovedidealer, betyder det, at (p) er et maksimalideal i R. Heraf følger, at (p) er et primideal (Sætning 2.6). Da $p \neq 0$ slutter vi heraf (Sætning 3.3(6)), at p er et primelement.

Den sidste påstand så vi undervejs. ▨

3.5. DEFINITION. Er der i R givet elementer $a, d_1, \cdots, d_s$ så at $a = d_1 \cdots d_s$, siger vi kort, at $a = d_1 \cdots d_s$ er en opløsning af a i faktorerne $d_1, \cdots, d_s$. Opløsningen kaldes irreducibel, hvis faktorerne er irreducible, og en primopløsning, hvis faktorerne er primelementer.

BEMÆRKNING. Ethvert element $a \in R$ har triviele opløsninger af formen $a = u(u^{-1}a)$, hvor den ene faktor u er en enhed (og den anden er associeret med a). Ifølge Observation 3.2 har et irreducibelt element kun sådanne triviele opløsninger. I en irreducibel opløsning $a = q_1 \cdots q_s$ kan faktorerne q_i altså kun trivielt opløses yderligere.

3.6. SÆTNING. Primopløsninger er entydige i følgende forstand: Er $p_1, \cdots, p_s, q_1, \cdots, q_t$ primelementer i R, og er $p_1 \cdots p_s$ associeret med $q_1 \cdots q_t$, så er $s = t$, og der gælder (eventuelt efter en passende permutation af q_i'erne), at p_i er associeret med q_i, $i = 1, \cdots, s$.

BEVIS. Der findes en enhed $u \in R$, så at

$$u p_1 \cdots p_s = q_1 \cdots q_t.$$

Da primelementet p_s således går op i produktet $q_1 \cdots q_t$, må

det gå op i et af q_i'erne. Vi kan antage, at p_s går op i q_t. Da q_t er irreducibel (Sætning 3.2), må p_s enten 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 $p_s = v q_t$, med en enhed $v \in R$, og får ved indsættelse:

$$uv\, p_1 \cdots p_{s-1}\, q_t = q_1 \cdots q_{t-1}\, q_t .$$

Da $q_t \neq 0$ følger heraf, at

$$(uv)\, p_1 \cdots p_{s-1} = q_1 \cdots q_{t-1},$$

og $p_1 \cdots p_{s-1}$ er derfor associeret med $q_1 \cdots q_{t-1}$.
Ved at fortsætte således fås det ønskede ▨

3.7. DEFINITION. Integritetsområdet R kaldes en <u>faktoriel ring</u>, hvis ethvert element $a \neq \{^{0}_{\text{enhed}}$ i R kan skrives som et produkt $a = p_1 \cdots p_s$ af primelementer $p_1, \cdots, p_s$.

I en faktoriel ring R har altså ethvert element $a \neq \{^{0}_{\text{enhed}}$ en primoplösning $a = p_1 \cdots p_s$, og af sætningen ovenfor fremgår, at disse oplösninger (bortset fra "permutation og association") er entydige.

SÆTNING. For et integritetsområde R er følgende betingelser ækvivalente:
(i) R er en faktoriel ring.

(ii) $\begin{cases} \text{(a) Hvert element } a \neq \{^{0}_{\text{enhed}} \text{ har en irreducibel oplösning,} \\ \text{og} \\ \text{(b) Hvert irreducibelt element i } R \text{ er et primelement.} \end{cases}$

(iii) $\begin{cases} \text{(a) Hvert element } a \neq \{^{0}_{\text{enhed}} \text{ har en irreducibel oplösning,} \\ \text{og} \\ \text{(c) Irreducible oplösninger er entydige.} \end{cases}$

BEMÆRKNING. Med den i (c) nævnte entydighed menes: Hvis $p_1, \cdots, p_s$ $q_1, \cdots, q_t$ er irreducible elementer i R, således at $p_1 \cdots p_s = q_1 \cdots q_t$, så er $s = t$ og (bortset fra "permutation og association") $p_i = q_i$, $i = 1, \cdots, s$.
BEVIS FOR SÆTNINGEN. Det er klart, at (a) $\wedge$ (b) $\Rightarrow$ (i). Af Sætning 3.2 følger (i) $\Rightarrow$ (a), og af Sætning 3.6 fås (b) $\Rightarrow$ (c). Det er derfor nok at vise, at (i) $\Rightarrow$ (b) og at (a) $\wedge$ (c) $\Rightarrow$ (b).

(i) ⇒ (b): Lad q være et irreducibelt element, og betragt en primoplösning af q. Da q er irreducibelt, har det kun trivielle oplösninger. Primoplösningen har derfor kun én faktor, og q er derfor et primelement.

(a) ∧ (c) ⇒ (b) Lad q være et irreducibelt element, og antag, at q/xy. Vi skal vise, at q/x eller q/y. Det er oplagt, hvis x eller y er $=0$ eller en enhed. I modsat fald skriver vi

$$rq = xy, \qquad r \in R,$$

og her er $r \neq 0$. Ifölge (a) kan vi finde irreducible oplösninger $x = x_1 \cdots x_s$, $y = y_1 \cdots y_t$, $r = r_1 \cdots r_n$ [i det mindste, hvis $r \neq$ enhed. Overvej selv hvorledes det följende skal modificeres, hvis r er en enhed!]. Indsættes, fås:

$$r_1 \cdots r_n q = x_1 \cdots x_s y_1 \cdots y_t$$

Ifölge (c) må den irreducible faktor q på venstre side også forekomme (på nær association) på höjre side. Vi kan antage, at q er associeret med x_1. Men så er q specielt divisor i x_1, og dermed også divisor i $x = x_1(x_2 \cdots x_s)$ □

3.8. LEMMA. Lad R være et integritetsområde, hvori der findes et element $a \neq \{^{0}_{\text{enhed}}$, der ikke kan skrives som et produkt af irreducible elementer. Da findes i R en uendelig følge af elementer

$$(a =)\ a_0, a_1, a_2, \cdots,$$

således at a_i er en ikke-triviel divisor i a_{i-1}, $i = 1, 2, \cdots$

BEVIS. Ifölge forudsætningen findes i R et element a, der har följende egenskab:

(*) $a \neq 0$, $a \neq$ enhed, a kan ikke skrives som produkt af irreducible elementer.

Et sådant element kan specielt ikke selv være irreducibelt, så det kan skrives

$$a = a'a'',$$

hvor a' og a'' er ikke-trivielle divisorer i a.

Specielt er begge divisorer ≠ enhed, og da $a'a'' = a \neq 0$

er begge divisorer $\neq 0$. Hvis både a' og a'' var et produkt af irreducible elementer, ville vi ved indsættelse i $a = a'a''$ se, at a var et produkt af irreducible elementer i modstrid med antagelsen. Følgelig vil mindst en af de to divisorer opfylde, at den ikke kan skrives som et produkt af irreducible, og denne divisor vil altså opfylde egenskaben (*).
Vi har vist, at hvert element med egenskaben (*) har en ikke-triviel divisor med egenskaben (*).
Startende med $a_0 = a$ kan vi derfor finde en følge som ønsket (endda således at hvert a_i har egenskaben (*)) ▨

KOROLLAR 1. Antag, at der i integritetsområdet R er givet en funktion $\nu : R \to \mathbb{Z}$, som er nedad begrænset og har følgende egenskab: For hvert $a \neq 0$ i R og hver ikke-triviel divisor a_1 i a gælder

$$\nu(a_1) < \nu(a).$$

Da har hvert element $a \neq \{^{0}_{\text{enhed}}$ en irreducibel opløsning.
BEVIS. I modsat fald ville der findes en uendelig følge $a_0, a_1, a_2, \ldots$ som angivet i Lemma'et, og så ville

$$\nu(a_1) > \nu(a_2) > \cdots$$

være i modstrid med at $\nu : R \to \mathbb{Z}$ var nedad begrænset. ▨

KOROLLAR 2. Lad R være et hovedidealområde. Da har hvert element $a \neq \{^{0}_{\text{enhed}}$ en irreducibel opløsning.
BEVIS. I modsat fald ville der findes en uendelig følge $a_0, a_1, a_2, \ldots$ som angivet i Lemmaet, og så ville

$$(a_0) \subset (a_1) \subset (a_2) \subset \cdots$$

være i modstrid med Den opstigende kædes egenskab 1.5. ▨

3.9. Vi samler nu resultaterne om hovedidealområder i følgende:

HOVEDSÆTNING. Lad R være et hovedidealområde. Da er R en faktoriel ring. Primidealerne $\neq (0)$ i R er netop idealerne af formen (p), hvor p er irreducibel, og disse idealer er maksimalidealer.

BEVIS. R er en faktoriel ring ifølge Sætning 3.7, thi betingelsen (ii,a) følger af Korollar 3.8.2 ovenfor, og betingelsen (ii,b) er indeholdt i Sætning 3.4. Af Sætning 3.4 følger videre, at idealer af formen (p), hvor p er irreducibelt, er maksimalidealer, og er omvendt $\mathfrak{p} \neq (0)$ et primideal, så er $\mathfrak{p}$ et hovedideal $\mathfrak{p} = (p)$ (da R var en hovedidealring), og p er et primelement, og dermed irreducibelt ▨

3.10. ANVENDELSE PÅ $\mathbb{Z}$. De hele tals ring $\mathbb{Z}$ er en faktoriel ring. I $\mathbb{Z}$ er enhederne ± 1. Ethvert helt tal $\neq 0$ er således associeret med netop et positivt tal. De positive irreducible elementer er netop primtallene. Primidealerne $\neq (0)$ i $\mathbb{Z}$ er altså idealerne af formen $(p) = \mathbb{Z}p$, hvor p er et primtal, og disse idealer er maksimalidealer (og kvotienten $\mathbb{F}_p := \mathbb{Z}/\mathbb{Z}p$ er altså et legeme). Videre er $(0) \subset \mathbb{Z}$ et primideal, der ikke er et maksimalideal.

3.11. ANVENDELSE PÅ $L[X]$. Enhver polynomiumsring $L[X]$, hvor L er et legeme, er en faktoriel ring. I $L[X]$ er enhederne konstanterne $\neq 0$. Ethvert polynomium $\neq 0$ er således associeret med med netop ét normeret polynomium.

For et normeret irreducibelt polynomium

$$p = X^n + p_{n-1}X^{n-1} + \cdots + p_1 X + p_0 \in L[X],$$

er kvotienten $K := L[X]/(p)$ altså et legeme. Ifølge Struktursætningen for polynomiumskvotienter indeholder dit således konstruerede legeme K det givne legeme L som dellegeme, og sætter vi $\xi := \otimes \in K$, kan hvert element i K entydigt skrives

$$r_0 + r_1\xi + \cdots + r_{n-1}\xi^{n-1}, \quad r_0, r_1, \ldots, r_{n-1} \in L.$$

Endvidere er $\xi^n = -p_0 - p_1\xi - \cdots - p_{n-1}\xi^{n-1}$.

EKSEMPEL. Polynomiet $X^2+1 \in \mathbb{R}[X]$ er irreducibelt, thi ellers var det et produkt af to 1$^{\text{ste}}$-gradspolynomier i $\mathbb{R}[X]$, og så ville det have en rod i $\mathbb{R}$. Det følger, at vi kunne

DEFINERE de komplexe tals legeme $\mathbb{C}$ som legemet

$$\mathbb{C} := \mathbb{R}[X]/(X^2+1),$$

thi dette legeme indeholder $\mathbb{R}$, og sætter vi $i := \overline{X} \in \mathbb{C}$, kan hvert element i $\mathbb{C}$ entydigt skrives

$$r_0 + r_1 i \quad , \quad r_0, r_1 \in \mathbb{R}.$$

Da vi endvidere har $i^2 = -1$, harmonerer dette med den sædvanlige definition af $\mathbb{C}$.

BEMÆRKNING. Spørgsmålet om hvilke polynomier i $L[X]$, der er irreducible, afhænger i høj grad af hvilket legeme L, der betragtes. I almindelighed er alle 1$^{\text{ste}}$-grads polynomier irreducible, og 2$^{\text{den}}$- og 3$^{\text{die}}$-grads polynomier er irreducible netop når de ikke har rødder i L.

Algebraens fundamentalsætning udsiger, at i $\mathbb{C}[X]$ er de irreducible polynomier netop 1$^{\text{ste}}$-gradspolynomierne. Heraf følger let, at i $\mathbb{R}[X]$ er de irreducible polynomier netop 1$^{\text{ste}}$-gradspolynomierne og de 2$^{\text{den}}$-gradspolynomier, der ikke har reelle rødder.

Man kan vise, at polynomierne $X^n - 2$, $n = 1, 2, 3, \ldots$ er irreducible polynomier i $\mathbb{Q}[X]$. I $\mathbb{Q}[X]$ findes altså irreducible polynomier af enhver grad ≥ 1.

3.12. I en faktoriel ring R tænkes ofte valgt et <u>repræsentantsystem</u> $\mathcal{P}$ 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 kan primelementerne q i R altså entydigt

skrives

$$q = up, \qquad u \in R^*, \ p \in \mathcal{P}.$$

Indsætter vi i en primopløsning

$$a = q_1 \cdots q_n$$

for de enkelte faktorer $q_i = u_i p_i$, $u_i \in R^*$, $p_i \in \mathcal{P}$, får vi en opløsning af formen

$$a = u p_1^{\nu_1} \cdots p_k^{\nu_k},$$

hvor $u \in R^*$, $p_1, \dots, p_k \in \mathcal{P}$ er indbyrdes forskellige, og $\nu_1, \dots, \nu_k \in \mathbb{N}$. Idet vi om fornødent tilføjer potenser med eksponent 0, kan opløsningen skrives

$$a = u \prod_{p \in \mathcal{P}} p^{\nu_p},$$

hvor kun endelig mange eksponenter er > 0. Denne fremstilling, som vi ofte også kalder <u>primopløsningen af a</u> er entydig i den forstand, at enheden u og eksponenterne $\nu_p \geq 0$, $p \in \mathcal{P}$, er entydigt bestemte ved a. Det ses, at også enhederne i R har en sådan opløsning, nemlig med alle $\nu_p = 0$, $p \in \mathcal{P}$.

Af entydigheden følger, at hvis et element $b \in R \setminus \{0\}$ har primopløsningen

$$b = w \prod_{p \in \mathcal{P}} p^{\mu_p},$$

så er b divisor i a, netop når $\mu_p \leq \nu_p$ for alle $p \in \mathcal{P}$.

Specielt ses, at "på nær associering" er <u>antallet</u> af divisorer i et element $a \neq 0$ med primopløsningen

$$a = u \cdot \prod_{p \in \mathcal{P}} p^{\nu_p}$$

bestemt som tallet

$$\prod_{p \in \mathcal{P}} (\nu_p + 1),$$

idet jo $\nu_p + 1$ er antallet af eksponenter μ_p med $0 \leq \mu_p \leq \nu_p$.

4. Største fælles divisor.

4.1. DEFINITION. Lad a, b være elementer i et integritetsområde R. Et element $c \in R$, som er divisor i a og i b, kaldes en <u>fælles divisor for a og b</u>, og c kaldes en <u>største fælles divisor for a og b</u>, hvis c er en fællesdivisor for a og b, og hvis der for enhver fælles divisor d for a og b gælder, at d er divisor i c.
At a og b kun har enhederne som fælles divisorer betyder således at $c = 1$ er en største fælles divisor for a og b. Er dette tilfældet siges <u>a og b at være primiske</u>

Tilsvarende defineres største fælles divisor for endelig mange elementer $a_1, \cdots, a_n \in R$, og vi siger, at <u>$a_1, \cdots, a_n$ er primiske</u>, hvis de har 1 som største fælles divisor.

BEMÆRKNING. At $a_1, \cdots, a_n \in R$ er primiske, er svagere end at elementerne er parvis primiske. F.eks. er tallene $6, 10, 15 \in \mathbb{Z}$ primiske, men (slet) ikke parvis primiske.

OBSERVATION. Betingelsen for at et element $c \in R$ er største fælles divisor for a og b kan skrives på en af følgende ækvivalente måder:

(i) $\forall d \in R : d \mid a \wedge d \mid b \Leftrightarrow d \mid c$

(ii) $\forall d \in R : a \in (d) \wedge b \in (d) \Leftrightarrow (c) \subseteq (d)$

(iii) $\forall d \in R : (a, b) \subseteq (d) \Leftrightarrow (c) \subseteq (d)$

(iv) $\bigcap \{(d) \mid (a,b) \subseteq (d)\} = (c)$,

hvor der for (ii) $\Leftrightarrow$ (iii) udnyttes, at et ideal indeholder både a og b, netop når det indeholder idealet $(a, b) = Ra + Rb$ frembragt af a og b.

4.2. SÆTNING. Elementer a, b i et integritetsområde R har en største fælles divisor, hvis og kun hvis fællesmængden

$$\bigcap \{ (d) \mid (a,b) \subseteq (d) \}$$

er et hovedideal. I bekræftende fald er de største fælles divisorer for a og b netop frembringerne for dette hovedideal.

BEVIS. Følger umiddelbart af Observation (iv) ovenfor ▨

4.3. SÆTNING. Hvis R er et hovedidealområde, så har elementer $a, b \in R$ altid en største fælles divisor. De største fælles divisorer for a og b er netop frembringerne for (hoved-)idealet $(a,b) = Ra + Rb$. Elementerne a og b er primiske, hvis og kun hvis der findes elementer $x, y \in R$, så at $xa + yb = 1$.

BEVIS. I et hovedidealområde er idealet (a,b) selv et hovedideal. De første påstande følger derfor umiddelbart af Sætning 4.2. Endvidere har vi $(a,b) = (1) = R$, netop når $1 \in (a,b)$, og det er jo den sidste påstand ▨

BEMÆRKNING. Tilsvarende ses i et hovedidealområde R, at de største fælles divisorer for elementer $a_1, \dots, a_n$ netop er frembringerne for (hoved-)idealet $(a_1, \dots, a_n)$, og at $a_1, \dots, a_n$ er primiske, hvis og kun hvis der findes elementer $x_1, \dots, x_n \in R$, så at $x_1 a_1 + \dots + x_n a_n = 1$.

NOTATION. I et hovedidealområde skrives ofte "$(a,b) = c$" i betydningen: "c er en største fælles divisor for a og b". Skrivemåden "$(a,b) = 1$" udtrykker altså, at a og b er primiske.

4.4. Vi har tidligere set, at hvis der i et integritets-

område R er givet en funktion $\nu: R \to \mathbb{Z}$, som er nedad begrænset og har følgende egenskab: For hvert $d \neq 0$ i R og hvert $a \in R$ findes et $q \in R$, så at

$$\nu(a - qd) < \nu(d),$$

så er R et hovedidealområde (Sætning 1.4.). Specielt har altså i en sådan ring to elementer a og b altid en største fælles divisor. En sådan kan bestemmes under brug af:

EUKLIDS ALGORITME. Sæt $d_0 = a$, $d_1 = b$, og antag, at $\nu(d_0) \geq \nu(d_1)$. Hvis $d_1 \neq 0$, bestemmes $q_1 \in R$, så at

$$\nu(d_0 - q_1 d_1) < \nu(d_1).$$

Hvis $d_2 := d_0 - q_1 d_1 \neq 0$, bestemmes $q_2 \in R$, så at

$$\nu(d_1 - q_2 d_2) < \nu(d_2)$$

Hvis $d_3 := d_1 - q_2 d_2 \neq 0$, bestemmes $q_3 \in R$, så at

$$\nu(d_2 - q_3 d_3) < \nu(d_3),$$

o.s.v. Denne proces vil stoppe efter endelig mange skridt, i den forstand, at der findes et $n \geq 1$, så at

$$d_{n-1} - q_n d_n = 0. \quad [\text{eventuelt: } d_1 = 0]$$

For dette n er d_n en største fælles divisor for $a = d_0$ og $b = d_1$.

BEVIS. Hvis processen ikke stoppede, ville vi få en uendelig følge $d_0, d_1, d_2, \cdots$, og

$$\nu(d_0) \geq \nu(d_1) > \nu(d_2) > \cdots$$

ville være i modstrid med at funktionen ν var nedad begrænset.

For elementer $x, y, q \in R$ har vi ögensynlig

$$(x, y) = (x - qy, y)$$

Det følger, at vi har

$$(a, b) = (d_0, d_1) = (d_0 - q_1 d_1, d_1) = (d_2, d_1) = (d_2, d_1 - q_2 d_2) =$$
$$= (d_2, d_3) = \cdots = (d_{n-1}, d_n) = (d_{n-1} - q_n d_n, d_n) =$$
$$= (0, d_n) = (d_n)$$

Idealet (a,b) er således (hoved-)idealet (d_n) ▨

4.5. I en faktoriel ring R kan spørgsmål om deliglighed afgøres ud fra primoplösninger. Vi får derfor umiddelbart følgende:

SÆTNING. Hvis R er en faktoriel ring, så har elementer $a, b \in R$ altid en største fælles divisor. Er der i R valgt et repræsentantsystem $\mathcal{P}$ for primelementerne, og er der givet primoplösninger

$$a = u p_1^{\nu_1} \cdots p_r^{\nu_r}, \qquad b = v p_1^{\mu_1} \cdots p_r^{\mu_r}, \quad u, v \in R^*, \ p_i \in \mathcal{P},$$

så er de største fælles divisorer netop elementerne associerede med

$$c = p_1^{\lambda_1} \cdots p_r^{\lambda_r},$$

hvor $\lambda_i = \min\{\nu_i, \mu_i\}$, $i = 1, \cdots, r$. ▨

4.6. LEMMA. Lad der i en faktoriel ring R være givet parvis primiske elementer $d_1, \cdots, d_n$, og sæt

$$a_i := d_1 \cdots d_{i-1} d_{i+1} \cdots d_n, \qquad i = 1, \cdots, n.$$

Da er elementerne $a_1, \cdots, a_n$ primiske.

BEVIS. I modsat fald findes et primelement p, der er divisor i alle a_i'erne. Da p går op i $a_1 = d_2 \cdots d_n$, vil p gå op i en af faktorerne, f.eks. i d_j. Da p også går op i $a_j = \prod_{i \neq j} d_i$, vil p gå op i et d_i, med $i \neq j$. Men så er p fælles divisor for d_j og d_i i modstrid med at d_j og d_i var primiske ▨

4.7. Da et hovedidealområde er en faktoriel ring, kan vi i et hovedidealområde kombinere Sætning 4.3 med ovenstående resultater. Som en anvendelse viser vi:

DEN KINESISKE RESTKLASSESÆTNING. Lad der i et hovedideal område R være givet parvis primiske ele-

mentin $d_1, \dots, d_n$, og sæt $d := d_1 \cdots d_n$. Den ved

$$x \longmapsto (\overline{x}_1, \dots, \overline{x}_n),$$

bestemte ringhomomorfi : $R \to R/(d_1) \times \cdots \times R/(d_n)$ er da surjektiv, og dens kerne er hovedidealet (d).

BEVIS. Sættes $a_i := d_1 \cdots d_{i-1} d_{i+1} \cdots d_n$, har vi

(1) $d = a_i d_i$, (2) $a_i \in (d_j)$, $j \neq i$, $i = 1, \dots, n$.

Ifølge Lemma 4.6 er $a_1, \dots, a_n$ primiske, og da R er et hovedidealområde, findes $r_1, \dots, r_n \in R$, så at

(3) $$r_1 a_1 + \cdots + r_n a_n = 1$$

<u>Kernen</u>: At x tilhører kernen, betyder, at $x \in (d_i)$, $i = 1, \dots, n$. Af (1) følger så, at $a_i x \in (d)$, $i = 1, \dots, n$, og så vil

$$x = (r_1 a_1 + \cdots + r_n a_n) x = r_1 a_1 x + \cdots + r_n a_n x \in (d).$$

Omvendt er det klart, at hvert element i (d) tilhører kernen.

<u>Surjektiviteten</u>: Ethvert element $y \in R/(d_1) \times \cdots \times R/(d_n)$ har formen $y = (\overline{y_1}_1, \dots, \overline{y_n}_n)$, hvor $y_1, \dots, y_n \in R$. Sæt

$$x = r_1 a_1 y_1 + \cdots + r_n a_n y_n \in R,$$

og slut v.hj.a. (2) og (3), at $x \equiv r_j a_j y_j \equiv y_j$ modulo (d_j), og altså at $(\overline{x}_1, \dots, \overline{x}_n) = y$ □

KOROLLAR. Homomorfien inducerer en isomorfi:

$$R/(d) \xrightarrow{\approx} R/(d_1) \times \cdots \times R/(d_n). \quad \square$$

4.8. BEMÆRKNING. For elementer a, b i et integritetsområde R defineres et <u>mindste fælles multiplum</u> ganske svarende til største fælles divisor.

5. Gauß' sætning.

5.1. Vi betragter ringen $R[X]$ af polynomier med koefficienter i ringen R. Enhederne i $R[X]$ er som bekendt de inverstible konstanter, d.v.s. enhederne i R. At et polynomium $A \in R[X]$ er deleligt med en konstant $d \in R$, betyder, at alle A's koefficienter er delelige med d. Hovedidealet $dR[X]$ frembragt af d i $R[X]$ består altså af de polynomier, hvis koefficienter alle tilhører hovedidealet $dR \subseteq R$.

SÆTNING. *Hvis p er et primelement i R, så er p ligeledes et primelement i $R[X]$.*

BEVIS. Den kanoniske homomorfi : $R \to R/pR$, der til et element $a \in R$ lader svare restklassen $\bar{a} \in R/pR$ kan udvides til en afbildning : $R[X] \to R/pR\,[X]$ betegnet $A \mapsto \bar{A}$, idet vi for et polynomium

$$A = a_0 + a_1X + \cdots + a_nX^n \in R[X]$$

sætter

$$\bar{A} = \bar{a}_0 + \bar{a}_1X + \cdots + \bar{a}_nX^n \in R/pR\,[X].$$

Det er klart, at $A \mapsto \bar{A}$ er en ringhomomorfi:

$$R[X] \longrightarrow R/pR\,[X],$$

hvis kerne er hovedidealet $pR[X]$.

Er p et primelement i R, altså pR et primideal i R, så er kvotienten R/pR et integritetsområde, og følgelig er også polynomiumsringen $R/pR\,[X]$ et integritetsområde. Homomorfiens kerne, altså $pR[X]$, er derfor et primideal i $R[X]$, men det betyder netop, at p er et primelement i $R[X]$. ▨

5.2 DEFINITION. *Et polynomium $A \in R[X]$ kaldes primitivt, hvis dets koefficienter er primiske i R.*

Dette betyder altså, at de eneste konstanter, der er divisorer i polynomiet A, er de trivielle, d.v.s. enhederne.

5.3. Gauß' LEMMA. *Lad R være en faktoriel ring. Hvis $A, B \in R[X]$ er primitive polynomier, så er også produktet AB et primitivt polynomium.*

BEVIS. At elementer i en faktoriel ring er primiske, er ensbetydende med at intet primelement er divisor i dem alle. Var AB ikke et primitivt polynomium, ville der i R findes et primelement p, som var divisor i AB. Da p også er et primelement i $R[X]$ (Sætning 5.1), kunne vi slutte, at p var divisor i A eller i B, i modstrid med at både A og B var primitive polynomier ▨

5.4. Udover integritetsområdet R betragter vi dets brøklegeme K og polynomiumsringen $K[X]$. Vi har da

$$\begin{array}{ccc} R & \subseteq & R[X] \\ \cap\!| & & \cap\!| \\ K & \subseteq & K[X] \end{array}$$

OBSERVATION. *Hvis R er faktoriel, så kan ethvert polynomium $\phi(X) \neq 0$ i $K[X]$ skrives*

$$\phi(X) = \frac{a}{s} F(X),$$

hvor $a, s \in R$ er primiske, og hvor $F(X)$ er et primitivt polynomium i $R[X]$.

Koefficienterne i $\phi(X)$ er jo endelig mange brøker. For disse kan vi finde en fælles nævner t (f.eks. produk-

tit af alle nævnerne), d.v.s. vi kan skrive

$$\phi(X) = \frac{a_0}{t} + \frac{a_1}{t}X + \cdots + \frac{a_m}{t}X^n = \frac{1}{t}(a_0 + a_1X + \cdots + a_mX^n),$$

hvor $a_0, \ldots, a_m \in R$. Er d en største fælles divisor for $a_0, \ldots, a_m$, kan vi skrive

$$a_0 + a_1X + \cdots + a_mX^n = d\,F(X),$$

hvor $F(X)$ er et primitivt polynomium. Vi får så

$$\phi(X) = \frac{d}{t}F(X),$$

og forkortes brøken $\frac{d}{t}$ med en største fælles divisor for d og t, får vi den ønskede fremstilling.

5.5. KOROLLAR TIL GAUSS' LEMMA. *Lad R være en faktoriel ring, lad $A(X) \in R[X]$ være et primitivt polynomium og lad $\phi(X) \in K[X]$ være et polynomium med koefficienter i brøklegemet K. Hvis $\phi(X)A(X) \in R[X]$, så vil $\phi(X) \in R[X]$.*

BEVIS. Vi skriver

$$\phi(X) = \frac{a}{s}F(X),$$

hvor $a, s \in R$ er primiske, og hvor $F(X) \in R[X]$ er et primitivt polynomium (jfr. 5.4), og vi viser, at elementet s må være en enhed i R.

Sætter vi $A(X)\phi(X) = G(X) \in R[X]$, har vi i $R[X]$:

$$a\,F(X)\,A(X) = s\,G(X).$$

Hvis s ikke er en enhed, findes i R et primelement p, som er divisor i s. Dette element p er ikke divisor i a (da a og s var primiske) og det er heller ikke divisor i $F(X)$ eller $A(X)$ (da disse polynomier er primitive). Da p er divisor i produktet $aF(X)A(X)$ er dette i modstrid med at p er

et primelement i $R[X]$ (Sætning 5.1) ▨
[Bemærk, at 5.5 egentlig kom ud som korollar til 5.1].

5.6. Er $A(X)$, $G(X)$ polynomier i $R[X]$ således at der i $K[X]$ gælder, at $A(X)$ er divisor i $G(X)$, kan vi i almindelighed ikke slutte, at $A(X)$ er divisor i $G(X)$ inden for $R[X]$. (Eks. $A(X) = 2X+2 \in \mathbb{Z}[X]$ er divisor i $G(X) = X^2-1 \in \mathbb{Z}[X]$ inden for $\mathbb{Q}[X]$, men ikke inden for $\mathbb{Z}[X]$).
Korollar 5.5 udsiger imidlertid for polynomier $A(X)$, $G(X)$ med koefficienter i en faktoriel ring R, at hvis $A(X)$ er divisor i $G(X)$ inden for $K[X]$, og $A(X)$ er et primitivt polynomium, så er $A(X)$ divisor i $G(X)$ inden for $R[X]$.

5.7. GAUSS' SÆTNING. Lad R være en faktoriel ring med brøklegemet K. Da er også polynomiumsringen $R[X]$ faktoriel, og primelementerne i $R[X]$ er dels de konstanter, der er primelementer i R, dels de polynomier, der er primitive i $R[X]$ og irreducible i $K[X]$.
Vi minder om, at ringen $K[X]$ er et hovedidealområde og dermed en faktoriel ring.
Bevis. ① Polynomier $P(X)$ i $R[X]$ af den angivne form er primelementer i $R[X]$. Er nemlig $P(X)$ en konstant, følger dette af Sætning 5.1 og er $\deg P \geqslant 1$ følger dette af Korollar 5.5. Er nemlig P inden for $R[X]$ divisor i et produkt AB, kan vi, da P er et primelement i $K[X]$, slutte, at P inden for $K[X]$ er divisor i en af faktorerne, og da P yderligere er

primitivt, kan vi slutte, at P endda inden for $R[X]$ er divisor i denne faktor.

② Hvert polynomium $A(X) \neq \{0\}$enhed i $R[X]$ har en opløsning i (prim-) faktorer af den angivne form. Er nemlig A en konstant, følger dette af at R er faktoriel, og er $\deg A \geqslant 1$, betragter vi først en primopløsning af $A(X)$ i $K[X]$:

$$A(X) = \Pi_1(X) \cdots \Pi_r(X).$$

Nu kan vi skrive $\Pi_i(X) = \alpha_i P_i(X)$, hvor $\alpha_i \in K^*$ og $P_i(X) \in R[X]$ er primitivt; da $\Pi_i(X)$ er irreducibel i $K[X]$, er også $P_i(X)$ irreducibel i $K[X]$, og altså af den angivne form, $i = 1, \cdots, r$. Sætter vi $\alpha = \alpha_1 \cdots \alpha_r \in K^*$, har vi

$$A(X) = \alpha P_1(X) \cdots P_r(X).$$

Her er produktet $P_1 \cdots P_r$ igen et primitivt polynomium (Gauß' lemma), og af Korollar 5.5 kan vi derfor slutte, at $\alpha \in R$. Idet vi nu primopløser α i R, får vi den søgte opløsning af $A(X)$:

$$A(X) = p_1 \cdots p_s P_1(X) \cdots P_r(X).$$

③ Det følger nu, at $R[X]$ er faktoriel. At samtlige primelementer i $R[X]$ er af den angivne form følger nu lit enten af ② eller ved at bemærke, at samtlige irreducible elementer i $R[X]$ må være af den angivne form ▨

KOROLLAR.

5.8. <u>Polynomiumsringen $\mathbb{Z}[X_1, \cdots, X_n]$ i n variable (specielt polynomiumsringen $\mathbb{Z}[X]$ i én variabel) er en faktoriel ring.</u>

<u>Polynomiumsringen $L[X_1, \cdots, X_n]$ i n variable med koefficienter i et legeme L er en faktoriel ring.</u>

Begge resultater bevises ved induktion ud fra Gauß' sætning, idet vi har

$$R[X_1,\dots,X_n] \simeq R[X_1,\dots,X_{n-1}][X_n].$$

5.9 SCHÖNEMANN - EISENSTEINS IRREDUCIBILITETSKRITERIUM. *Lad R være en faktorisk ring, og lad*

$$f = a_0 + a_1X + \dots + a_nX^n \in R[X]$$

være et primitivt polynomium. Hvis der findes et primelement $p \in R$, så at

$$p \mid a_0,\ p \mid a_1,\ \dots,\ p \mid a_{n-1} \text{ og } p^2 \nmid a_0,$$

så er f et primelement i $R[X]$ (dvs. et irreducibelt polynomium).

Er K brøklegemet for R, kan vi altså slutte, at f er irreducibel i $K[X]$.

BEVIS. (Indirekte). Antag, at $f(X) = g(X)\,h(X)$ i $R[X]$, hvor g og h ikke er enheder. Da f er et primitivt polynomium, må vi have $\deg g \geqslant 1$, $\deg h \geqslant 1$:

$$a_0 + \dots + a_nX^n = (b_0 + \dots + b_kX^k)(c_0 + \dots + c_{n-k}X^{n-k}),$$

hvor $0 < k < n$. Da f er primitivt, er $p \nmid a_n$. Ved overgang til restklasseringen $R/(p)$ får vi

$$\overline{a_n}X^n = (\overline{b_0} + \dots + \overline{b_k}X^k)(\overline{c_0} + \dots + \overline{c_{n-k}}X^{n-k})$$

og $\overline{a_n} \neq 0$. Nu er (p) et primideal, og $R/(p)$ et integritetsområde. Vi slutter derfor let, at vi må have $\overline{b_0} = \dots = \overline{b_{k-1}} = 0$ og $\overline{c_0} = \dots = \overline{c_{n-k-1}} = 0$. Specielt er altså $p \mid b_0$ og $p \mid c_0$, men så er $p^2 \mid b_0c_0 = a_0$ i modstrid med forudsætningen ▨

5.10 EKSEMPLER. Polynomiet $X^n \pm p$, hvor p er et primtal, er irreducibelt i $\mathbb{Z}[X]$ (eller $\mathbb{Q}[X]$). Dermod er $X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$ reducibelt i $\mathbb{Z}[X]$.

Polynomiet $F_p(X) = X^{p-1} + X^{p-2} + \dots + X + 1 = \frac{X^p - 1}{X - 1}$, hvor p er et primtal, er irreducibelt i $\mathbb{Z}[X]$ (eller $\mathbb{Q}[X]$), idet kriteriet kan anvendes på

$$F_p(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \sum_{1 < i < p} \binom{p}{i} X^{i-1} + p.$$

Er L et legeme, således at $n1 \neq 0$ i L (dvs. er L's karakteristik ikke divisor i n), så er polynomiet

$$X^n + Y^n - 1$$

irreducibelt i $L[X,Y] = L[Y][X]$,
thi for primelementet $Y - 1 \in L[Y]$ har vi $(Y-1) \mid Y^n - 1$, og da $Y^n - 1 = [(Y-1)+1]^n - 1 = \sum_{1 \leq i \leq n} \binom{n}{i} (Y-1)^i$
$= (Y-1) + (Y-1)^2 q(Y)$, har vi $(Y-1)^2 \nmid Y^n - 1$.

6. Appendix: Kvadratiske talringe.

6.1. DEFINITION. Et tal $\xi \in \mathbb{C}$ kaldes et (helt) kvadratisk tal, hvis der findes et normeret 2den-gradspolynomium

$$X^2 + bX + c \in \mathbb{Z}[X],$$

der har ξ som rod.

Indføres for polynomiet X^2+bX+c diskriminanten

$$D = b^2 - 4c,$$

kan polynomiet skrives

$$X^2 + bX + c = (X + \tfrac{b}{2})^2 - \frac{D}{4}.$$

Det følger, at et kvadratisk tal har formen

$$\xi = \frac{-b \pm \sqrt{D}}{2}, \quad b, D \in \mathbb{Z}, \quad D \equiv b^2 \pmod 4$$

[hvor vi sætter $\sqrt{D}$ = sædvanlig kvadratrod (≥ 0), hvis $D \geq 0$, og $\sqrt{D} = i\sqrt{-D}$, hvis $D < 0$]. Et kvadratisk tal kan være reelt (nemlig når $D \geq 0$) eller imaginært (nemlig når $D<0$).

OBSERVATION. Diskriminanten ovenfor er et helt tal, $\equiv \begin{cases} 0 \\ 1 \end{cases} \pmod 4$, thi $D \equiv b^2$, og et kvadrat b^2 er altid $\equiv \begin{cases} 0 \\ 1 \end{cases} \pmod 4$.

BEMÆRKNING. Et kvadratisk tal ξ er enten irrationalt ($\text{d}: \in \mathbb{C} \setminus \mathbb{Q}$) eller et sædvanligt helt tal ($\text{d}: \in \mathbb{Z}$). Er nemlig ξ en rational rod i X^2+bX+c, $b,c \in \mathbb{Z}$, og skrives $\xi = a/s$, $a \in \mathbb{Z}$, $s \in \mathbb{N}$, kan vi antage, at intet primtal går op i både a og s. Af $(a/s)^2 + b(a/s) + c = 0$ får vi

$$s(-ba - cs) = a^2.$$

Ethvert primtal, der går op i s, går derfor også op i a. Det følger, at $s=1$, således at $\xi = a/1 \in \mathbb{Z}$.

6.2. LEMMA. Lad $\xi \in \mathbb{C}$ være et komplekst tal. Da er ξ kvadratisk, hvis og kun hvis der findes et tal $\eta \in \mathbb{C}$, så at

$$\xi + \eta \in \mathbb{Z} \quad \text{og} \quad \xi\eta \in \mathbb{Z}.$$

BEVIS. For polynomier udtrykker ligningen:

$$(*) \qquad X^2 + bX + c = (X - \xi)(X - \eta),$$

at

$$b = -(\xi + \eta), \quad c = \xi\eta.$$

"hvis": Polynomiet $X^2 + bX + c$ defineret ved ligningen (*) har ifølge forudsætningen koefficienter i $\mathbb{Z}$. Da det øjensynlig har ξ som rod, er ξ kvadratisk.

"kun hvis": Hvis ξ er kvadratisk, og altså rod i et polynomium $X^2 + bX + c$, $b, c \in \mathbb{Z}$, kan dette polynomium skrives på formen (*). Som η kan altså bruges "den anden rod" i dette polynomium. ▨

6.3. OBSERVATION. Hvis et kvadratisk tal ξ er irrationalt, så er det i Lemma 6.2 nævnte tal η entydigt bestemt.

Er nemlig $\tilde{\eta} \in \mathbb{C}$ endnu et tal, der opfylder betingelserne, fås

$$\tilde{\eta} - \eta \in \mathbb{Z}, \quad \xi(\tilde{\eta} - \eta) \in \mathbb{Z}.$$

Af $\eta \neq \tilde{\eta}$ følger derfor $\xi \in \mathbb{Q}$.

DEFINITION. For et irrationalt kvadratisk tal ξ kaldes ovennævnte entydigt bestemte tal η for ξ's <u>konjugerede</u> tal, og det betegnes ξ'. Hvis et kvadratisk tal ξ er rationalt, og dermed helt, jfr. Bemærkning 6.1, sættes $\xi' = \xi$. Tallet

$$N(\xi) := \xi\xi'$$

kaldes <u>normen</u> af det kvadratiske tal ξ, og tallet

$$D(\xi) := (\xi - \xi')^2 = (\xi + \xi')^2 - 4\xi\xi'.$$

kaldes <u>diskriminanten</u> af ξ.

6.4. OBSERVATION. Hvis et irrationalt kvadratisk tal ξ er rod i polynomiet $X^2 + bX + c$, og altså af formen

$$\xi = \frac{-b \pm \sqrt{D}}{2}, \quad D = b^2 - 4c,$$

finder vi for det konjugerede tal:

$$\xi' = \frac{-b \mp \sqrt{D}}{2},$$

og videre:

$$\xi + \xi' = -b, \quad N(\xi) = \xi\xi' = c, \quad D(\xi) = (\xi - \xi')^2 = D.$$

Er det kvadratiske tal ξ derimod rationalt, og altså $\xi = a \in \mathbb{Z}$, finder vi

$$N(a) = a^2 \qquad D(a) = 0.$$

Normen og diskriminanten er altså i begge tilfælde hele tal.

BEMÆRKNING. Hvis et kvadratisk tal ξ er imaginært, så er dets konjugerede ξ' det sædvanlige komplekst konjugerede tal $\overline{\xi}$. Det følger, at $N(\xi) = \xi\overline{\xi} = |\xi|^2$. Specielt er altså i så fald $N(\xi) \geq 0$.

6.5. SÆTNING. Lad $\xi \in \mathbb{C}$ være et irrationalt kvadratisk tal, rod i polynomiet $X^2 + bX + c$, $b, c \in \mathbb{Z}$. Da er delmængden

$$\mathbb{Z}[\xi] := \{ x + y\xi \mid x, y \in \mathbb{Z} \} \subseteq \mathbb{C}$$

en delring af $\mathbb{C}$, og for tal $\alpha \in \mathbb{Z}[\xi]$ er fremstillingen

$$\alpha = x + y\xi, \quad x, y \in \mathbb{Z},$$

entydig. Alle tal $\alpha \in \mathbb{Z}[\xi]$ er kvadratiske, og konjugering:

$$\alpha \longmapsto \alpha'$$

er en involutorisk automorfi i ringen $\mathbb{Z}[\xi]$.

BEVIS. Det er klart, at $\mathbb{Z}[\xi] \supseteq \mathbb{Z}$, og at $\mathbb{Z}[\xi]$ er stabil under addition. Da vi endvidere har

$$\xi^2 = -c - b\xi \in \mathbb{Z}[\xi],$$

følger det let, at $\mathbb{Z}[\xi]$ er stabil under multiplikation. Følgelig er $\mathbb{Z}[\xi] \subseteq \mathbb{C}$ en delring.

Entydigheden af en fremstilling $\alpha = x + y\xi$, $x, y \in \mathbb{Z}$, følger let af at tallet ξ ikke er rationalt.

For det konjugerede tal ξ' har vi

$$\xi + \xi' = -b, \quad \xi\xi' = c.$$

For et tal $\alpha = x + y\xi \in \mathbb{Z}[\xi]$ finder vi derfor

$$\alpha + (x + y\xi') = 2x + y(-b) \in \mathbb{Z} \text{ og } \alpha(x + y\xi') = x^2 - bxy + cy^2 \in \mathbb{Z}.$$

Af Lemma 6.2 følger nu, at α er kvadratisk. Hvis α er irrationalt følger det videre, at $\alpha' = x + y\xi'$, og hvis α er ra-

tional, må vi have $y = 0$ (hvorfor?), og altså $\alpha' = \alpha = x$. I begge tilfælde gælder altså

$$\alpha' = x + y\xi'.$$

Da $\xi' = -b - \xi \in \mathbb{Z}[\xi]$, følger det, at $\alpha' \in \mathbb{Z}[\xi]$. At konjugering er involutorisk (altså at $(\alpha')' = \alpha$) følger umiddelbart af definition 6.3. At $\alpha \mapsto \alpha'$ er en ringhomomorfi (altså at $(\alpha+\beta)' = \alpha' + \beta'$, $(\alpha\beta)' = \alpha'\beta'$ og $1' = 1$) fås lit af det fundne udtryk for α'. At $\alpha \mapsto \alpha'$ er en automorfi følger af, at en involution er bijektiv □

. DEFINITION. En delring $R \subseteq \mathbb{C}$ af formen $R = \mathbb{Z}[\xi]$ med et passende irrationalt kvadratisk tal ξ kaldes en <u>kvadratisk talring</u>. Den kaldes <u>reel</u> eller <u>imaginær</u> eftersom tallet ξ er reelt eller imaginært.

KOROLLAR. For en kvadratisk talring R er normen en multiplikativ homomorfi

$$N : R \to \mathbb{Z},$$

og for $\alpha \in R$ gælder:

$$N(\alpha) = 0 \iff \alpha = 0.$$

BEVIS. Da afbildningen $\alpha \mapsto \alpha'$ er multiplikativ, er også afbildningen $\alpha \mapsto N(\alpha) = \alpha\alpha'$ multiplikativ. At $N(\alpha) \in \mathbb{Z}$ har vi set i Observation 6.4. Den sidste påstand følger af, at nulreglen gælder i $\mathbb{C}$ ▨

6.6. UDREGNING. Lad ξ være en irrational rod i polynomiet $X^2 + bX + c$, $b, c \in \mathbb{Z}$. For et element

$$x + y\xi, \quad x, y \in \mathbb{Z},$$

i den kvadratiske talring $\mathbb{Z}[\xi]$ gælder da:

$$N(x + y\xi) = x^2 - bxy + cy^2 \quad (\text{og } D(x+y\xi) = y^2(b^2 - 4c).)$$

BEVIS. Regn selv □

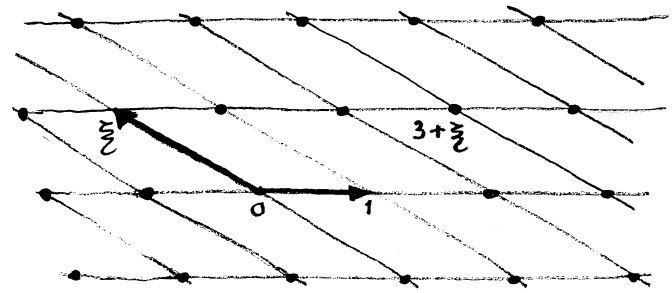
MORALE. Elementerne $\alpha = x + y\xi$ i en kvadratisk talring $\mathbb{Z}[\xi]$ svarer bijektivt til par $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ af hele tal.

Elementer $\alpha \in \mathbb{Z}[\xi]$ med en given norm $N(\alpha) = k$, hvor $k \in \mathbb{Z}$, svarer bijektivt til løsninger $(x,y) \in \mathbb{Z}\times\mathbb{Z}$ til ligningen

$$\boxed{x^2 - bxy + cy^2 = k.}$$

Det er her forudsat, at diskriminanten $D = b^2 - 4c$ ikke er et kvadrat i ringen $\mathbb{Z}$.

BEMÆRKNING. Idet vi på sædvanlig måde opfatter $\mathbb{C}$ som et 2-dimensionalt vektorrum over $\mathbb{R}$, ser vi for en imaginær kvadratisk talring $\mathbb{Z}[\xi]$, at "vektorerne" $1, \xi \in \mathbb{C}$ er en basis, og elementerne $\alpha \in \mathbb{Z}[\xi]$ kan opfattes som de vektorer $\alpha \in \mathbb{C}$ der har heltalskoordinater m.h.t. denne basis. De kan anskueliggøres som gitterpunkter i et Wesseldiagram:



Vi minder om, at vi i denne situation har $N(\alpha) = |\alpha|^2$. Elementer $\alpha \in \mathbb{Z}[\xi]$ med en given norm $N(\alpha) = k \in \mathbb{N}$ svarer således til gitterpunkter på cirklen med radius $\sqrt{k}$ og centrum i 0.

6.7. SÆTNING. Lad $R = \mathbb{Z}[\xi]$ være en kvadratisk talring. Et element $\varepsilon \in R$ er da en enhed i R, hvis og kun hvis $N(\varepsilon) = \pm 1$.

BEVIS. "hvis": Af $N(\varepsilon) = \varepsilon\varepsilon' = \pm 1$, følger $\varepsilon(\pm\varepsilon') = 1$. Da $\pm\varepsilon' \in R$, er ε altså invertibel (med $\pm\varepsilon'$ som invers).
"kun hvis": Af en ligning $\varepsilon\eta = 1$ i ringen R, får vi $N(\varepsilon)N(\eta) = N(1) = 1$ i ringen $\mathbb{Z}$. Det følger, at $N(\varepsilon)$ er en enhed i $\mathbb{Z}$, altså at $N(\varepsilon) = \pm 1$ ▨

MORALE. For en irrational rod ξ i polynomiet X^2+bX+c, $b,c\in\mathbb{Z}$, svarer enhederne ε i $R=\mathbb{Z}[\xi]$ til løsninger $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ til ligningen

$$\boxed{x^2-bxy+cy^2=\pm 1.}$$

At $\varepsilon\in R^* \Rightarrow \pm\varepsilon^n\in R^*$, når $n\in\mathbb{Z}$, kan derfor udnyttes til ud fra én løsning (x,y) til ligningen, at bestemme yderligere en række.

SIDEBEMÆRKNING 1. For en imaginær kvadratisk talring $R=\mathbb{Z}[\xi]$, hvor ξ er rod i polynomiet X^2+bX+c, $b,c\in\mathbb{Z}$, og hvor altså $D=b^2-4c<0$, gælder, at

$$R^*=\{\pm 1\},$$ undtagen hvis

$D=-3$, hvor $R^*=\{1,\zeta,\zeta^2,\zeta^3,\zeta^4,\zeta^5\}$, $\zeta=\frac{1+\sqrt{-3}}{2}$, eller hvis

$D=-4$, hvor $R^*=\{1,i,i^2,i^3\}$, $i=\sqrt{-1}$.

BEVIS. Da $D\equiv\begin{cases}0\\1\end{cases}\pmod 4$, har vi $D\le -3$. Det er klart, at vi altid har $\{\pm 1\}\subseteq R^*$. Antag derfor, at $\varepsilon=u+v\xi$, $u,v\in\mathbb{Z}$, er en enhed $\neq\pm 1$. Det følger, at ε må være imaginær og kvadratisk, og da $\varepsilon\bar\varepsilon=1$ må ε følgelig være rod i et polynomium

$$X^2+eX+1, \text{ hvor } e\in\mathbb{Z} \text{ og } e^2-4<0.$$

Heraf følger $e=0$ eller $e=\pm 1$.

Hvis $e=0$, har vi $\varepsilon=\pm i$, og dermed

$$-4=(\varepsilon-\bar\varepsilon)^2=D(\varepsilon)=v^2D \quad (\text{jfr. Udregning 6.6}),$$

hvoraf $D=-4$, $v=\pm 1$ (idet $D=-1$ er udelukket). Er omvendt $D=-4$, så må b være lige, og da $\xi=\frac{-b+\sqrt{-4}}{2}=-\frac{b}{2}+i$, ses at $i=\frac{b}{2}+\xi\in\mathbb{Z}[\xi]$.

Hvis $e=\pm 1$, har vi $\varepsilon=\frac{\mp 1\pm\sqrt{-3}}{2}\in\{\zeta,\zeta^2,\zeta^4,\zeta^5\}$, hvoraf

$$-3=(\varepsilon-\bar\varepsilon)^2=D(\varepsilon)=v^2D,$$

hvoraf $D=-3$, $v=\pm 1$. Er omvendt $D=-3$, så må b være ulige, og da $\xi=\frac{-b+\sqrt{-3}}{2}$, ses, at

$\zeta=\frac{b+1}{2}+\xi\in\mathbb{Z}[\xi]$.

Heraf følger påstandene □

MORALE. Ligningen

$$\boxed{x^2-bxy+cy^2=1,} \quad \text{hvor } b,c\in\mathbb{Z},\ D=b^2-4c<0$$

har af løsninger $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ kun de trivielle $(\pm 1, 0)$, undtagen hvis $D = -3$, hvor løsningerne er $(\pm 1, 0)$ og $\left(\frac{b \pm 1}{2}, \pm 1\right)$, eller hvis $D = -4$, hvor løsningerne er $(\pm 1, 0)$ og $\left(\frac{b}{2}, \pm 1\right)$.

SIDEBEMÆRKNING 2. For en reel kvadratisk talring $R = \mathbb{Z}[\xi]$, hvor ξ er rod i polynomiet $X^2 + bX + c$, $b, c \in \mathbb{Z}$, og hvor altså $D = b^2 - 4c > 0$ ikke er et kvadrat, kan man bevise, at der altid findes en enhed $\varepsilon_0 \neq \pm 1$ i R, så at

$$R^* = \{ \pm \varepsilon_0^n \mid n \in \mathbb{Z} \}.$$

Specielt er der altid uendelig mange enheder. En sådan enhed ε_0 kaldes en grundenhed. [Hvis grundenheden ε_0 har $N(\varepsilon_0) = 1$, ses, at alle enheder $\varepsilon \in R^*$ har $N(\varepsilon) = 1$. Er derimod $N(\varepsilon_0) = -1$, ses, at

$$\{ \varepsilon \in R \mid N(\varepsilon) = 1 \} = \{ \pm (\varepsilon_0^2)^n \mid n \in \mathbb{Z} \}. \ ]$$

MORALE. Ligningen

$$\boxed{x^2 - bxy + cy^2 = \pm 1,}$$

hvor $b, c \in \mathbb{Z}$, og $D = b^2 - 4c > 0$ ikke er et kvadrat, har af løsninger $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ altid en ikke-triviel grundløsning (u_0, v_0), således at den fuldstændige løsning er givet ved

$$\pm (u_n, v_n), \quad n \in \mathbb{Z},$$

hvor u_n og v_n er bestemt ved ligningen

$$(u_0 + v_0 \xi)^n = u_n + v_n \xi, \quad \xi \text{ en rod i } X^2 + bX + c.$$

[Et tilsvarende resultat gælder for ligningen $x^2 - bxy + cy^2 = 1$]

6.8. SÆTNING. Lad $R = \mathbb{Z}[\xi]$ være en kvadratisk talring, og lad $\alpha, \delta \in R$. Hvis δ er divisor i α, så gælder i ringen $\mathbb{Z}$, at $N(\delta)$ er divisor i $N(\alpha)$, og divisoren δ i α er en ikke-triviel divisor, hvis og kun hvis $N(\delta)$ i ringen $\mathbb{Z}$ er en ikke triviel divisor i $N(\alpha)$.

BEVIS. Hvis $\alpha = \delta\beta$, $\beta \in R$, får vi i $\mathbb{Z}$, at $N(\alpha) = N(\delta) N(\beta)$, hvoraf den første påstand. Den anden påstand følger nu af Sætning 6.7. ∎

KOROLLAR. I en kvadratisk talring $R = \mathbb{Z}[\xi]$ har hvert element $\neq \{^0_{\text{enhed}}$ i R en irreducibel opløsning.

BEVIS. Dette følger af Korollar 3.8.1, thi ifølge det lige viste har den ved $\nu(\alpha) = |N(\alpha)|$ definerede funktion

$$\nu : R \to \mathbb{Z}$$

den i Korollar 3.8.1 nævnte egenskab □

BEMÆRKNING. En kvadratisk talring $R = \mathbb{Z}[\xi]$ er delring af legemet $\mathbb{C}$. For elementer $\alpha, \delta \in R$, $\delta \neq 0$, ser vi derfor, at δ er divisor i α, netop når det komplekse tal $\frac{\alpha}{\delta}$ tilhører R. Skriver vi $\frac{\alpha}{\delta} = \frac{\alpha\delta'}{\delta\delta'}$, har vi $\delta\delta' = N(\delta) \in \mathbb{Z}\setminus\{0\}$, og $\alpha\delta' \in R$ og har derfor formen $x + y\xi$. Følgelig har vi $\frac{\alpha}{\delta} = \frac{x}{N(\delta)} + \frac{y}{N(\delta)}\xi$, så $\frac{\alpha}{\delta}$ har formen

$$(*) \qquad \frac{\alpha}{\delta} = \lambda + \mu\xi, \quad \lambda, \mu \in \mathbb{Q}.$$

Tallene af denne form udgør således brøklegemet for R. Vi ser, at δ er divisor i α, netop når koefficienterne λ, μ i fremstillingen (*) tilhører $\mathbb{Z}$.

Det er således en simpel sag for givne $\alpha, \delta \in R$ at afgøre om δ er divisor i α, men det må fremhæves, at det for et givet $\alpha \in R$ sædvanligvis er kompliceret at bestemme de δ'er, der er divisorer i α.

6.9. SPECIELLE RESULTATER. (1). Den kvadratiske talring $\mathbb{Z}[\sqrt{-1}]$ et hovedidealområde.

(2) Den kvadratiske talring $\mathbb{Z}[\sqrt{2}]$ er et hovedidealområde

(3) Den kvadratiske talring $\mathbb{Z}[\sqrt{-5}]$ er ikke faktoriel.

BEVIS. (1): Vi viser for $R = \mathbb{Z}[\sqrt{-1}]$, at den ved $\nu : \alpha \longmapsto N(\alpha) = |\alpha|^2$ definerede funktion $\nu : R \to \mathbb{Z}$ har den i Sætning 1.4 nævnte egenskab. Funktionen er nedad begrænset, idet $\nu(\alpha) \geqslant 0$, så vi mangler at vise for givne $\delta, \alpha \in R$, $\delta \neq 0$, at der findes et element $\eta \in R$ med $\nu(\alpha - \eta\delta) < \nu(\delta)$. Denne ulighed er åbenbart ensbetydende med uligheden

$$(*) \qquad \left|\frac{\alpha}{\delta} - \eta\right| < 1.$$

Idet tallene $\eta \in R$ er gitterpunkterne $x+yi$, $x,y \in \mathbb{Z}$, ser vi, at der for *hvert* kompleks tal $w \in \mathbb{C}$ findes et gitterpunkt η hvis afstand til w er $\leq \frac{1}{2} \cdot$ (diagonalen i et kvadrat med side 1) $= \frac{1}{2}\sqrt{2}$. Vi kan altså for $w \in \mathbb{C}$ opfylde:

$$|w - \eta| \leq \tfrac{1}{2}\sqrt{2}, \quad \eta \in R,$$

og dermed for $w = \frac{\alpha}{\delta}$ specielt uligheden (*).

(2): Vi anvender igen Sætning 1.4, på $R = \mathbb{Z}[\sqrt{2}]$, med $v: R \to \mathbb{Z}$ givet ved $v(\alpha) = |N(\alpha)| = |\alpha\alpha'|$, og skal altså for givne $\alpha = a+b\sqrt{2}$, $\delta = c+d\sqrt{2} \in R$, $\delta \neq 0$, bestemme $\eta = x+y\sqrt{2} \in R$, så at

$$v(\alpha - \eta\delta) < v(\delta).$$

Efter division med $|\delta\delta'| = v(\delta)$ fås den ensbetydende ulighed

$$\left|\left(\frac{\alpha}{\delta} - \eta\right)\left(\frac{\alpha'}{\delta'} - \eta'\right)\right| < 1$$

Indsættes her $\frac{\alpha}{\delta} = \lambda + \mu\sqrt{2}$, $\lambda, \mu \in \mathbb{Q}$ (jfr. Bemærkning 6.8), og $\eta = x+y\sqrt{2}$, kan uligheden skrives

$$|(\lambda - x)^2 - 2(\mu - y)^2| < 1.$$

Her er λ, μ specielt reelle tal, og vi kan følgelig finde hele tal $x, y \in \mathbb{Z}$, så at $|\lambda - x| \leq \frac{1}{2}$ og $|\mu - y| \leq \frac{1}{2}$. Med dette valg af x og y er den søgte ulighed specielt opfyldt.

(3): I ringen $R = \mathbb{Z}[\sqrt{-5}]$ har vi øjensynlig opløsningen

$$(*) \quad 6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

Tallet $2 \in R$ har normen $N(2) = 2^2$. En ikke-triviel divisor $\delta = x+y\sqrt{-5}$ måtte derfor ifølge Sætning 6.8 have normen $N(\delta) = x^2 + 5y^2 = 2$, men denne ligning kan øjensynlig ikke gælde når $(x,y) \in \mathbb{Z} \times \mathbb{Z}$. Følgelig er tallet 2 et irreducibelt element i R, og det er derfor nok at vise, at 2 ikke er et primelement.

Tallet 2 er hverken divisor i $1+\sqrt{-5}$ eller i $1-\sqrt{-5}$, thi

$$\frac{1+\sqrt{-5}}{2} = \frac{1}{2} + \frac{1}{2}\sqrt{-5} \notin R \quad \text{og} \quad \frac{1-\sqrt{-5}}{2} = \frac{1}{2} - \frac{1}{2}\sqrt{-5} \notin R.$$

Af (*) fremgår imidlertid, at 2 er divisor i produktet $(1+\sqrt{-5})(1-\sqrt{-5})$, og 2 er derfor ikke et primelement ▨

6.10. EKSEMPEL. I den kvadratiske talring $R = \mathbb{Z}[\sqrt{-5}]$ har elementet 6 to forskellige irreducible opløsninger

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

thi ganske som i beviset ovenfor følger det, at elementerne $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ er irreducible i R.

6.11. Man ved ikke, om der er uendelig mange reelle kvadratiske talringe, der er faktorielle. Man kan vise (men det er svært), at der blandt de imaginære kun er 9, der er faktorielle.

FORGRENINGS-SÆTNING. Lad $R = \mathbb{Z}[\xi]$ være en kvadratisk talring, og antag, at R er en faktoriel ring. Ethvert sædvanligt primtal $p \in \mathbb{N}$ vil da m.h.t. R være af en af følgende 3 typer:

Type 1: p er et primelement i R

Type 2: p har i R en primopløsning $p = \pm \pi\pi'$, hvor det konjugerede primelement π' ikke er associeret med π.

Speciel type: p har i R en primopløsning $p = \pm \pi\pi'$, hvor det konjugerede primelement π' er associeret med π

Omvendt gælder, at hvert primelement π i R er associeret med et af primelementerne nævnt under de 3 typer.

BEVIS. Et primtal p er ikke en enhed i R, og der findes derfor et primelement π i R, som er divisor i p. Følgelig er $N(\pi)$ inden for $\mathbb{Z}$ divisor i $N(p) = p^2$ (Sætning 6.8), så vi har $N(\pi) = \pm p^2$ eller $N(\pi) = \pm p$. Hvis $N(\pi) = \pm p^2$, er π en triviel divisor i p, og derfor associeret med p, og så er også p et primelement i R, og altså af type 1. Hvis derimod $N(\pi) = \pm p$, så har vi $p = \pm N(\pi) = \pm \pi\pi'$, og så er p af type 2 eller af speciel type.

Er omvendt π et primelement, så er $\pi\pi' = N(\pi) \in \mathbb{Z}$. Skrives dette tal inden for $\mathbb{Z}$ som et produkt af $\pm$primtal, går π altså op i produktet, og dermed i en af faktorerne. Der findes derfor et sædvanligt primtal $p \in \mathbb{N}$, så at

π er divisor i p. Heraf følger påstanden, idet vi ovenfor har angivet primoplösninger i R for alle sædvanlige primtal p. ▨

6.12. Det må fremhæves, at inddelingen af primtallene i de 3 typer, der også kaldes primtallenes <u>forgrening</u>, naturligvis afhænger af den givne (<u>faktorielle</u>) kvadratiske talring R.

Vi vil her betragte den kvadratiske talring $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$, som også kaldes <u>Gauss' talring</u>. Vi har set (Resultat 6.9), at $\mathbb{Z}[i]$ er et hovedidealområde, og dermed en faktoriel ring. Enhederne $\varepsilon = x+yi \in \mathbb{Z}[i]$ svarer (Morale 6.7) til løsninger $(x,y) \in \mathbb{Z}\times\mathbb{Z}$ til ligningen $x^2+y^2 = 1$. Løsningerne er øjensynlig $(\pm 1, 0)$ og $(0, \pm 1)$, og enhederne er derfor

$$1, i, -1, -i.$$

Videre gælder følgende om:

FORGRENING I GAUSS' TALRING. M.h.t. Gauss' talring $\mathbb{Z}[i]$ falder de sædvanlige primtal i følgende typer:

<u>Type 1</u> er netop primtallene $\equiv 3 \pmod 4$.

<u>Type 2</u> er netop primtallene $\equiv 1 \pmod 4$

<u>Speciel type</u> har kun primtallet 2 (med primoplösningen $2 = (1+i)(1-i)$).

BEVIS. <u>Speciel type</u>: Primtallet $2 = (1+i)(1-i)$ er specielt, da $1-i = (-i)(1+i)$ er associeret med $1+i$. Er omvendt p et specielt primtal, så har vi en primoplösning $p = \pi\bar{\pi}$, hvor $\pi = x+iy$ er et primelement associeret med $\bar{\pi}$, altså

$$\bar{\pi} = \pi, \quad \bar{\pi} = i\pi, \quad \bar{\pi} = -\pi \quad \text{eller} \quad \bar{\pi} = (-i)\pi$$

Var $\bar{\pi} = \pi$, ville $\pi = x \in \mathbb{Z}$, og dermed $p = \pi\bar{\pi} = x^2$, være i modstrid med at p var et primtal. Tilsvarende er $\bar{\pi} \neq -\pi$, thi ellers var $\pi = yi$, og $p = \pi\bar{\pi} = y^2$. Følgelig er $\bar{\pi} = \pm i\pi$, hvoraf $\pi = x \pm xi$, og så er $p = \pi\bar{\pi} = 2x^2$, og da p er et primtal, får vi endelig $p = 2$.

<u>Type 2</u>: Lad p være et primtal af type 2. Vi har da $p = \pi\bar{\pi}$ med et primelement $\pi = x+yi \in \mathbb{Z}[i]$, og altså

$$p = \pi\bar{\pi} = x^2 + y^2, \quad x, y \in \mathbb{Z}.$$

Da et kvadrat i $\mathbb{Z}$ er $\equiv \begin{cases} 0 \\ 1 \end{cases} \pmod 4$ (hvorfor?), har vi følgelig $p \equiv \begin{cases} 0 \\ 2 \end{cases} \bmod 4$. Da primtallet p er $\neq 2$ (ifølge det allerede viste) og dermed ulige, må vi have $p \equiv 1 \pmod 4$.

For at fuldføre beviset, er det nok at vise, at et primtal $p \equiv 1 \pmod 4$ ikke kan være af type 1 (!).

Lad altså p være et primtal $\equiv 1 \pmod 4$. Det er vel-kendt (jfr. "Hele tal", Korollar 6.10.), at kongruensen

$$x^2 \equiv -1 \pmod p$$

da har løsninger. Der findes altså tal $x, d \in \mathbb{Z}$, så at

$$pd = x^2 + 1.$$

I Gauss' talring kan denne ligning skrives

$$pd = (x+i)(x-i),$$

og p er altså divisor i produktet $(x+i)(x-i)$. Hvis p var af type 1, ville p være et primelement i $\mathbb{Z}[i]$, og dermed divisor i en af faktorerne, men det er i modstrid med at hverken

$$\frac{x+i}{p} = \frac{x}{p} + \frac{1}{p}i \quad \text{eller} \quad \frac{x-i}{p} = \frac{x}{p} - \frac{1}{p}i$$

tilhører $\mathbb{Z}[i]$. ▨

KOROLLAR. For hvert primtal $p \equiv 1 \pmod 4$ har ligningen

$$x^2 + y^2 = p$$

løsninger $(x,y) \in \mathbb{Z} \times \mathbb{Z}$.

BEVIS. Er $p = \pi\bar{\pi}$, $\pi = x + iy \in \mathbb{Z}[i]$, så er (x,y) en løsning ▨

6.13. For bedre at kunne udnytte primoptløsninger 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 $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ er hvert primelement associeret med netop ét primelement i området bestemt ved

$$-\frac{\pi}{4} < \operatorname{Arg}(\alpha) \leqslant \frac{\pi}{4},$$

og som repræsentantsystem $\mathcal{P}$ vælger vi primelementer i dette område. Ifølge de fundne resultater er primelementerne i $\mathcal{P}$ enten $1+i$ (svarende til det specielle primtal $2 = (-i)(1+i)^2$), eller de er sædvanlige primtal $q \equiv 3 \pmod 4$ eller de findes i par $\pi, \bar{\pi}$ med $\pi\bar{\pi} = p$ et sædvanligt primtal $\equiv 1 \pmod 4$.

Hvert element $\alpha \neq 0$ i $\mathbb{Z}[i]$ har altså en entydig primoplösning af formen

$$(*) \quad \alpha = \varepsilon (1+i)^\lambda q_1^{\nu_1} \cdots q_r^{\nu_r} \pi_1^{\mu_1'} \bar{\pi}_1^{\mu_1''} \cdots \pi_s^{\mu_s'} \bar{\pi}_s^{\mu_s''}, \qquad \pi_j \bar{\pi}_j = p_j$$

hvor ε er en enhed, dvs $\in \{1, i, -1, -i\}$.

Lad os vise følgende

ANVENDELSE. Lad $k \in \mathbb{N}$ være et naturligt tal med primoplösningen

$$k = 2^t q_1^{n_1} \cdots q_r^{n_r} p_1^{m_1} \cdots p_s^{m_s},$$

hvor q_i'erne er $\equiv 3 \pmod 4$ og p_j'erne er $\equiv 1 \pmod 4$. 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 netop tallet

$$4(m_1+1)\cdots(m_s+1).$$

BEVIS. Ved den bijektive forbindelse mellem par $(x,y) \in \mathbb{Z}\times\mathbb{Z}$ og elementer $\alpha = x+iy \in \mathbb{Z}[i]$ svarer ligningen $x^2+y^2 = k$ til ligningen

$$N(\alpha) = k.$$

Elementerne $\alpha \in \mathbb{Z}[i] \setminus \{0\}$ er helt bestemt ved deres primoplösning af formen (*) ovenfor. [Idet vi om fornødent tilføjer potenser med eksponent 0 i (*) og (Δ) kan vi antage, at q_i'erne og p_j'erne er de samme]. Af (*) fås

$$N(\alpha) = 1 \cdot 2^\lambda q_1^{2\nu_1} \cdots q_r^{2\nu_r} p_1^{\mu_1'} p_1^{\mu_1''} \cdots p_s^{\mu_s'} p_s^{\mu_s''}.$$

Af sætningen om (sædvanlige) primopløsningers entydighed følger, at α med primopløsningen (*) vil opfylde ligningen

$$N(\alpha) = k,$$

netop når eksponenterne opfylder ligningerne

$$\lambda = t,\ 2\nu_1 = m_1, \dots, 2\nu_r = m_r,\ \mu_1' + \mu_1'' = m_1, \dots, \mu_s' + \mu_s'' = m_s.$$

Dette er naturligvis kun muligt, når m_i'erne er lige. Og er det tilfældet, kan vi løse ligningerne, og frit vælge $\mu_1' = 0, \dots, m_1, \dots, \mu_s' = 0, \dots, m_s$. Desuden har vi 4 mulige valg af enheden ε, altså i alt $4(m_1+1)\cdots(m_s+1)$ elementer α, som opfylder $N(\alpha) = k$ ▨

6.14. Det fremhæves, at vi i beviset ovenfor eksplicit har bestemt 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 ligningen $x_j^2 + y_j^2 = p_j$.

Som eksempel vil vi betragte <u>pytagoræiske talsæt</u>, dvs talsæt $(x,y,z) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$, som er en løsning til ligningen

$$x^2 + y^2 = z^2$$

En sådan løsning vil vi kalde <u>ikke-triviel</u>, hvis x og y er primiske [Er $d > 1$ divisor i både x og y, så er d også divisor i z (hvorfor?), så vi kan skrive $x = dx'$, $y = dy'$, $z = dz'$. En triviel løsning har altså formen $(x,y,z) = (dx', dy', dz')$, hvor (x',y',z') er pytagoræisk og (specielt) $|z'| < |z|$].

Endvidere vil vi kalde to løsninger <u>essentielt ens</u>, hvis man kan komme fra den ene til den anden ved at erstatte (x,y) med $(\pm x, \pm y)$ eller $(\pm y, \pm x)$.

Idet vi kalder et tal $k \in \mathbb{N}$ <u>pytagoræisk</u>, hvis ligningen

$$x^2 + y^2 = k^2$$

har en ikke-triviel løsning, gælder følgende:

SÆTNING OM PYTAGORÆISKE TAL. Et naturligt tal $k > 1$ med primoplösningen

$$k = p_1^{m_1} \cdots p_s^{m_s}, \quad m_j \geq 1$$

er pytagoræisk, hvis og kun hvis primfaktorerne p_j alle er $\equiv 1 \pmod 4$. I bekræftende fald har ligningen

$$x^2 + y^2 = k^2$$

præcis 2^{s-1} essentielt forskellige, ikke-trivielle løsninger.

BEVIS. Skrives som i Anvendelsen ovenfor k's primoplösning på formen $k = 2^\ell q_1^{n_1} \cdots q_r^{n_r} p_1^{m_1} \cdots p_s^{m_s}$, skal vi vise:

$$k \text{ er pytagoræisk} \Leftrightarrow \ell = 0,\ n_1 = 0, \cdots, n_r = 0.$$

Udfra primoplösningen af k får vi

$$k^2 = 2^{2\ell} q_1^{2n_1} \cdots q_r^{2n_r} p_1^{2m_1} \cdots p_s^{2m_s}$$

Ligningen $x^2 + y^2 = k^2$ har derfor altid løsninger, svarende til elementer $\alpha = x + yi \in \mathbb{Z}[i]$ med primoplösninger

$$\alpha = \varepsilon (1+i)^{2\ell} q_1^{n_1} \cdots q_r^{n_r} \pi_1^{\mu_1'} \bar{\pi}_1^{\mu_1''} \cdots \pi_s^{\mu_s'} \bar{\pi}_s^{\mu_s''}, \quad \mu_j' + \mu_j'' = 2m_j.$$

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 afgöre ud fra ovenstående primoplösning af α, og vi ser, at $\alpha = x + yi$ giver en ikke-triviel løsning (x, y), netop når:

$$\ell = 0,\ n_1 = 0, \cdots, n_r = 0 \text{ og for hvert } j: \text{ enten } \mu_j' = 0 \text{ eller } \mu_j'' = 0.$$

Der er således ikke-trivielle løsninger netop når k har den angivne form. Er dette tilfældet får vi præcis $4 \cdot 2^s$ ikke-trivielle løsninger, og da disse 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) er der kun $\frac{1}{8} \cdot 4 \cdot 2^s = 2^{s-1}$ essentielt forskellige løsninger. ∎

BEMÆRK. Også her får vi explicit beskrevet løsningerne til $x^2 + y^2 = k^2$ ved at löse ligningerne $x_j^2 + y_j^2 = p_j$, $j = 1, \cdots, s$.

1. Angiv for hvert af nedenstående udtryk en mængde, hvori udtrykket definerer en komposition, og undersøg, om den er kommutativ, er associativ, har et neutralt element og om der findes invertible elementer:

(i) $(x,y) \longmapsto x+y$ (ii) $(x,y) \longmapsto x+2y$

(ii) $(x,y) \longmapsto x/y$ (iv) $(x,y) \longmapsto x^y$

(v) $(x,y) \longmapsto \sqrt{x^2+y^2}$ (vi) $(x,y) \longmapsto x+y-xy$

2. Samme spørgsmål som opgave 1 for udtrykkene:

(i) $(p,q) \longmapsto p \wedge q$ (ii) $(p,q) \longmapsto p \Rightarrow q$

(iii) $(p,q) \longmapsto \neg p$ (non p). (iv) $(p,q) \longmapsto p \Leftrightarrow q$

3. Samme spørgsmål som opgave 1 for udtrykkene

(i) $(A,B) \longmapsto A \cup B$ (ii) $(A,B) \longmapsto A \cap B$

(iii) $(A,B) \longmapsto A \oplus B := (A \setminus B) \cup (B \setminus A)$.

4. Lad E være en mængde og sæt $M = \mathcal{P}(E)$ (mængden af delmængder af E).

(i) Vis, at hver af kompositionerne $\cup$ og $\cap$ i M er distributiv m.h.t. den anden.

(ii) Vis, at der ved $A \longmapsto CA = E \setminus A$ defineres en isomorfi: $(M, \cup) \longrightarrow (M, \cap)$

(iii) Er $(M, \cup, \cap)$ en ring?

(iv) Vis, idet $A \oplus B := (A \setminus B) \cup (B \setminus A)$, at $(M, \oplus, \cap)$ er en ring.

5. Vis, at hvis x og y er inverbible elementer i et monoid, så er også xy inverbibel og $(xy)^{-1} = y^{-1}x^{-1}$!

Algebra 1984

Opgaver 7
("Strukturer")

1. Lad M være en mængde og lad $\mathrm{End}(M)$ betegne monoidet af alle afbildninger $: M \to M$ (med $\circ$ som komposition). Lad $*$ være en komposition i M.
   (i) Vis, at den ved $a \mapsto l_a$ bestemte afbildning $l : M \to \mathrm{End}(M)$ er en homomorfi $: (M,*) \to (\mathrm{End}(M,\circ))$, hvis og kun hvis $*$ er associativ.
   (ii) Hvad er det tilsvarende resultat for højrekomposition r_a?

2. Et element s i en semigruppe $(M,\cdot)$ siges at være <u>venstre-regulær</u>, hvis l_s er injektiv, <u>venstre-invertibelt</u>, hvis l_s er bijektiv og at <u>have</u> $u \in M$ som <u>venstre-invers</u>, hvis $l_u \circ l_s = Id_M$.
   (i) Hvad er de analoge definitioner med "højre-"?
   (ii) Vis: (s er venstre-invertibel) $\Rightarrow$ (s har venstre-invers) $\Rightarrow$ (s er venstre-regulær).
   (iii) Vis: (s er venstre-invertibel) $\Leftrightarrow$ (s har en venstre-regulær venstre-invers).
   (iv) Der gælder, at følgende betingelser er ækvivalente:
      (α) s har en venstre-invers og en højre-invers.
      (β) s er venstre-invertibel og højre-invertibel.
      (γ) s er venstre-invertibel og der findes et højre-regulært element.
      (δ) M har et neutralt element e og der findes $u \in M$ så $us = su = e$.
      (ε) Både l_s og r_s er surjektive.
   Vis nogle af implikationerne.

3. Lad $(M,\cdot)$ være en semigruppe.
   (i) Vis, at hvis $s \in M$ har $u \in M$ som venstre-invers, så er $e := us$ et <u>venstre-neutralt</u> element i M. Elementet u siges at være venstre-invers m.h.t. e. Vis, at hvis der findes et venstre-neutralt element $e \in M$, så at alle elementer i M har en venstre-invers m.h.t. e, så er M en gruppe.
   (ii) Vis, at hvis der findes venstre-regulære og højre-regulære elementer i M, og hvis hvert element i M har en venstre-invers eller en højre-invers, så er M en gruppe.

4. Hvad viser kompositionen $x * y := y$ om det foregående?

Algebra 1984

Opgaver
("Strukturer")

1. Angiv for hvert af nedenstående udtryk en mængde, hvori udtrykket definierer en relation, og undersøg, om den er refleksiv, irrefleksiv, o.s.v.
   (i) "er parallel med" (ii) "er vinkelret på"
   (iii) "er ensvinklet med" (iv) "har en divisor $\neq 1$ fælles med"
   (v) "er disjunkt med" (vi) "er ikke disjunkt med".

2. Samme spørgsmål som opgave 1 for udtrykkene:
   (i) "er gift med" (ii) "er barn af"
   (iii) "er født før" (iv) "er stærkere end".

3. Lad R være en relation i mængden M, altså $R \subseteq M \times M$.
   (i) Vis, at der blandt relationerne (d: delmængderne af $M \times M$), som indeholder R, findes en mindste refleksiv relation R_r, en mindste symmetrisk relation R_s, en mindste transitiv relation R_t og en mindste ækvivalensrelation $\tilde{R}$.
   (ii) Beskriv R_{rs} $(= (R_r)_s)$ og vis, at $R_{sr} = R_{rs}$
   (iii) Beskriv R_t.
   (iv) Vis, at hvis R er refleksiv og symmetrisk, så er $R_t = \tilde{R}$.
   (v) Vis, at $R_{rst} = \tilde{R}$.
   (vi) Beskriv R_r, R_s, R_{rs}, R_t og $\tilde{R}$ for nogle af relationerne i Opg 1 & 2.

4. (i) Vis, at en irrefleksiv, transitiv relation er asymmetrisk.
   (ii) Antag, at relationen R i M er symmetrisk og transitiv. Lad $a \in M$. Af aRx følger xRa (symmetrien) og dernæst aRa (transitiviteten). Da x var vilkårlig, er aRa, så R er altså refleksiv. Hvor var fejlen?

5. For en relation R i mængden M og $a \in M$ sættes
$$M_a = \{ x \in M \mid a = x \vee aRx \vee a(R \circ R)x \}.$$
Vis: Hvis R er total og M er endelig, så findes et element $b \in M$, så at $M_b = M$.

Algebra 1984 — Opgaver 9 ("Strukturer")

1. Vis, at nedenstående relationer i $\mathbb{N}$ er ordninger, og undersøg, om de er totale og om der er maksimale og minimale elementer.

(i) $x \prec y \overset{DEF}{\Leftrightarrow} \exists n \in \mathbb{N} : x = y + n.$

(ii) $x \prec y \overset{DEF}{\Leftrightarrow} \exists n \in \mathbb{N} : x + 2n = y$

(iii) $x \prec y \overset{DEF}{\Leftrightarrow} \exists n \in \mathbb{N} : xn = y$

(iv) $x \prec y \overset{DEF}{\Leftrightarrow} p\left(\frac{x}{d_{x,y}}\right) \prec p\left(\frac{y}{d_{x,y}}\right)$, hvor $d_{x,y}$ = største fælles divisor for x og y, og p er funktionen defineret ved

$$p(n) = \begin{cases} 1 & \text{hvis } n = 1 \\ \text{mindste primtal, der går op i } n, & \text{hvis } n > 1. \end{cases}$$

(v) Undersøg også den inducerede ordning på $\mathbb{N} \setminus \{1\}$.

2. Lad X og Y være ordnede mængder. Vis, at følgende definerer ordninger i produktmængden $X \times Y$.

(i) $(x,y) \prec (x',y') \overset{DEF}{\Leftrightarrow} x \prec x'$ og $y \prec y'$ ("produkt-ordning")

(ii) $(x,y) \prec (x',y') \overset{DEF}{\Leftrightarrow} x \precneqq x' \vee (x = x' \wedge y \prec y')$ ("leksikografisk ordning").

3. Generalisér ordningerne fra opgave 2 til

(i) et endeligt produkt $X_1 \times \cdots \times X_n$

(ii) et numerabelt produkt $X_1 \times X_2 \times \cdots$

(iii) Vis, at hvis hvert X_i er totalt ordnet, så er leksikografisk ordning en total ordning af produktet.

4. Lad $(M, <)$ være totalt ordnet. Vis, at der ved

$$(x,y) < (x',y') \Leftrightarrow \max\{x,y\} < \max\{x',y'\}$$
$$\vee \left[\max\{x,y\} = \max\{x',y'\} \wedge x < x'\right]$$
$$\vee \left[\max\{x,y\} = \max\{x',y'\} \wedge x = x' \wedge y < y'\right]$$

defineres en total ordning af $M \times M$.

5. Sammenlign de tre ordninger af $\mathbb{N} \times \mathbb{N}$ defineret i Opgave 2 og 4 ($X = Y = M = \mathbb{N}$).

Algebra 1984

Opgaver 10
("Struktur")

1. Lad $(A_n)_{n\in\mathbb{N}}$ være en familie af delmængder af mængden E, med $E = \bigcup_{n=1}^{\infty} A_n$. Vis, at de ikke-tomme mængder blandt mængderne

$$A_n \setminus \bigcup_{i=1}^{n-1} A_i \quad , \quad n = 1, 2, \ldots$$

udgør en klassedeling af E. Lad R være den tilsvarende ækvivalensrelation. Angiv en afbildning $f: E \to \mathbb{N}$, så at den tilhørende ækvivalensrelation $\tilde{f}$ er R.

2. Bestem for hver af nedenstående afbildninger $f: \mathbb{R} \to \mathbb{R}$ den tilhørende ækvivalensrelation $\tilde{f}$:

(i) $f(x) = e^x$ (ii) $f(x) = x^2$

(iii) $f(x) = \sin x$ (iv) $f(x) = \max\{1, |x|\}$

3. Lad $\prec$ være en transitiv relation i M. Vis, at der ved

$$x \sim y \overset{\text{DEF}}{\iff} x = y \vee (x \prec y \wedge y \prec x)$$

defineres en ækvivalensrelation $\sim$ i M. Overvej hvordan kvotientmængden $M/\sim$ "fornuftigt" kan ordnes.

4. For en given relation R i M kan vi betragte den "frembragte" ækvivalensrelation $\tilde{R}$, jfr. Opgave s8;3. For den tilhørende kvotientmængde skrives $M/\tilde{R} =: M/R$. Ofte skrives i stedet for R en liste over de (x,y) for hvilke xRy; oftest skrives i listen blot $x = y$ i stedet for xRy, og kvotient siges at fås ved de anførte identifikationer. Beskriv følgende kvotienter ($I = [0,1]$ er enhedsintervallet):

(i) $I/0 = 1$ (ii) $I/0 = \frac{1}{2} = 1$

(ii) $I/\frac{p-1}{n} = \frac{p}{n}$, $p = 1, \ldots, n$ (iv) $I/0 = \frac{5}{8}$, $\frac{1}{8} = \frac{7}{8}$, $\frac{3}{8} = 1$

(v) $I\times I/(x,0) = (x,1)$ (vi) $I\times I/(x,0) = (x,1)$, $(0,y) = (1,y)$

(vii) $I\times I/(0,x) = (1,1-x)$.

Algebra 1984

Opgaver 11
("Grupper")

1. For $L = \mathbb{Q}, \mathbb{R}$ eller $\mathbb{C}$ sættes $L^* = L \setminus \{0\}$. Endvidere sættes $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{R}_+^* = \{t \in \mathbb{R} \mid t > 0\}$ og $\mathbb{U} = \{u \in \mathbb{C} \mid |u| = 1\}$.

(i) De eftenfølgende mængder er grupper m.h.t. en "fornuftig" komposition:
$\mathbb{Z}^*, \mathbb{Z}, \mathbb{Q}, \mathbb{Q}^*, \mathbb{R}, \mathbb{R}_+^*, \mathbb{R}^*, \mathbb{C}, \mathbb{C}^*, \mathbb{U}$. Hvad er kompositionen?

(ii) Hvilke af disse grupper er "undergrupper i hinanden"?

(iii) De eftenfølgende afbildninger er homomorfier mellem nogle af disse grupper:
$z \mapsto \bar{z}$, $z \mapsto \mathrm{Re}(z)$, $z \mapsto \mathrm{Im}(z)$, $z \mapsto \frac{z}{|z|}$, $z \mapsto |z|$, $z \mapsto \log|z|$
$z \mapsto z^n$ $(n \in \mathbb{Z})$, $z \mapsto e^{iz}$.
Hvilke? Bestem for hver af dem kerne og billede.

2. For $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ eller $\mathbb{C}$ (og $n \geq 1$) betegnes med
$\mathrm{Mat}_n(R)$ mængden af $n \times n$-matricer α med koefficienter i R,
$GL_n(R) = \{\alpha \in \mathrm{Mat}_n(R) \mid \det(\alpha) \in R^*\}$ (generelle lineære gruppe)
$SL_n(R) = \{\alpha \in \mathrm{Mat}_n(R) \mid \det(\alpha) = 1\}$. (specielle lineære gruppe)
$T_n(R) = \{\alpha \in \mathrm{Mat}_n(R) \mid \alpha$ er en øvre trekantsmatrix$\}$
$T_n^*(R) = \{\alpha \in \mathrm{Mat}_n(R) \mid \alpha \in T_n(L) \wedge \det(\alpha) \in R^*\}$.
Besvar spørgsmål svarende til opgave 1 for nogle af mængderne
$\mathrm{Mat}_n(R)$, $GL_n(R)$, $SL_n(R)$ $T_n(R)$, $T_n^*(R)$, $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
og nogle af afbildningerne
$\alpha \mapsto \bar{\alpha}$, $\alpha \mapsto \det(\alpha)$, $\alpha \mapsto \alpha^t$ ("transponering af α").

3(i) Vis, at matricerne af formen $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$, $t \in \mathbb{Z}$, udgør en undergruppe af $SL_2(\mathbb{Z})$, og bestem en "pæn" gruppe, som denne undergruppe er isomorf med.

(ii) Vis, at matricen $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$ har endelig orden og angiv denne orden.

4. Lad $c > 0$ og lad I_c betegne intervallet $I_c =]-c, c[$. Vis, at

$$v_1 * v_2 = \frac{v_1 + v_2}{1 + v_1 v_2 / c^2}$$

definerer en gruppekomposition i I_c.

Algebra 1984

Opgaver 12
("Grupper")

1. (i) Vis, at afbildningerne $: \mathbb{R} \to \mathbb{R}$ af formen
$$f_{a,b} : t \mapsto at + b, \quad a \in \mathbb{R}^*, b \in \mathbb{R}$$
er bijektive og at de udgør en undergruppe $(A, \circ)$ af $\mathrm{Aut}(\mathbb{R})$.

(ii) Vis, at matricerne
$$g_{a,b} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \quad a \in \mathbb{R}^*, \ b \in \mathbb{R},$$
er invertible og at de udgør en undergruppe $(B, \cdot)$ af $GL_2(\mathbb{R})$.

(iii) Vis, at $(A, \circ)$ og $(B, \cdot)$ er isomorfe.

2. Lad $c > 0$. Vis at matricerne af formen
$$\begin{pmatrix} \cosh t & -c \sinh t \\ -\sinh t & c \cosh t \end{pmatrix}, \quad t \in \mathbb{R}$$
udgør en undergruppe i $GL_2(\mathbb{R})$, og at denne undergruppe er isomorf med $(\mathbb{R}, +)$.

3. Sæt $\mathbb{U} = \{ u \in \mathbb{C} \mid |u| = 1 \}$.

(i) Vis, at $\mathbb{U}$ er en undergruppe i den multiplikative gruppe $\mathbb{C}^*$.

(ii) Vis, at $u = \cos 10^\circ + i \sin 10^\circ \in \mathbb{U}$, og at u har endelig orden i $\mathbb{U}$. Bestem denne orden.

(iii) Bestem delmængden $A := \{ u \in \mathbb{C}^* \mid u \text{ har endelig orden} \}$, og vis, at $A \subseteq \mathbb{U}$.

(iv) Vis, at A er en undergruppe i $\mathbb{U}$.

(v) Vis, at A er uendelig. Er $A = \mathbb{U}$?

4. En undergruppe H i $(\mathbb{R}, +)$ kaldes <u>diskret</u>, hvis der findes et $\varepsilon > 0$, så at $H \cap \{ x \in \mathbb{R} \mid |x| < \varepsilon \} = \{0\}$.

(i) Vis, at enhver ikke-diskret undergruppe H er <u>tæt</u> i $\mathbb{R}$; dvs at ethvert interval af længde > 0 indeholder elementer fra H.

(ii) Vis, at enhver diskret undergruppe $\neq \{0\}$ er isomorf med $\mathbb{Z}$.

(iii) Lad $f : \mathbb{R} \to \mathbb{R}$ være en afbildning. Et tal $h \in \mathbb{R}$ kaldes en <u>periode</u> for f, hvis $f(x + h) = f(x)$ for alle $x \in \mathbb{R}$. Har dette noget at gøre med undergrupper i $(\mathbb{R}, +)$?

Algebra 1984

Opgaver 13
("Grupper")

1. Lad G_1 og G_2 være grupper. (i) Vis, at produktmængden $G_1 \times G_2$ med kompositionen

$$(x_1, x_2) \cdot (y_1, y_2) := (x_1 y_1, x_2 y_2).$$

organiseres til en gruppe.

(ii) Vis, at "projektionen" : $(x_1, x_2) \mapsto x_1$ er en surjektiv gruppehomomorfi : $G_1 \times G_2 \longrightarrow G_1$, og bestem kernen.

(iii) Vis, at $x \mapsto (x, e_2)$, hvor e_2 er neutralt element i G_2 definerer en injektiv gruppehomomorfi : $G_1 \longrightarrow G_1 \times G_2$.

2. Lad H og K være undergrupper i G. Vis, at $H \cup K$ kun er en undergruppe, når $H \subseteq K$ eller $K \subseteq H$.

3. Lad G være en gruppe. (i) Vis, at en vilkårlig fællesmængde af (normale) undergrupper i G selv er en (normal) undergruppe.

(ii) Slut, at der for enhver delmængde $P \subseteq G$ findes en mindste undergruppe, som indeholder P. Den kaldes undergruppen frembragt af P og betegnes $\langle P \rangle$.

(iii) Prøv at beskrive elementerne i $\langle P \rangle$.

4. Lad $G = \mathbb{Q}^*$ betegne den multiplikative gruppe af rationale tal $\neq 0$.

(i) Beskriv for en given mængde P af primtal undergruppen $\langle P \rangle \subseteq \mathbb{Q}^*$.

(ii) Vis, at hvis P og Q er forskellige mængder af primtal, så er $\langle P \rangle \neq \langle Q \rangle$.

(iii) Vis, at mængden af undergrupper i $\mathbb{Q}^*$ er ækvipotent med $\mathbb{R}$.

5. Lad G være en gruppe. (i) Hvornår er afbildningen $x \mapsto x^{-1}$ en homomorfi : $G \to G$?

(ii) Vis, at hvis alle elementer $\neq e$ har orden 2, så er G kommutativ.

6. Lad H være en undergruppe af index 2 i gruppen G. Vis, at H er normal.

Algebra 1984

Opgaver 14
("Grupper")

1. Lad G være en endelig gruppe.
   (i) Vis, at antallet af elementer af orden 2 i G er lige eller ulige eftersom $|G|$ er ulige eller lige.
   (ii) Vis, at en gruppe af lige orden indeholder et element af orden 2.
   (iii) Vis, at hvis G er kommutativ, så er produktet af alle elementer af orden $\neq 2$ lig med det neutrale element.

2. Lad G være en gruppe.
   (i) Vis, at der for hvert element $g \in G$ gælder, at $C(g) := \{x \in G \mid xg = gx\}$ er en undergruppe. (Centralisatoren for g).
   (ii) Vis, at hvis $g \in G$ har orden n, så er n divisor i $|C(g)|$.

3. Lad G være en gruppe.
   (i) Vis, at der for hver delmængde $P \subseteq G$ gælder, at $N(P) := \{x \in G \mid xPx^{-1} = P\}$ er en undergruppe (Normalisatoren for P).
   (ii) Vis, at hvis $H \subseteq G$ er en undergruppe, så er $H \subseteq N(H)$ og H er en normal undergruppe af $N(H)$. Hvornår er $N(H) = G$?

4. Lad G være en gruppe. (i) Vis, at $Z(G) = \{x \in G \mid \forall g \in G : gx = xg\}$ er en undergruppe i G (Gruppens centrum). Hvornår er $Z(G) = G$?
   (ii) Vis, at $Z(G)$ er en normal undergruppe.

5. Lad G være en gruppe og lad H og K være undergrupper.
   (i) Vis, at hvis $H \subseteq K$, så er $|G : H| = |G : K| \cdot |K : H|$.
   (ii) Vis, at $|G : H \cap K| = |G : H|\,|H : H \cap K|$.
   (iii) Vis, at $|G : H \cap K| \leq |G : H| \cdot |G : K|$ [Vink: Søg en injektiv afbildning: $G/H \cap K \to G/H \times G/K$]
   (iv) Vis, at hvis en af undergrupperne H og K er normal, så er $HK = \{hk \mid h \in H \wedge k \in K\}$ en undergruppe, $HK = KH$ og $|HK : H| = |K : K \cap H|$.

Algebra 1984

Opgaver 15
("Grupper")

1. Gruppen S_3 består af permutationerne $t_1 = (2,3)$, $t_2 = (3,1)$, $t_3 = (1,2)$, $s_1 = (1,2,3)$, $s_2 = (1,3,2)$ samt identiteten e. Opskriv kompositionstavlen.

2. I $\mathbb{R}^2$ med den kanoniske basis e_1, e_2 fortolkes vektorerne i $X := \{e_1, e_2, -e_1, -e_2\}$ som hjørnerne i et kvadrat (tegn!).
(i) Vis, at $D_4 := \{\alpha \in GL_2(\mathbb{R}) \mid \alpha(X) = X\}$ er en undergruppe af orden 8 i $GL_2(\mathbb{R})$. Beskriv elementerne i D_4, dels som matricer, dels geometrisk som afbildninger: $\mathbb{R}^2 \to \mathbb{R}^2$.
(ii) Vis, at $\alpha \mapsto \det(\alpha)$ definerer en gruppehomomorfi: $D_4 \to \mathbb{R}^*$, bestem billedet og vis, at kernen er den cykliske gruppe C_4 af orden 4.
[D_4 er <u>diedergruppen</u> af grad 4]

3. Generaliser resultatet fra opgave 2 til tilfældet, hvor $X \subseteq \mathbb{R}^2$ består af hjørnerne i en regulær n-kant ($n \geq 3$).
(i) Vis, at den tilhørende gruppe D_n har orden $2n$ og at den har C_n som normal undergruppe med $D_n / C_n \simeq C_2$.
[D_n er <u>diedergruppen</u> af grad n]
(ii) Find en isomorfi: $D_3 \xrightarrow{\sim} S_3$.

4. Betragt i $Mat_2(\mathbb{C})$ matricerne $\underline{\underline{i}} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $\underline{\underline{j}} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\underline{\underline{k}} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, $\underline{\underline{1}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
(i) Udregn produkterne $\underline{\underline{i}}^2$, $\underline{\underline{j}}^2$, $\underline{\underline{k}}^2$, $\underline{\underline{i}}\,\underline{\underline{j}}$, $\underline{\underline{j}}\,\underline{\underline{k}}$, $\underline{\underline{k}}\,\underline{\underline{i}}$ og vis, at
$$Q := \{\pm \underline{\underline{1}}, \pm \underline{\underline{i}}, \pm \underline{\underline{j}}, \pm \underline{\underline{k}}\}$$
er en undergruppe af orden 8 i $SL_2(\mathbb{C})$ [<u>kvaterniongruppen</u>]
(ii) Vis, at Q og D_4 ikke er isomorfe.

5. Vis, at de ved $\tau(z) := \bar{z}$ og $\delta(z) := iz$ definerede afbildninger $: \mathbb{C} \to \mathbb{C}$ er bijektive, og at de i $Aut(\mathbb{C})$ frembringer en undergruppe isomorf med D_4.

6. Vis, idet $T := \mathbb{R} \setminus \{0,1\}$, at de ved $f_1(t) = t$, $f_2(t) = 1/t$, $f_3(t) = 1-t$, $f_4(t) = \frac{1}{1-t}$, $f_5(t) = \frac{t-1}{t}$, $f_6(t) = \frac{t}{t-1}$ afbildninger udgør en undergruppe $\simeq S_3$ af $Aut(T)$.

Algebra 1984

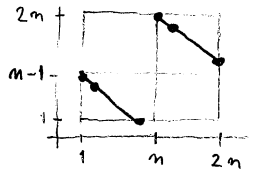
Opgaver 16
("Grupper")

1. Følgende er en tabel over en permutation $\sigma \in S_{13}$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 8 & 10 & 9 & 4 & 12 & 11 & 5 & 13 & 3 & 2 & 7 & 6 & 1 \end{pmatrix}.$$

Skriv σ som produkt af disjunkte cykler og bestem $\operatorname{sign}(\sigma)$.

2. Følgende antyder grafen for en permutation $\sigma \in S_{2n}$:



Skriv σ som produkt af disjunkte cykler og bestem $\operatorname{sign}(\sigma)$.

3. Lad $\tau \in \mathrm{Aut}(X)$ være en p-cykel. Hvad kan siges om τ^2?

4. Lad $\sigma \in S_n$. (i) Vis, at kvadratet σ^2 er en lige permutation.
(ii) Gælder der omvendt, at enhver lige permutation er et kvadrat?

5. (i) Vis, at der for enhver fremstilling af $\sigma \in S_n$ som produkt af q transpositioner gælder $q \geq z(\sigma)$.
(ii) Vis at der for enhver permutation $\sigma \in S_n$ gælder $z(\sigma) \leq n-1$, og afgør, hvornår $z(\sigma) = n-1$.

6. (i) Vis, at der for en undergruppe $H \leq G$ af indeks 2 gælder $g^2 \in H$ for $g \in G$.
(ii) Vis, at $A_n \leq S_n$ $(n \geq 2)$ er den eneste undergruppe af indeks 2.
(iii) Vis, at sign er den eneste ikke-trivielle homomorfi: $S_n \to \{\pm 1\}$, $n \geq 2$.

7. Lad $\sigma \in S_n$. Udfra en tabelfremstilling $\sigma = \begin{pmatrix} x_1 & \cdots & x_n \\ y_1 & \cdots & y_n \end{pmatrix}$ defineres tallet $s(\sigma)$ ved $s(\sigma) = \prod_{1 \leq i < j \leq n} \frac{x_i - x_j}{y_i - y_j}$.
(i) Vis, at $s(\sigma) = \pm 1$ [Vink: vis, at $s(\sigma) \in \mathbb{Q}^*$ og at $|s(\sigma)| = 1$].
(ii) Vis, at $s(\sigma) = (-1)^{I(\sigma)}$, hvor $I(\sigma)$ er antallet af par (a,b), $1 \leq a \leq n$, $1 \leq b \leq n$ med $a < b$ og $\sigma(a) > \sigma(b)$.
(iii) Slut, at $s(\sigma)$ ikke afhænger af rækkefølgen i tabelfremstillingen, og dernæst, at $s(\sigma\tau) = s(\sigma)s(\tau)$, $\sigma, \tau \in S_n$.
(iv) Vis, at $s(\sigma) = \operatorname{sign}(\sigma)$.

Algebra 1984

Opgaver 17
("Grupper")

1. Diedergruppen D_4 virker naturligt på $\mathbb{R}^2$. Bestem for hvert af punkterne $(1,0)$ $(1,1)$ og $(1,2)$ den tilhørende bane og isotropigruppe. Hvilke punkter i $\mathbb{R}^2$ er fixpunkter?

2. Gruppen $O_2(\mathbb{R})$ består af de automorfier $: \mathbb{R}^2 \to \mathbb{R}^2$, der enten er en drejning om $(0,0)$ eller en spejling i en linie gennem $(0,0)$. Angiv baner og isotropigrupper.

3. Gruppen S_n virker på $\mathbb{R}^n$ ved permutation af koordinaterne. Angiv nogle isotropigrupper. Hvilke elementer i $\mathbb{R}^n$ er fixe?

4. En virkning af en gruppe G på en mængde X kaldes <u>transitiv</u>, hvis der kun er én bane. Vis, at der i så fald gælder, at antallet af fixpunktsfri elementer $g \in G$ er $\geq |X| - 1$.

5. (i) Lad $a_{p,n}$ betegne antallet af permutationer $\sigma \in S_n$ med præcis p fixpunkter. Vis, at $\sum_{p=0}^{n} p\, a_{p,n} = n!$
(ii) Bestem antallet $a_{0,n}$ af fixpunktfri permutationer i S_n og undersøg om $\lim_{n\to\infty} \frac{a_{0,n}}{n!}$ eksisterer.

6. En klassedeling af en mængde X med n elementer siges at være af <u>type</u> $(m_1, m_2, \ldots)$ hvis den indeholder m_1 klasser med 1 element, m_2 klasser med 2 elementer o.s.v. Vis, at antallet af klassedelinger af en given type $(m_1, m_2, \ldots)$ er lig

$$\frac{n!}{m_1! \cdot m_2! (2!)^{m_2} \cdot m_3! \cdot (3!)^{m_3} \cdot \ldots}$$

7. Vis, at mængden $\{1,2,3,4\}$ på netop 3 måder kan deles i 2 lige store delmængder. Gruppen S_4 virker på $\{1,2,3,4\}$ og dermed også på mængden bestående af de 3 delinger. Angiv de permutationer, der virker trivielt.

Algebra 1984

Opgaver 18*
("Grupper")

1. Lad G være en ikke-kommutativ gruppe med centrum $Z(G)$. Vis, at $G/Z(G)$ ikke kan være cyklisk.

2. Lad p være et primtal.
(i) Vis, at enhver <u>p-gruppe</u> G, dvs en gruppe, hvis orden er en potens af p, har $Z(G) \supset \{e\}$.
(ii) Vis, at enhver gruppe af orden p^2 er kommutativ.

3. Angiv centralisatorerne $C(g)$ for elementerne g i
(i) gruppen S_3 (ii) Diedergruppen D_4.

4. I fremstillingen $\sigma = c_1 \cdots c_r$ af en permutation $\sigma \in S_n$ som produkt af disjunkte cykler (1-cykler medregnet) antages at cyklerne har indbyrdes forskellige længder $p_1, \ldots, p_r$. Vis, at $C(g) = \langle c_1, \ldots, c_r \rangle$, og at denne gruppe er isomorf med $\mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r\mathbb{Z}$.

5. Lad $\sigma \in S_n$ være en p-cykel. Bestem $C(\sigma)$, og vis $|C(\sigma)| = (n-p)!\,p$.

6. Lad $\sigma = (x_1, \ldots, x_p)(y_1, \ldots, y_p)$ være et produkt af 2 disjunkte p-cykler. Vis, at permutationen $(x_1, y_1) \cdots (x_p, y_p) \in C(\sigma)$.

7. Vis, at antallet af permutationer i S_n af type $(m_1, m_2, \ldots)$ (hvor altså $\sum p m_p = n$) er lig $\dfrac{n!}{1! \cdot m_1! \cdot 2! m_2! \cdot 3! m_3! \cdot \ldots}$

8. (i) Lad $\sigma \in S_n$ være af type $(m_1, m_2, \ldots)$. Vis, at

$$C(\sigma) \subseteq A_n \iff m_i \text{ er } \begin{cases} = 0 & \text{når } i \text{ er lige} \\ \leq 1 & \text{når } i \text{ er ulige} \end{cases}, \quad i = 1, 2, \ldots$$

(ii) Der er en forbindelse mellem cykeltyper og konjugeretklasser i A_n. Hvilken?

(iii) Hvilke konjugeretklasser har A_5? Angiv deres elementantal.

Algebra 1984 — Opgaver 19 ("Grupper")

1. (i) Vis, at en undergruppe N i en gruppe G er normal, hvis og kun hvis den er en forening af konjugeretklasser.
(ii) En undergruppe N har en ordn, der er divisor i G's ordn, og den indeholder konjugeretklassen $\{1\}$. Overvej, at dette lægger bånd på hvilke foreningsmængder af konjugeretklasser, der kan være undergrupper, og bestem alle normale undergrupper i D_4, Q og S_4.

2. Vis, at A_5 er en <u>simpel</u> gruppe, dvs at $\{1\}$ og A_5 er de eneste normale undergrupper.

3. Gruppen G virker på sig selv ved konjugering og dermed også på mængden $\mathcal{P} = \mathcal{P}(G)$ af alle delmængder af G.
(i) Vis, at for hvert element $P \in \mathcal{P}$ (dvs $P \subseteq G$) er isotropigruppen netop <u>normalisatoren</u> $N(P) = \{g \in G \mid gPg^{-1} = G\}$, og at antallet af delmængder konjugerede med P er $|G : N(P)|$.
(ii) Vis, at mængden af undergrupper i G er en stabil delmængde af $\mathcal{P}$.
(iii) Vis, når $H \subseteq G$ er en undergruppe, at $N(H) \supseteq H$, og at antallet af undergrupper konjugerede med H er divisor i $|G:H|$.

4. Lad G virke på X, lad $x \in X$ og lad $H \subseteq G$ være isotropigruppen for x. Vis, at isotropigrupperne for de øvrige elementer i banen $G.x$ netop er undergrupperne konjugerede med H.

5. Lad G være en gruppe. Automorfier i G af formen $x \mapsto gxg^{-1}$ med $g \in G$, kaldes <u>indre</u> automorfier.
(i) Konjugering giver repræsentationen $: G \to Aut(G)$. Vis, at billedet netop er undergruppen $Aut_i(G)$ af indre automorfier i G og bestem repræsentationens kerne.
(ii) Lad $Aut_{gr}(G)$ betegne mængden af gruppeautomorfier i G. Vis, at $Aut_{gr}(G)$ er en undergruppe af $Aut(G)$, og at $Aut_i(G)$ er en normal undergruppe i $Aut_{gr}(G)$.

Algebra 1984

Opgaver 20
("grupper")

1. Gruppen G af ordnen n virker på sig selv ved translation og derfor også på mængden $\mathcal{P} = \mathcal{P}(G)$ af alle delmængder af G.
(i) Vis, at et element $P \in \mathcal{P}$ er en venstresideklasse, hvis og kun hvis det er en højresideklasse og vis, at delmængden $\mathcal{S} \subseteq \mathcal{P}$ bestående af sideklasser er en stabil delmængde.
(ii) Vis, at banen for en undergruppe H er mængden G/H af venstresideklasser. Hvad er isotropigruppen for en venstre sideklasse xH.
(iii) Vis for hvert d, at delmængderne $\mathcal{P}_d = \{P \in \mathcal{P} \mid |P| = d\}$ og $\mathcal{S}_d = \mathcal{P}_d \cap \mathcal{S}$ er stabile delmængder.
(iv) Vis, at hvis $n = ad$, så er $|\mathcal{S}_d| = a \cdot ug(d)$, hvor $ug(d)$ betegner antallet af undergrupper i G af ordnen d.
(v) Lad ${}_pG$ være isotropigruppen for et element $P \in \mathcal{P}$. Vis, at der for alle $x \in \mathcal{P}$ gælder ${}_pG \cdot x \subseteq P$ og slut heraf at P er en forening af højresideklasser modulo ${}_pG$ og specielt, at $|{}_pG|$ er divisor i $|P|$.
(vi) Vis, at $P \in \mathcal{P}$ er en sideklasse, hvis og kun hvis $|{}_pG| = |P|$ og slut heraf når $n = ad$: $\mathcal{P}_d \setminus \mathcal{S}_d$ er en foreningsmængde af baner B_i, hvis elementantal har formen $|B_i| = ad_i$, hvor $d_i \mid d$ og $d_i > 1$.
(vii) Udled formlen $\binom{n-1}{d-1} = \sum d_i + ug(d)$, hvor $d_i \mid d$, $d_i > 1$ og vis herved Sylows 1. sætning: Hvis divisoren d i $|G|$ er en potens af et primtal p, så er $ug(d) \equiv 1 \bmod p$.

2.* Betragt restriktionen til en undergruppe K af den i opg. 1 beskrevne virkning af G på G/H.
(i) Hvornår er en sideklassen xH invariant under virkningen af K.
(ii) Vis, at hvis K er en p-gruppe, så er $|N(K,H)| = |\{g \in G \mid gKg^{-1} \subseteq H\}|$ deleligt med $|H|$ og $|N(K,H)|/|H| \equiv |G:H| \bmod p$.
(iii) Hvad følger heraf, hvis $p \nmid |G:H|$, specielt hvis H er en Sylow-p-undergruppe, dvs en p-gruppe med $p \nmid |G:H|$?

Algebra 1984 Opgaver 21
("Ringe")

1. AT påstår, at der findes en ring med 4 elementer 0, 1, a, b, hvori 0 = nul-element 1 = ét-element, $1+1=0$, $a^2=a$.
(i) Bestem kompositionstavlerne for + og ·.
(ii) Har AT ret?
(iii) Løs de samme spørgsmål når $a^2=a$ ændres til $a^2=b$.

2. Vis, at mængden $\mathbb{H} := \left\{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \mid z, w \in \mathbb{C} \right\}$ er en delring af $\mathrm{Mat}_2(\mathbb{C})$. Vis, at $\mathbb{H}$ er et skævlegeme. [Elementerne i $\mathbb{H}$ kaldes kvaternioner]. Vis, at kvaternion-gruppen Q af orden 8 er undergruppe i $\mathbb{H}^*$.

3. (i) Hvilken orden har ringen $\mathrm{Mat}_2(\mathbb{F}_2)$? Og grupperne $GL_2(\mathbb{F}_2)$ og $SL_2(\mathbb{F}_2)$.
(ii) Samme spørgsmål når legemet erstattes med $\mathbb{F}_3$.

4. Vis, at en matrix $\alpha \in \mathrm{Mat}_n(\mathbb{R})$ er "Mat 1 LD - regulær", netop når den er "Mat 2 AL - regulær". [Vink: Udnyt, at $\xi \mapsto \alpha\xi$ er en lineær afbildning : $\mathrm{Mat}_n(\mathbb{R}) \to \mathrm{Mat}_n(\mathbb{R})$].

5. Overvej, at en endelig ring Λ, hvis karakteristik er et primtal p, kan opfattes som vektorrum over legemet $\mathbb{F}_p$. Slut heraf, at $|\Lambda|$ er en potens af p. Hvor mange ringe findes der med 6 elementer?

6. En af ringene fra opgave 1 er et legeme. Hvilken?

7. Vis, at enhver ringhomomorfi : $\Lambda \to \Gamma$ inducerer en gruppehomomorfi : $\Lambda^* \to \Gamma^*$

8. Hvilken orden har gruppen $\mathbb{F}_{17}^*$? Vis, at $\mathbb{F}_{17}^*$ er cyklisk.

9. Lad p være et primtal. Vis, at der for elementer λ, μ med $\lambda\mu = \mu\lambda$ i en ring af karakteristik p gælder:

$$(\lambda+\mu)^p = \lambda^p + \mu^p.$$

Algebra 1984

Opgaver 22
("Ringe")

1. Divider med rest

$X^4 + 3X^3 + 2X^2 + X + 1$	med	X^2+1	i $\mathbb{Z}[X]$
$X^4 + 4$	"	X^2+2X+2	i $\mathbb{Z}[X]$
$X^n - 1$	"	$X - 1$	i $\mathbb{Z}[X]$
X^2	"	$X+2X+2$	i $\mathbb{Z}/4\,[X]$

2. Bestem for polynomiet $X^5+X^4+X^2+X \in \mathbb{F}_2[X]$ den i "Ringe" 2.7 nævnte fremstilling.

3. Vis, at polynomiet $X^3+X+1 \in \mathbb{F}_7[X]$ ikke har rødder.

4. Vis, at polynomiet $X^2+1 \in \mathbb{Z}/65\,[X]$ har 4 rødder.

5. Lad R være ringen af alle afbildninger $\varphi : \mathbb{N} \to \mathbb{R}$. Hvor mange rødder har polynomiet $X^2 - X \in R[X]$.

6. Lad $R \subseteq S$ være kommutative ringe. Lad $\varphi \in S[X]$ og lad $d \in R[X]$ være normeret.
(i) Vis, at $d\varphi \in R[X] \Rightarrow \varphi \in R[X]$.
(ii) Kan man droppe forudsætningen om at d er normeret?

7. For $\alpha \in L$, hvor L er et legeme skrives $\operatorname{ord}(\alpha) = n$, hvis $\alpha \neq 0$ og α har (endelig) orden n i gruppen L^*. Det n-te <u>cirkeldelingspolynomium</u> $\Phi_n \in \mathbb{C}[X]$ er polynomiet

$$\Phi_n = \prod_{\operatorname{ord}\zeta = n} (X - \zeta).$$

(i) Vis, at $\Phi_1 = X-1$, $\Phi_2 = X+1$, $\Phi_3 = X^2+X+1$, $\Phi_4 = X^2+1$, $\Phi_5 = X^4+X^3+X^2+X+1$, $\Phi_6 = X^2-X+1$, og bestem Φ_{15}.

(ii) Vis, at $X^n - 1 = \prod_{d/n} \Phi_d$

og vis derefter, at $\Phi_n \in \mathbb{Z}[X]$.

(iii) Vis, at Φ_n's konstantled er $= \begin{cases} -1 & \text{når } n = 1 \\ 1 & \text{når } n > 1. \end{cases}$

Algebra 1984 — Opgaver 23 ("Ringe")

1. Lad L være et legeme af karakteristik p ($=0$ eller et primtal). Det n-te cirkeldelingspolynomium Φ_n har koefficienter i $\mathbb{Z}$ og kan derfor opfattes som polynomium $\Phi_n \in L[X]$. Vis, at hvis $p \nmid n$, så gælder for $\alpha \in L$:

$$\operatorname{ord}(\alpha) = n \iff \Phi_n(\alpha) = 0.$$

[Vink: Udnyt, at $X^n - 1 = \prod_{d \mid n} \Phi_d$; pas på multible rødder!]

2. Lad L være et legeme af karakteristik p ($= 0$ eller et primtal), og lad G være en endelig undergruppe af L^*. (i) Vis, at

$$\prod_{\alpha \in G} (X - \alpha) = X^n - 1, \quad n = |G|.$$

(ii) Slut heraf, at G er cyklisk og at $p \nmid |G|$. [Brug opgave 1.]

(iii) Vis, når legemet L er endeligt, at L^* er cyklisk.

3. Sæt $\Lambda = \mathbb{F}_2[X]/(X^3 + X + 1)$, $\xi = \textcircled{X} \in \Lambda$.

(i) Begrund, at Λ er en ring med 8 elementer.

(ii) Bestem (dvs skriv på formen $r_0 + r_1\xi + r_2\xi^2$, $r_0, r_1, r_2 \in \mathbb{F}_2$) potenserne ξ^i, $i \in \mathbb{N}$.

(iii) Vis, at Λ er et legeme.

4. For et legeme L betragtes $\Lambda = L[X]/(X^2 + 1)$.

(i) Vis, at Λ er et legeme, når $L = \mathbb{R}$ og når $L = \mathbb{F}_3$.

(ii) Vis, at Λ ikke er et legeme, når $L = \mathbb{C}$ og når $L = \mathbb{F}_5$.

5. For et legeme et legeme L betragtes ringen $\Lambda = L[X]/(X^2)$, $\varepsilon := \textcircled{X}$. Vis, at der for hvert polynomium $f \in L[X]$ og $a \in L$ gælder

$$f(a + \varepsilon) = f(a) + f'(a)\varepsilon.$$

Algebra 1984 — Opgaver 24 ("Idealer")

1. Lad $R = \mathcal{C}([0,1])$ betegne ringen af kontinuerte funktioner $\varphi : [0,1] \to \mathbb{R}$. For hvert $a \in [0,1]$ sættes

$$I_a = \{\varphi \in R \mid \varphi(a) = 0\}.$$

$$J_a = \{\varphi \in R \mid \exists \text{ omegn } U \text{ af } a \text{ så at } \varphi(t) = 0 \text{ for } t \in U\}.$$

(i) Vis, at I_a og J_a er idealer i R.

(ii) Vis, at idealet J_a ikke er endeligt frembragt.

(iii) Vis, at når $a, b \in [0,1]$, $a \neq b$, så er $J_a + J_b = R$.

(iv) Angiv fællesmængden $\bigcap_{a \in [0,1] \cap \mathbb{Q}} I_a$

(v)* Vis, at idealet I_a ikke er endeligt frembragt.

2. Lad p være et primtal, og betragt idealet $(p, X) \subseteq \mathbb{Z}[X]$.

(i) Vis, at (p, X) består af de polynomier $a_0 + a_1 X + \cdots + a_n X^n$ for hvilke $p \mid a_0$.

(ii) Vis, at (p, X) ikke er et hovedideal.

3. Lad $R \subseteq \mathbb{Q}[X]$ være delmængden bestående af polynomier $a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Q}[X]$, for hvilke $a_0 \in \mathbb{Z}$.

(i) Vis, at R er en delring af $\mathbb{Q}[X]$.

(ii) Vis, at den ovn hovedidealerne $\mathfrak{a}_n = R \frac{1}{n!} X$ gælder

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$$

(iii) Vis, at R ikke er en hovedidealring.

(iv) Vis ved et eksempel at den ved $p \mapsto \text{grad}(p)$ definerede funktion $: R \to \mathbb{Z}$ ikke opfylder det krav, der stilles i "den numeriske betingelse".

4. Lad p være et primtal og lad $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$ være delmængden $\mathbb{Z}_{(p)} := \{ a/s \mid a, s \in \mathbb{Z},\ p \nmid s \}$.

(i) Vis, at $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$ er en delring.

(ii) Vis, at den ovn hovedidealerne $\mathfrak{a}_n = \mathbb{Z}_{(p)} p^n$ gælder

$$\mathbb{Z}_{(p)} = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots .$$

(iii) Vis, at idealerne $\mathfrak{a}_n$ samt (0) er samtlige idealer i $\mathbb{Z}_{(p)}$.

Algebra 1984 — Opgaver 25 ("Idealer")

1. Lad $R = \mathcal{C}([0,1])$ være ringen af kontinuerte funktioner $\varphi : [0,1] \to \mathbb{R}$ og lad $a \in [0,1]$.
(i) Vis, at $I_a = \{\varphi \in R \mid \varphi(a) = 0\}$ er et maksimalideal og bestem kvotienten R/I_a.
(ii) Er $J_a = \{\varphi \in R \mid \varphi = 0$ i en omegn af $a\}$ et maksimalideal? Er det et primideal?
(iii)* Vis, at ethvert maksimalideal i R har formen I_a med $a \in [0,1]$.

2. Lad p være et primtal. I $\mathbb{Z}[X]$ betragtes idealerne $(0), (X), (p), (p,X)$.
(i) Vis, at disse idealer er primidealer og bestem de tilhørende kvotienter.
(ii) Hvilke af idealerne var maksimalidealer.

3. Lad K være et legeme. For elementer $a, s \in K$ med $s \neq 0$ skrives $a/s = a s^{-1} \in K$. Lad $R \subseteq K$ være en delring og lad $\mathfrak{p} \subset R$ være et primideal.
(i) Vis, at R er et integritetsområde.
(ii) Vis, at $R_{\mathfrak{p}} := \{a/s \mid a \in R \wedge s \in R \setminus \mathfrak{p}\}$ er en delring af K og at $R \subseteq R_{\mathfrak{p}}$.
(iii) Vis, at $m_{\mathfrak{p}} := \{a/s \mid a \in \mathfrak{p} \wedge s \in R \setminus \mathfrak{p}\}$ er et maksimalideal i $R_{\mathfrak{p}}$.
(iv) Vis, at $m_{\mathfrak{p}}$ er det eneste maksimalideal i $R_{\mathfrak{p}}$
(v) Vis, at $R_{\mathfrak{p}}$ er et legeme, hvis og kun hvis $\mathfrak{p} = (0) \subset R$.
[Legemet $R_{(0)} \subseteq K$ kaldes <u>brøklegemet</u> for R]

4. Lad p være et primtal og betragt i $\mathbb{Z}_{(p)}[X]$ hovedidealet $(pX-1)$. Find en isomorfi $\mathbb{Z}_{(p)}[X]/(pX-1) \cong \mathbb{Q}$.

5.* Lad L være et endeligt legeme. Vis, at der i $\mathbb{Z}[X]$ findes et maksimalideal m og en isomorfi $\mathbb{Z}[X]/m \cong L$.
[Vink. Udnyt f.eks. at L^* er cyklisk].

Algebra 1984 — Opgaver 26 ("Ideale")

1. (i) Hvor mange normerede polynomier af grad ≤ 4 findes der i $\mathbb{F}_2[X]$?
(ii) Hvilke af disse polynomier er irreducible.

2. Samme spørgsmål som opgave 1 når legemet er $\mathbb{F}_3$, og graden ≤ 3.

3. Lad p være et primtal og lad $f \in \mathbb{F}_p[X]$ være et (normeret) irreducibelt polynomium af grad $n \geq 1$. Vis, at $\Lambda = \mathbb{F}_p[X]/(f)$ er et legeme med p^n elementer.

4. Lad Λ være et endeligt legeme. Som bekendt er da karakteristikken af Λ et primtal p og elementantallet q i Λ er en potens $q = p^n$. Videre er Λ^* en cyklisk gruppe. Lad $\xi \in \Lambda^*$ være en frembringer. Vis, at $\{ g \in \mathbb{F}_p[X] \mid g(\xi) = 0 \}$ er et hovedideal i $\mathbb{F}_p[X]$ frembragt af et (normeret) irreducibelt polynomium af grad n, og angiv en isomorfi: $\mathbb{F}_p[X]/(f) \xrightarrow{\sim} \Lambda$.

5.* Lad $q = p^m$ være en potens af et primtal p.
(i) Lad L være et legeme af karakteristik p. Vis, at delmængden $\{\alpha \in L \mid \alpha^q = \alpha\}$ højst har q elementer og at den er et dellegeme i L [Vink: I karakteristik p er $(\alpha+\beta)^p = \alpha^p + \beta^p$].
(ii) Cirkeldelingspolynomiet Φ_{q-1} har koefficienter i $\mathbb{Z}$ og kan derfor betragtes i $\mathbb{F}_p[X]$. Lad $f \in \mathbb{F}_p[X]$ være en irreducibel divisor i Φ_{q-1}, og sæt $\Lambda = \mathbb{F}_p[X]/(f)$, $\xi = \overline{X}$. Vis, at $\Phi_{q-1}(\xi) = 0$ og dermed at ξ har ordnen $q-1$ i Λ^*. Slut heraf, at Λ er et legeme med q elementer, og at $\operatorname{grad}(f) = n$.
(iii) Vis, at ethvert legeme med q elementer er $\simeq \Lambda$.

6.* Vis, at antallet af irreducible polynomier af grad n i $\mathbb{F}_p[X]$ er $\geq \dfrac{\varphi(p^n-1)}{n}$.

Algebra 1984 — Opgaver 27 ("Idealer")

1. Lad L være et legeme og lad $R \subseteq L[X]$ være mængden af polynomier uden førstegradsled dvs
$$R = \{a_0 + a_1 X + \cdots + a_n X^n \in L[X] \mid a_1 = 0\}.$$
(i) Vis, at R er en delring og bestem enhederne i R.
(ii) Vis, at hvert element $\neq \{0, \text{enhed}\}$ i R har en irreducibel opløsning.
(iii) Vis, at elementerne X^2 og X^3 er irreducible i R.
(iv) Vis, at R ikke er faktoriel.

2. Lad R være en faktoriel ring og lad $p \in R$ være et primelement. For hvert $a \in R$ sættes $v_p(a) =$ "antallet af gange p går op i a". At $v_p(a) = n \in \mathbb{N} \cup \{0\}$ betyder således at $a = p^n a'$, hvor $p \nmid a'$. For $a = 0$ sættes $v_p(0) = +\infty$.
(i) Vis, at der for $a, b \in R$ gælder
(*) $\quad v_p(ab) = v_p(a) + v_p(b)$, $\quad v_p(a+b) \geq \inf\{v_p(a), v_p(b)\}$,
og at "$=$" gælder i uligheden, når $v_p(a) \neq v_p(b)$.
(ii) Vis, idet K betegner brøklegemet for R, at funktionen v_p entydigt kan udvides til en funktion
$$v_p : K \to \mathbb{Z} \cup \{+\infty\},$$
så at (*) bevarer sin gyldighed for alle $a, b \in K$.

3.* Lad R være et hovedidealområde med brøklegeme K, lad der være valgt et repræsentantsystem $\mathcal{P} \subseteq R$ for primelementerne og for hvert $p \in \mathcal{P}$ et repræsentantsystem $\mathcal{A}_p \subseteq R$ for elementerne $\neq 0$ i $R/(p)$.
(i) Hvilke naturlige sådanne valg findes når $R = \mathbb{Z}$ og når $R = L[X]$, L et legeme (spec. $L = \mathbb{R}$ og $L = \mathbb{C}$)?
(ii) Er der givet sådanne repræsentantsystemer kaldes brøker af formen x/p^n, $n \in \mathbb{N}$, $p \in \mathcal{P}$, $x \in \mathcal{A}_p$ for <u>partialbrøker</u>. Vis, at enhver brøk $\alpha \in K$ entydigt kan skrives som sum af et element i R og endelig mange partialbrøker.
[Vink: Antag $v_p(\alpha) = -n < 0$, skriv $\alpha = \frac{a}{b p^n}$, $p \nmid a$, $p \nmid b$, løs ligningen $\textcircled{a} = \textcircled{b}\textcircled{x}$, $x \in \mathcal{A}_p$ og betragt $\alpha - \frac{x}{p^n}$].

Algebra 1984

Opgaver 28
("Idealer")

1. Bestem det mindste tal $d \in \mathbb{N}$ så at ligningen
$$553x - 203y = d$$
har løsninger $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, og angiv for denne værdi af d en løsning $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

2. (i) Bestem største fælles divisor for polynomierne
$$X^4 + X^2 + 1 \quad \text{og} \quad X^3 - 2X^2 + 2X - 1 \quad \text{i } \mathbb{Q}[X]$$
(ii) Samme spørgsmål, idet polynomiernes koefficienter opfattes som elementer i $\mathbb{Z}/3 = \mathbb{F}_3$.

3. Lad R være en faktoriel ring med brøklegeme K. Vis, at hvis et polynomium $p_0 + p_1 X + \cdots + p_n X^n \in R[X]$ har en uforkortelig brøk a/s som rod, så er s divisor i p_n og a er divisor i p_0.

4. Lad R være en faktoriel ring. Et element $a \in R$ kaldes <u>kvadratfrit</u>, hvis det ikke kan skrives på formen $a = bc^2$, hvor $c \neq \{$enhed$\}$.
(i) Vis, at $q \in R$ er <u>kvadratfrit</u>, hvis og kun hvis der for hvert primelement $p \in R$ gælder $p \mid q \Rightarrow p^2 \nmid q$.
(ii) Vis, at hvert element $a \in R$, $a \neq 0$, har en fremstilling
$$a = qc^2,$$
hvor q er kvadratfrit. Er en sådan fremstilling entydig?
(iii) Lad L være et legeme af karakteristik 0. Vis, at et polynomium $f \in L[X]$ er kvadratfrit, netop når f og f' er primiske.

5. Lad R være en faktoriel ring, lad $a, b \in R$, lad d være en største fælles divisor for a og b og lad m være et mindste fælles multiplum for a og b. Vis, at dm er associeret med ab.

Algebra 1984 — Opgaver 29 ("Ideale")

1. Lad $\xi \in \mathbb{C} \setminus \mathbb{Q}$ være rod i $f = X^2 + bX + c \in \mathbb{Z}[X]$. Bestem en isomorfi $\mathbb{Z}[X]/(f) \xrightarrow{\sim} \mathbb{Z}[\xi]$.

2. Lad $\alpha \in \mathbb{C}$ være et (helt) kvadratisk tal. Vis, at
$$D(\alpha) = 0 \iff \alpha \in \mathbb{Z}.$$

3. Lad R være en kvadratisk talring og vælg $\xi \in R$ så at $R = \mathbb{Z}[\xi]$.
(i) For hvilke elementer $\alpha = x + y\xi \in R$ gælder $R = \mathbb{Z}[\alpha]$.
(ii) Vis, at disse elementer α alle har den samme diskriminant. [Kaldet <u>diskriminanten</u> af R].

4. Lad $R = \mathbb{Z}[\xi]$ være en kvadratisk talring og lad α være et kvadratisk tal. Vis, at
$$\mathbb{Z}[\alpha] \subseteq \mathbb{Z}[\xi] \iff \exists\, y \in \mathbb{Z} : D(\alpha) = y^2 D(\xi).$$

5. Lad $D \in \mathbb{Z}$ være et tal som er $\equiv \begin{cases} 0 \\ 1 \end{cases} \bmod 4$ og som ikke er et kvadrat. (i) Vis, at der findes en og kun én kvadratisk talring R_D med diskriminant D [Vink: For eksistensen betragtes polynomierne $X^2 - \frac{D}{4}$ og $X^2 - X + \frac{1-D}{4}$ eftersom D er lige eller ulige]
(ii) Vis, for "diskriminanter" D og $\tilde{D}$, at
$$R_{\tilde{D}} \subseteq R_D \iff \exists\, y \in \mathbb{Z} : \tilde{D} = y^2 D.$$

6. Vis, at den kvadratiske talring R_D, hvor $D = -3, -4, -7, -8, -11$, er et hovedidealområde [Vink: $R_{-4} = \mathbb{Z}[\sqrt{-1}]$ er Gauss' talring].

7. Vis om $R_{-3} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ og $R_{-12} = \mathbb{Z}[\sqrt{-3}]$, at $R_{-12} \subseteq R_{-3}$ og bestem enhederne i de to ringe. Vis, at R_{-12} ikke er faktoriel.

Algebra 1984

Opgaver 30
("Idealer")

1. Lad R være en kvadratisk talring med diskriminanten D.
(i) Vis, at $\sqrt{D} \in R$.
(ii) Vis, at $\frac{1}{2}\sqrt{D} \in R \Leftrightarrow D \equiv 0 \pmod 4$.
(iii) Vis, at $\frac{1}{n}\sqrt{D} \notin R$, når $n > 2$, $n \in \mathbb{N}$.

2. Lad R være en kvadratisk talring og lad $\pi \in R$ være et element med $p := |N(\pi)|$ et sædvanligt primtal. Vis, at så er π et primelement i R, hovedidealet $R\pi$ er et maksimalideal i R og $R/R\pi \cong \mathbb{F}_p$. [Vink: Da $p = \pm \pi'\pi$, er $Rp \subset R\pi$. Vis og udnyt nu, at $|R : Rp| = p^2$].

3. Lad R være en kvadratisk talring og lad p være et sædvanligt primtal. Vis, at hvis p er reducibel i R, så er $p = \pm \pi\pi'$, hvor π (og π') er et primelement i R.
[p siges at være af <u>type 2</u> eller af <u>special type</u> eftersom π' <u>ikke er</u> eller <u>er</u> associeret med π].

4.* Lad $R = \mathbb{Z}[\xi]$ være en kvadratisk talring med diskriminant D og lad p være et sædvanligt primtal.
(i) Lad $\alpha = x + y\xi \in R$ og antag, at $p \nmid \alpha$ og $p \mid \alpha^2$. Vis, at så er $p \mid D$.
[Vink. At $p \mid \alpha^2 = (x^2 - cy^2) + (2xy - by^2)\xi$ betyder at $p \mid x^2 - cy^2$ og $p \mid 2xy - by^2$. Vis, at påstanden følger heraf]
(ii) Vis, at et primtal af special type er divisor i D.

5. Lad R være en kvadratisk talring med diskriminant D. Antag, at R er faktoriel.
(i) Vis, at de ulige primdivisorer i D netop er de ulige primtal af special type og vis, at de forekommer i D med eksponent 1 [Vink. Brug opgave 1 og 4].
(ii)* Antag $D \equiv 0 \bmod 4$, $D = 4D_0$. Vis, at så er 2 af special type og $D_0 \equiv \begin{cases} 2 \\ 3 \end{cases} \bmod 4$. [Vink: Hvis D_0 er lige gås frem som i (i). Hvis D_0 er ulige ses på $(1 + \sqrt{D_0})^2$].

Algebra 1984

Opgaver 31
("Idealer")

1. Lad R være en kvadratisk talring.
(i) Vis for $n \in \mathbb{N}$ at kvotienten R/Rn er en endelig ring med n^2 elementer.
(ii) Vis, at hvert ideal $\alpha \neq (0)$ i R er endeligt frembragt og at R/α er en endelig ring.
(iii) Vis, at hvert primideal $\neq (0)$ i R er et maksimalideal. [Udnyt f.eks. at et endeligt int. omr. er et legeme].

2. Lad R være en kvadratisk talring.
(i) Vis, at hvis R er faktoriel, så er hvert maksimalideal $\mathfrak{M}$ et hovedideal (af formen $\mathfrak{M} = (\pi)$, hvor π er et primideal)
[Vink. Søg et primelement $\pi \in \mathfrak{M}$ og brug opgave 1]
(ii) Vis, at det omvendte også gælder.

3*. Vis, at en faktoriel kvadratisk talring er et hovedidealområde.

4. Lad R være en kvadratisk talring og lad $\alpha \in R \setminus \{0\}$. Vis, at $R/R\alpha$ er en endelig ring med $n = |N(\alpha)|$ elementer.
[Vink. Find en surjektiv ringhomomorfi $R/Rn \to R/R\alpha$ og bestem ordenen af kernen]

5. Lad $R = \mathbb{Z}[i]$ være Gauß' talring. Vis, at 11 er irreducibel i R. Hvor mange elementer har legemet $R/(11)$?

6. Bestem det mindste pythagoræiske tal så at ligningen $x^2 + y^2 = k^2$ har mere end 2 forskellige løsninger. Bestem de 4 løsninger til ligningen.

7. Lad p være et primtal $\equiv 1 \bmod 4$. Bevis, at kongruensen $x^2 \equiv -1 \pmod{p}$ har løsninger ved at vise, at $x = (2h)!$ er en løsning når $p = 4h+1$.