MATEMATIK 3 AL

Klassisk Algebra

Christian U. Jensen

2004

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Matematisk Afdeling
Universitetsparken 5
2100 København Ø

FORORD TIL 1998-UDGAVEN

At lære og at tilegne sig et nyt stof, er en *uhyre* kompliceret proces. Der findes mange teorier inden for denne problemkreds. Sandheden er nok, at der ikke findes nogen entydig optimal metode endsige en "vidundermetode". Dette gælder i særlig grad i matematik, jfr. Euklids bemærkning til Menelaos: "Der findes ingen kongevej til matematikken." Tilegnelse af nyt matematisk stof vil altid kræve en vis portion slid og sved.

Når man skriver noter til et kursus, gør man sig naturligvis mange overvejelser over indlæringsmetoder, specielt i hvilken form noterne skal præsenteres. Nogle lærere mener, at noter bør skrives meget bredt, andre er ikke helt overbevist herom. Selv mener jeg, at noter til 1-ste og 2-den årskurser bør være ret udførlige, mens noter til 3-die årskurser og senere kurser med fordel kan overlade en hel del overvejelser til læseren.

I første omgang kan det måske føles som en lettelse at se alle argumenter gennemført til mindste detalje. Men hvis man tvinges til selv at gennemføre detaljer og eventuelt udarbejde notater herom, så læseren/den studerende føler selv at være med i teoriens opbygning, vil man få et helt andet forhold til stoffet. Og først når man har fået fuld forståelse af f.eks. Galoisteori, vil man kunne påskønne denne teoris skønhed. Det er mit håb, at disse noter og forelæsningerne hertil vil hjælpe deltagerne til at kunne glæde sig over en af matematikkens smukkeste teorier.

Juli 1998 C.U.J.

FORORD TIL 2001-UDGAVEN

Der er i denne udgave foretaget en del redaktionelle ændringer, der er tilpasset den seneste udgave af Matematik 2AL. Endvidere er en række trykfejl mm. blevet rettet.

Juni 2001 C.U.J.

FORORD TIL 2004-UDGAVEN

I denne udgave er foretaget mindre redaktionelle ændringer, idet jeg har fulgt tidligere kursusdeltageres forslag til forbedring på forskellige punkter. Desuden er denne udgave blevet suppleret med en opgavesamling.

Juli 2004 C.U.J.

Matematisk Institut

INDHOLD

Kapitel I. Gruppeteori

Grundlæggende definitioner og begreber 1.1

Automorfier 1.5

Direkte produkt 1.8

Noethers isomorfisætninger 1.9

Kommutatorgrupper 1.10

Grupper af given endelig orden 1.11

Flytningsgrupper 1.16

Permutationsgrupper 1.18

Normalrækker 1.24

Opløselighed 1.28

Sylows gruppesætninger 1.36

Verlagerung og anvendelser heraf 1.35

Abelske grupper 1.42

Kapitel II. Ringe og Polynomier

Lidt alment om ringe og idealer 2.1

Faktorisieringer af polynomier 2.2

Symmetriske polynomier 2.5

Algebraiske udvidelser 2.8

Adjunktion af rod til et polynomium. Spaltningslegemer 2.12

Største fælles divisor for polynomier 2.16

Karakteristik af et legeme 2.17

Multiple rødder, formel differentiation og separabilitet 2.19

Abel-Steinitz's sætning 2.22

Endelige legemer 2.23

Diskriminant for et polynomium 2.26

Kapitel III. Galoisteori

Indledende sætninger og begreber 3.1

Galoisteoriens hovedsætning 3.8

Translationssætningen 3.13

Kapitel IV. Cirkeldelingslegemer og anvendelser heraf

Enhedsrødder og cirkeldelingspolynomier 4.1

Dirichlets sætning om primtal i aritmetiske progressioner 4.4

Cirkeldelingslegemer 4.5

Konstruktion af regulære polygoner med passer og lineal 4.7

En anvendelse på "Galoisteoriens omvendingsproblem" 4.10

Kapitel V. Opløselighed ved rodtegn

Krydsede produkter og anvendelser heraf 5.1

Radikaludvidelser 5.5

Eksplicitte eksempler 5.10

Polynomier af grad $\geqq 5$ 5.12

Kapitel VI. Kvadratiske rester

Den kvadratiske reciprocitetssætning 6.4

Fremstilling som sum af to kvadrater 6.9

Nogle bemærkninger om højere potensrester 6.16

Kapitel I. Grupper

Alice: The question is, whether you can make words mean so many different things.
Humpty Dumpty: The question is, who is to be master - that's all.
(Fra: Alice in Wonderland and Through the Looking Glass)

GRUNDLÆGGENDE DEFINITIONER OG BEGREBER.

Definition. En gruppe er en ikke-tom mængde G med en kompositionsforskrift $\circ$, så følgende betingelser er opfyldt:

1) $\circ$ er associativ (dvs.: $(a \circ b) \circ c = a \circ (b \circ c) \quad \forall a, b, c \in G$)
2) Der findes et neutralt element $e \in G$ (dvs.: $e \circ g = g \circ e = g \quad \forall g \in G$)
3) Til ethvert element g i G findes et inverst element $g^{-1} \in G$ (dvs.: $g \circ g^{-1} = g^{-1} \circ g = e$).

Bemærkning. Det neutrale element e i ovenstående er nødvendigvis entydigt bestemt. Endvidere er g^{-1} entydigt bestemt ved g.

Definition. For hvert $n \in \mathbb{Z}$ defineres for et element g i gruppen G

$$g^n = \begin{cases} g \circ g \circ \cdots \circ g \quad (n \text{ faktorer}) & \text{for} \quad n > 0 \\ e & \text{for} \quad n = 0 \\ (g^{-1})^{-n} & \text{for} \quad n < 0\,. \end{cases}$$

Da gælder potensreglerne

$$\begin{aligned} g^{n+m} &= g^n \circ g^m \qquad && \forall n, m \in \mathbb{Z} \\ (g^n)^m &= g^{nm} && \forall n, m \in \mathbb{Z}\,. \end{aligned}$$

Derimod gælder $(a \circ b)^n = a^n \circ b^n$ normalt *ikke*. For $n = -1$ gælder derimod $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$. (Hvorfor?)

Definition. Elementerne a og b i gruppen G kaldes *ombyttelige*, hvis $a \circ b = b \circ a$.

Definition. En gruppe kaldes *kommutativ* (eller *abelsk*), hvis alle elementerne i gruppen er indbyrdes ombyttelige.

Definition. Lad $(G, \circ)$ være en gruppe og lad S være en ikke-tom delmængde i G. Da kaldes S en undergruppe af $(G, \circ)$, hvis S med $\circ$ som kompositionsforskrift udgør en gruppe.

Sætning 1. *Lad $(G, \circ)$ være en gruppe og S en ikke-tom delmængde i G. Da gælder: S er en undergruppe hvis og kun hvis $a, b \in S \Rightarrow a \circ b^{-1} \in S$.*

Bevis. Simpel øvelse.

EKSEMPEL. Enhver fællesmængde af undergrupper i en gruppe er selv en undergruppe.

BEMÆRKNING. Når der ikke er mulighed for misforståelse, vil vi i det følgende i stedet for $a \circ b$ blot skrive ab.

BEMÆRKNING. For enhver delmængde S i en gruppe findes en mindste undergruppe i G indeholdende S (hvorfor ?). Denne kaldes undergruppen frembragt af S og består af alle elementer af formen $s_1^{t_1} \dots s_n^{t_n}$, $t_1, \dots, t_n \in \mathbb{Z}$, $n \in \mathbb{N}$ (gentagelser tilladt).

DEFINITION. G kaldes cyklisk, hvis G er frembragt af et enkelt element. Dvs.: hvis $\exists g \in G$ så $G = \{g^n \mid n \in \mathbb{Z}\}$.

Det er kendt fra Mat 2AL, at en undergruppe i en cyklisk gruppe selv er cyklisk.

DEFINITION. Ved *ordenen* af en gruppe G forstås antallet (kardinaltallet) $|G|$, af elementer i G. Ved *ordenen* $\operatorname{Ord} a$ af et element $a \in G$ forstås ordenen af den af a frembragte undergruppe.

BEMÆRKNING. Hvis ordenen t af et element a er endelig, gælder for ethvert helt tal n:

$$a^n = e \iff t|n .$$

Lagrange's sætning. *Hvis G er en endelig gruppe, vil $\operatorname{Ord} a \mid |G|$ for alle $a \in G$.*

BEMÆRKNING. Det er klart, at G endelig $\Rightarrow$ alle elementer i G har endelig orden.

EKSEMPEL. I ovenstående bemærkning kan implikationen ikke vendes om. Mængden af alle komplekse enhedsrødder $\{e^{\frac{2\pi i}{n} a} , n \in \mathbb{N} , a \in N\}$ udgør med sædvanlig multiplikation en uendelig gruppe, hvor alle elementer har endelig orden.

Sætning 2. *Hvis samtlige fra e forskellige elementer i en gruppe G har orden 2, da er G abelsk.*

Bevis. $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$, da generelt $g^2 = e \Rightarrow g = g^{-1}$. □

De elementer i en gruppe der er ombyttelige med samtlige elementer i G udgør en undergruppe i G, som kaldes *centrum* for G og ofte betegnes $Z(G)$. Åbenbart gælder $Z(G) = G \iff G$ er abelsk.

EKSEMPEL Hvis G har netop ét element af orden 2, da vil dette element tilhøre $Z(G)$. (Hvorfor ?)

En afbildning f fra gruppen G til gruppen H kaldes en *homomorfi*, hvis $f(g_1 \circ g_2) = f(g_1) \circ f(g_2) \quad \forall g_1, g_2 \in G$. Øjensynligt vil en homomorfi f fra G til H føre det neutrale element i G over i det neutrale element i H og føre inverst element over i inverst element: $f(g^{-1}) = f(g)^{-1}$.

Hvis desuden f er bijektiv, kaldes f en *isomorfi*, og G og H kaldes i så fald for isomorfe grupper. Isomorfe grupper er "i det væsentlige" ens.

EKSEMPEL. Enhver cyklisk gruppe er enten isomorf med den cykliske gruppe $\mathbb{Z}_n$ af orden n for passende $n \in \mathbb{N}$ eller isomorf med de hele tals additive gruppe $\mathbb{Z}$.

Lad nu S være en vilkårlig undergruppe i gruppen G. Vi indfører relationen: $a \underset{v}{\sim} b$ hvis $ab^{-1} \in S$. $\underset{v}{\sim}$ ses let at være en ækvivalensrelation "$a \underset{v}{\sim} b$" læses "a venstre-ækvivalent med b". Analogt indføres "$a \underset{h}{\sim} b$", hvis $a^{-1}b \in S$.

Svarende til $\underset{v}{\sim}$ fås inddeling af G's elementer i ækvivalensklasser. Ækvivalensklassen $\textcircled{a}_v$ indeholdende a består af elementerne $\{sa \mid s \in S\}$, hvilket kort skrives $\textcircled{a}_v = Sa$. (Ækvivalensklassen $\textcircled{a}$ betegnes af typografiske grunde undertiden som $\overline{a}$.) Alle ækvivalensklasserne indeholder derfor $|S|$ elementer. Vi bemærker endvidere $a \underset{v}{\sim} b \Rightarrow ag \underset{v}{\sim} bg$ for alle g i G. Ækvivalensklasserne svarende til $\underset{v}{\sim}$ kaldes G's venstre-sideklasser med hensyn til S. Tilsvarende for "$\underset{h}{\sim}$".

Hvis $\{a_i\}$ udgør et fuldstændigt repræsentantsystem for venstre- sideklasserne vil $\{a_i^{-1}\}$ udgøre et fuldstændigt repræsentantsystem for højre-sideklasserne. Følgelig findes lige mange venstre-sideklasser og højre-sideklasser.

DEFINITION. Det fælles antal venstre- og højre-sideklasser kaldes G's index med hensyn til S og betegnes $[G : S]$.

BEMÆRKNING. Hvis G er endelig, gælder $|G| = |S| \cdot [G : S]$.

BEMÆRKNING. Terminologien angående venstre-/højre-sideklasser ligger ikke fast i gruppeteorien. Hos nogle gruppeteoretikere kaldes de her indførte venstre-sideklasser for højre-sideklasser og de her indførte højre-sideklasser for venstre-sideklasser.

Sætning 3. *Lad S være en undergruppe i gruppen G. Da er følgende betingelser ækvivalente:*

1) *For alle $a, b \in G$ gælder: $a \underset{v}{\sim} b \iff a \underset{h}{\sim} b$.*
2) *For alle $a, b \in G$ gælder: $a \underset{v}{\sim} b \Rightarrow ga \underset{v}{\sim} gb \ \forall g \in G$.*
3) *For alle $a, b \in G$ gælder: $a \underset{h}{\sim} b \Rightarrow ag \underset{h}{\sim} bg \ \forall g \in G$.*
4) *$g\, Sg^{-1} \subseteq S \ \forall g \in G$,*
5) *$g\, Sg^{-1} = S \ \forall g \in G$.*

Bevis. Nok at godtgøre 1) $\Rightarrow$ 2), 1) $\Rightarrow$ 3), 2) $\Rightarrow$ 4), 3) $\Rightarrow$ 4), 4) $\Rightarrow$ 5), og 5) $\Rightarrow$ 1).

1) $\Rightarrow$ 2). $a \underset{v}{\sim} b \Rightarrow a \underset{h}{\sim} b \Rightarrow ga \underset{h}{\sim} gb \Rightarrow ga \underset{v}{\sim} gb$.

1) $\Rightarrow$ 3). Analogt.

2) $\Rightarrow$ 4). $sg^{-1} \underset{v}{\sim} g^{-1} \Rightarrow gsg^{-1} \underset{v}{\sim} gg^{-1} = e$ for alle $s \in S$ hvoraf $gsg^{-1} \in S$ for alle $s \in S$.

3) $\Rightarrow$ 4). Analogt.

4) $\Rightarrow$ 5). $g\ S\ g^{-1} \subseteq S$ for alle $g \in G$ medfører: $S = g^{-1}(gSg^{-1})g \subseteq g^{-1}Sg \subseteq S$, hvoraf $g^{-1}Sg = S\ \forall g \in G$.

5) $\Rightarrow$ 1). Antag $a \underset{v}{\sim} b$.
Da er $ab^{-1} \in S$ og dermed ifl. 5) $b^{-1}ab^{-1}b = b^{-1}a \in S$, hvorfor $a \underset{h}{\sim} b$.
Analogt ses, at $a \underset{h}{\sim} b \Rightarrow a \underset{v}{\sim} b$.

$\square$

Definition. En undergruppe S i gruppen G kaldes *normaldeler* (eller *normal* undergruppe) i G, hvis én og dermed samtlige betingelser i ovenstående sætning er opfyldt. S normal undergruppe i G skrives $S \lhd G$.

Bemærkning. Hvis G er abelsk, er alle undergrupper normale. Endvidere bemærker vi, at enhver undergruppe af index 2 er normaldeler.

Hvis S er en normal undergruppe i G, stemmer venstre- og højre side-klasserne overens. Da, for $S \lhd G$, $a \underset{v}{\sim} b \Rightarrow ag \underset{v}{\sim} bg$ og $ga \underset{v}{\sim} gb$ vil der ved $a \cdot b = \overline{ab}$ defineres en komposition på mængden af sideklasser. Disse udgør herved en gruppe, der kaldes *faktorgruppen* (eller kvotientgruppen) for G m.h.t. S og betegnes G/S. Afbildningen κ fra G til G/S defineret ved $\kappa g = g$ er en surjektiv homomorfi. κ betegnes den *kanoniske homomorfi* fra G på G/S.

For en homomorfi f fra en gruppe G til en gruppe H vil *kernen*, $\operatorname{Ker} f = \{g \in G \mid f(g) = e\}$ være en normal undergruppe i G. Omvendt vil enhver normal undergruppe S i G være kerne for en homomorfi, nemlig den kanoniske homomorfi fra G til G/S.

Homomorfisætning. *Lad f være en surjektiv homomorfi fra en gruppe G på en gruppe H. Da er $\operatorname{Ker} f \lhd G$ og $G/\operatorname{Ker} f \simeq H$. Mere præcist: der findes netop én isomorfi $\overline{f}$ fra $G/\operatorname{Ker} f$ til H så $f = \overline{f} \circ \kappa$ hvor κ er den kanoniske homomorfi fra G på $G/\operatorname{Ker} f$.*

Bevis. $\operatorname{Ker} f \lhd G$ har vi allerede bemærket. For en sideklasse g i $G/\operatorname{Ker} f$ definerer vi $\overline{f}\, g = fg$, hvor $g \in g$. Dette giver veldefineret afbildning; thi $g_1 = g_2 \Rightarrow g_1 g_2^{-1} \in \operatorname{Ker} f \Rightarrow f(g_1 g_2^{-1}) = e \Rightarrow f(g_1)f(g_2)^{-1} = e \Rightarrow f(g_1) = f(g_2)$. $\overline{f}$ ses umiddelbart at være en homomorfi. $\overline{f}$ er injektiv, thi $\overline{f}\,\overline{g_1} = \overline{f}\,\overline{g_2} \Rightarrow f(g_1) = f(g_2)$, hvor $g_1 \in \overline{g_1}$, $g_2 \in \overline{g_2}$. Heraf ses, at $f(g_1) \cdot f(g_2)^{-1} = f(g_1 g_2^{-1}) = e$ og herved $g_1 g_2^{-1} \in \operatorname{Ker} f$ dvs. $\overline{g_1} = \overline{g_2}$; $\overline{f}$ endvidere surjektiv; thi da f er surjektiv, findes til ethvert $h \in H$ et $g \in G$ som $h = f(g)$. Men da er $h = \overline{f}\,(g)$. $\overline{f}$ altså isomorfi. Af $\overline{f}$'s definition fås øjensynligt $f = \overline{f} \circ \kappa$.

Hvis f^* er en afbildning fra $G/\operatorname{Ker} f$ til H så $+f = f^* \circ \kappa$ da er

$$f^* \circ \kappa(g) = f^* \; \bigcirc\!\!\!\!g = f \; g \quad \forall g \text{ dvs.}: \quad f^* = \overline{f}\,.$$

$\square$

AUTOMORFIER.

En isomorfi φ af en gruppe G på sig selv kaldes en *automorfi*. Automorfierne for G udgør med successiv sammensætning som komposition en gruppe, $\operatorname{Aut}(G)$.

For ethvert $g \in G$ vil afbildningen $k_g : G \to G$ defineret ved $k_g(x) = gxg^{-1}$ være en automorfi, kaldet den *indre automorfi* bestemt ved g. De indre automorfier for G udgør en undergruppe, $\operatorname{Aut}_i(G)$, i $\operatorname{Aut}(G)$.

Sætning 4. $\operatorname{Aut}_i(G) \triangleleft \operatorname{Aut}(G)$.

Bevis. For $\varphi \in \operatorname{Aut}(G)$ gælder $\varphi \circ k_g \circ \varphi^{-1} = k_{\varphi g}$. $\square$

Sætning 5. $\operatorname{Aut}_i(G) \simeq G/Z(G)$.

Bevis. Afbildningen $G \xrightarrow[k]{} \operatorname{Aut}_i(G)$, defineret ved $k(g) = k_g$ er en surjektiv homomorfi med $Z(G)$ som kerne. Homomorfisætningen giver den ønskede isomorfi. $\square$

På baggrund af ovenstående kan vi udtrykke at en undergruppe H er normal i G ved at sige, at H er invariant overfor alle indre automorfier, dvs. $k_g(H) \subseteq H \; \forall k_g$. I den forbindelse indføres begrebet karakteristisk undergruppe.

Definition. En undergruppe H i gruppen G kaldes *karakteristisk*, hvis $\varphi(H) \subseteqq H$ for alle automorfier $\varphi \in \operatorname{Aut}(G)$.

Enhver karakteristisk undergruppe er således specielt en normaldeler.

Bemærkning. Hvis H er en karakteristisk undergruppe i G, vil der gælde $\varphi(H) = H$ for alle automorfier $\varphi \in \operatorname{Aut}(G)$. (Hvorfor?)

Eksempel. For enhver gruppe G er centrum $Z(G)$ karakteristisk i G.

Eksempel. I en cyklisk gruppe er enhver undergruppe karakteristisk.

Bemærkning. Relationen "H karakteristisk undergruppe i G" er transitiv (dvs.: K karakteristisk i H og H karakteristisk i $G \Rightarrow K$ karakteristisk i G). Det tilsvarende gælder *ikke* for normale undergrupper.

Vigtigt eksempel. Af hensyn til senere anvendelser minder vi kort om begrebet primisk restklasse modulo et naturligt tal n.

En restklasse @ kaldes primisk, hvis $(a, n) = 1$, dvs. a og n er indbyrdes primiske for én og dermed for enhver repræsentant a for restklassen.

Restklasserne modulo n udgør en kommutativ ring $(\mathbb{Z}_n, +, \cdot)$.

De primiske restklasser er netop de invertible elementer i denne ring.

Thi, antag ⓐ er en primisk restklasse; da $(a, n) = 1$ findes hele tal x og y så $ax + ny = 1$. Men da er ⓐ$\cdot$ ⓧ= ①, dvs. ⓐ er invertibelt.

Omvendt gælder for en invertibel restklasse ⓐ, at der findes et helt tal x så $ax = 1$, modulo n dvs. $ax = 1 + ny$ for et passende helt tal y. Men ligningen $1 = ax - ny$ viser, at a og n må være indbyrdes primiske.

De primiske restklasser udgør en multiplikativ gruppe, der betegnes G_n eller $\mathbb{Z}_n^*$.

I en øvelse skal vi vise, at G_n er isomorf med automorfigruppen for den cykliske gruppe af orden n.

Som det fremgår af ovenstående er der for enhver gruppe G en veldefineret homomorfi: $G \xrightarrow[k_g]{} \mathrm{Aut}(G)$. Hvis denne homomorfi er en isomorfi kaldes G *fuldkommen*. Med andre ord er G fuldkommen netop når $Z(G) = \{e\}$ og enhver automorfi er indre.

Definition. En gruppe $G \neq \{e\}$ kaldes *simpel*, hvis den kun har de to trivielle normaldelere $\{e\}$ og G.

Opgave. Vis, at en abelsk gruppe G er simpel $\iff$ $|G|$ er primtal.

Sætning 6. *Automorfigruppen* $\mathrm{Aut}(G)$ *for en simpel ikke-abelsk gruppe G er fuldkommen.*

Beviset føres i flere skridt. Først et generelt lemma.

Lemma. *Lad A og B være normaldelere i en gruppe G. Hvis $A \cap B = \{e\}$, da er $ab = ba$ $\forall a \in A$, $\forall b \in B$.*

Bevis. $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) = (aba^{-1})b \in A \cap B$ dvs.: $(ab) \cdot a^{-1}b^{-1} = e$ og dermed $ab = ba$. □

Vi skal vise, at $\mathrm{Aut}(G)$ har trivielt centrum og at enhver automorfi for $\mathrm{Aut}(G)$ er indre.

Vi viste i Sætning 4 at $\mathrm{Aut}_i(G) \triangleleft \mathrm{Aut}(G)$.

1°. $\alpha \in \mathrm{Aut}(G)$, $\alpha k_g = k_g \alpha$ $\forall k_g \in \mathrm{Aut}_i(G) \Rightarrow \alpha =$ *Identiteten.*

Bevis.

$$\begin{aligned} \alpha k_g[x] = {} & \alpha(gxg^{-1}) = \alpha g \alpha x (\alpha g)^{-1}, \\ k_g \alpha[x] = {} & g\alpha(x) g^{-1}. \end{aligned}$$

$\alpha k_g[x] = k_g \alpha[x]$ $\forall x \in G \Rightarrow g^{-1}(\alpha g)(\alpha x) = (\alpha x) \cdot g^{-1}(\alpha g), \forall x \in G \Rightarrow g^{-1}\alpha g \in Z(G) = \{e\}$. Dette gælder for alle $g \in G$, dvs.: $\alpha g = g$ dvs.: $\alpha =$ Identiteten på G. Vi har her benyttet, at G simpel, ikke-abelsk $\Rightarrow Z(G) = \{e\}$.

1° indebærer specielt, at $\mathrm{Aut}(G)$ har trivielt centrum.

2°. *For alle* $\psi \in (\mathrm{Aut}(\mathrm{Aut}(G)))$ *gælder* $\psi(\mathrm{Aut}_i(G)) = \mathrm{Aut}_i(G)$.

Bevis. $\psi(\mathrm{Aut}_i(G)) \triangleleft \mathrm{Aut}(G)$, dermed er $\psi(\mathrm{Aut}_i(G)) \cap \mathrm{Aut}_i(G) \triangleleft \mathrm{Aut}_i(G) \simeq G/Z(G) \simeq G$. (Jfr. Sætning 4). Da G er simpel, er $\psi(\mathrm{Aut}_i(G)) \cap \mathrm{Aut}_i(G) = \{e\}$ eller $\mathrm{Aut}_i(G)$. Den første mulighed udelukkes af lemmaet og 1°. Altså gælder $\psi(\mathrm{Aut}_i(G)) \supseteqq \mathrm{Aut}_i(G)$. Dette gælder for alle ψ, hvorfor $\psi^{-1}(\mathrm{Aut}_i(G)) \supseteqq \mathrm{Aut}_i(G)$, hvoraf $\psi(\mathrm{Aut}_i(G)) = \mathrm{Aut}_i(G)$.

3°. $\psi \in \mathrm{Aut}(\mathrm{Aut}(G))$, $\psi(k_g) = k_g \ \forall k_g \in \mathrm{Aut}_i(G) \Rightarrow \psi =$ *Identiteten på* $\mathrm{Aut}(G)$.

Bevis. Lad β være vilkårlig i $\mathrm{Aut}\, G$. Da er ifølge beviset for sætning 4 $\beta k_g \beta^{-1} = k_{\beta g}$ for alle $g \in G$. Anvendes ψ på denne ligning og benyttes forudsætningerne $\psi(k_g) = k_g$ og $\psi(k_{\beta g}) = k_{\beta g}$, fås heraf:

$$\psi\beta k_g \psi\beta^{-1} = k_{\beta g} = \beta k_g \beta^{-1}.$$

Altså kommuterer $\beta^{-1}\psi\beta$ med k_g for alle $g \in G$ og må således ifl. 1 ° være identiteten på G. Dette medfører, at $\psi\beta = \beta$ for alle $\beta \in \mathrm{Aut}(G)$ og dermed $\psi =$ identiteten på $\mathrm{Aut}(G)$.

4°. *To automorfier* ψ_1 *og* ψ_2 *i* $\mathrm{Aut}(\mathrm{Aut}(G))$ *stemmer overens, hvis de har samme restriktion til* $\mathrm{Aut}_i(G)$.

Bevis. Anvend 3° på ${\psi_1}^{-1}\psi_2$.

5°. *For* $\psi \in \mathrm{Aut}(\mathrm{Aut}(G))$ *gælder* $\psi(k_g) = k_{\alpha g}$ *for en passende automorfi* $\alpha \in \mathrm{Aut}(G)$.

Bevis. Ifølge 2° er $\psi(k_g) \in \mathrm{Aut}_i(G)$, dvs. $\psi(k_g) = k_{g^*}$ for passende $g^* \in G$. Da $Z(G) = e$ er g^* entydigt bestemt ved g. Vi kan derfor sætte $g^* = \alpha g$ for en vis afbildning α af G ind i G. Igen ved brug af $Z(G) = \{e\}$ ses α at være injektiv. På grund af 2° er α også surjektiv dvs.: α er bijektiv.

Vi mangler at bevise, at α er en homomorfi. Af $k_{g_1 g_2} = k_{g_1} \cdot k_{g_2}$ fås $\psi(k_{g_1 g_2}) = \psi(k_{g_1}) \cdot \psi(k_{g_2})$ og dermed $k_{\alpha(g_1 g_2)} = k_{\alpha g_1} \cdot k_{\alpha g_2} = k_{\alpha g_1 \alpha g_2}$. Da $Z(G) = \{e\}$, slutter vi nu, at $\alpha(g_1 g_2) = \alpha g_1 \cdot \alpha g_2$.

6°. *Med benævnelserne fra* 5° *gælder* $\psi(\beta) = \alpha\beta\alpha^{-1}$ *for alle* $\beta \in \mathrm{Aut}(G)$.

Bevis. På grund af 4° er det nok at vise $\psi(k_g) = \alpha k_g \alpha^{-1}$ for alle $k_g \in \mathrm{Aut}_i(G)$. Men dette følger af $\psi(k_g) = k_{\alpha g}$ og af at $k_{\alpha g} = \alpha k_g \alpha^{-1}$.

Hermed er beviset for Sætning 6 afsluttet. □

DIREKTE PRODUKT.

Lad H og K være undergrupper i gruppen G. Med HK betegner vi delmængden $\{hk | h \in H,\ k \in K\}$. Denne delmængde HK er i almindelighed ikke en undergruppe i G. I den forbindelse viser vi

Sætning 7. *For undergrupper H og K i G gælder:*

$$HK \text{ er undergruppe i } G \iff HK = KH\,.$$

Bevis $\Rightarrow$. Vi viser $KH \subseteqq HK$ og $HK \subseteqq KH$.

$KH \subseteqq HK$: For vilkårlige elementer $h \in H$, $k \in K$ gælder $h \in HK$, $k \in HK$; da HK undergruppe er $kh \in HK$.

$HK \subseteqq KH$: Lad $h \in H$, $k \in K$. Ifølge ovenstående kan $k^{-1}h^{-1}$ skrives $\widetilde{h}\,\widetilde{k}$, $\widetilde{h} \in H$, $\widetilde{k} \in K$. Heraf $hk = (k^{-1}h^{-1})^{-1} = (\widetilde{h}\,\widetilde{k})^{-1} = \widetilde{k}^{-1}\widetilde{h}^{-1}$.

$\Leftarrow$ Lad h_1k_1 og h_2k_2 være elementer i HK. På grund af $HK = KH$ er $h_1k_1h_2k_2 \in HK$.

For ethvert $hk \in HK$ er $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. $\square$

Sætning 8. *Hvis $H \lhd G$, og K er en undergruppe i G, da er $HK = KH$ (som dermed ifølge ovenstående sætning er en undergruppe i G).*

Bevis. For vilkårlige elementer $h \in H$, $k \in K$ gælder

$$kh = (khk^{-1})k \in HK\,, \qquad \text{da} \quad H \lhd G$$
$$hk = k(k^{-1}hk) \in KH\,, \qquad \text{da} \quad H \lhd G\,.$$

$\square$

Sætning 9. *Hvis $H \lhd G$, $K \lhd G$, $HK = G$, $H \cap K = \{e\}$, da kan ethvert $g \in G$ på entydig vis skrives $g = hk$ ($h \in H$, $k \in K$), og regning sker "komponentvis": $(h_1k_1)(h_2k_2) = (h_1h_2)(k_1k_2)$, hvor $h_1, h_2 \in H$, $k_1, k_2 \in K$.*

Bevis. Antag $g = hk = \widetilde{h}\,\widetilde{k}$, $h, \widetilde{h} \in H$, $k, \widetilde{k} \in K$. Da var $\widetilde{h}^{-1}h = \widetilde{k}k^{-1} \in H \cap K = \{e\}$, dvs. $h = \widetilde{h}$, $k = \widetilde{k}$.

For vilkårlige elementer $h \in H$, $k \in K$ gælder, at $hkh^{-1}k^{-1} \in H \cap K = \{e\}$, dvs. h og k er ombyttelige, hvorfor $(h_1k_1)(h_2k_2) = h_1(h_2k_1)k_2$. $\square$

Definition. I situationen fra ovenstående sætning siges G at være det *indre direkte produkt* af H og K. H (og K) kaldes en *direkte faktor* i G.

Bemærkning. I Mat 2AL (GRP 3.19) er det direkte produkt af to grupper indført indført som produktmængden af de to grupper med koordinatvis komposition. Det på den vis definerede direkte produkt kaldes ofte det *ydre direkte produkt* af grupperne. Hvis G er det indre direkte produkt af undergrupperne H og K, er det en simpel opgave at vise, at G er isomorf med det ydre direkte produkt af H og K. Forskellen mellem ydre og indre direkte produkt er derfor af mere formel karakter. Ofte udelades prædikaterne "ydre" og "indre", når der ikke kan opstå nogen misforståelse.

Sætning 10. *Hvis en fuldkommen gruppe H er normal undergruppe i en gruppe G, er H direkte faktor i G.*

Bevis. Hvis $g \in G$, er $ghg^{-1} \in H$ for alle $h \in H$, da $H \triangleleft G$. *Afbildningen* $h \longrightarrow ghg^{-1}$ er derfor en automorfi for H. Da H er fuldkommen findes der til ethvert g et entydigt bestemt element $\eta \in H$ så $ghg^{-1} = \eta h \eta^{-1}$ $\forall h \in H$. Lad K være "H's centralisator i G", dvs.: $K = \{k \in G | hk = kh \text{ for alle } h \in H\}$.

K er undergruppe i G indeholdende alle elementer $\eta^{-1}g$. Påstand: G er direkte produkt af H og K.

$G = HK$ da $g = \eta(\eta^{-1}g)$ [bemærk $G = HK \iff G = KH$]. Endvidere da centrum for H er $\{e\}$, bliver $H \cap K = \{e\}$. Mangler blot at vise $K \triangleleft G$.

For ethvert $k \in K$ og ethvert $g \in G$ gælder

$$g^{-1}kg = g^{-1}\eta\eta^{-1}k\eta\eta^{-1}g = g^{-1}\eta k \eta^{-1} g \in K\,.$$

Vi har her benyttet, at $\eta^{-1}k\eta = k$ på grund af definitionen af K. □

Bemærkning. Man kan omvendt vise, at en gruppe er fuldkommen, såfremt den er direkte faktor i enhver gruppe der indeholder den som normaldeler.

NOETHERS ISOMORFISÆTNINGER.

Nu to vigtige isomorfisætninger.

Noethers 1. isomorfisætning. *Lad H og K være undergrupper i gruppen G og antag $H \triangleleft G$; da er $H \cap K \triangleleft K$ og $HK/H \simeq K/H \cap K$.*

Bevis.

Lad κ betegne den kanoniske homomorfi af G på G/H, her betegnet G^*. Da er $\kappa(HK) = \kappa(K)$, $\kappa(HK) \supseteqq \kappa(K)$ triviel; den modsatte inklusion følger af $\kappa(hk) = \kappa(h)\kappa(k) = e^* \cdot \kappa(k) = \kappa(k) \in \kappa(K)$. Sæt $\kappa(K) = K^*$. Lad os betragte κ's restriktion til K, $\kappa_{\mathrm{Res},K}$; homomorfisætningen anvendt på $\kappa_{\mathrm{Res},K}$ giver: $K^* \simeq K/\operatorname{Ker}(\kappa_{\mathrm{Res},K})$. Nu er

$$\operatorname{Ker}(\kappa_{\mathrm{Res},K}) = \{x \in K | \kappa(x) = e^*\} = \{x \in K | x \in H\} = H \cap K\,.$$

Følgelig er $H \cap K \triangleleft K$ og $K/H \cap K \simeq K^*$.

Dernæst betragtes $\kappa_{\mathrm{Res},HK}$. Her er $\operatorname{Ker}(\kappa_{\mathrm{Res},HK}) = H$ og homomorfisætningen giver $HK/H \simeq \kappa(HK) = K^*$. Heraf fås $HK/H \simeq K/H \cap K$. □

Noethers 2. isomorfisætning. *Lad H være en normaldeler i gruppen G og κ den kanoniske homomorfi $G \xrightarrow[\kappa]{} G/H = G^*$. Da giver tilordningen $K \longrightarrow \kappa(K) \subseteq G^*$ og $K^* \longrightarrow \kappa^{-1}(K^*)$ en $1-1$ korrespondance mellem undergrupperne K i G indeholdende H og undergrupperne K^* i G^*. Ved denne korrespondance gælder $K \triangleleft G \iff \kappa(K) \triangleleft G^*$. Hvis $K \triangleleft G$, da er $G/K \simeq G^*/\kappa(K)$. (Hvis $\kappa(K)$ skrives K/H, kan isomorfien formuleres $G/K \simeq G/H \;\big/\; K/H$.)*

Bevis. Den påståede $1-1$ korrespondance eftervises ved at godtgøre

i) $\kappa^{-1}\kappa(K) = K$ for $H \subseteq K \subseteq G$,

ii) $\kappa\kappa^{-1}(K^*) = K^*$ for $K^* \subseteq G$.

Ad i) $\kappa^{-1}\kappa(K) \supseteq K$ er en almen mængdeteoretisk inklusion. Den modsatte inklusion følger af: $g \in \kappa^{-1}\kappa(K) \Rightarrow \kappa(g) = \kappa(k)$ for passende $k \in K \Rightarrow \kappa(gk^{-1}) = e^* \Rightarrow gk^{-1} \in \operatorname{Ker}\kappa = H \Rightarrow g \in HK \subseteq K$, da $H \subseteq K$.

Ad ii) $\kappa\kappa^{-1}(K^*) \subseteq K^*$ er en almen (triviel) mængdeteoretisk inklusion. Den modsatte inklusion følger af: $k^* \in K^* \Rightarrow k^* = \kappa(g)$ for passende $g \in G$. Dette g må tilhøre $\kappa^{-1}(K^*)$ dvs.: $k^* \in \kappa\kappa^{-1}(K^*)$.

"$\Rightarrow$"

$$K \triangleleft G \Rightarrow \kappa g \kappa k \kappa g^{-1} = \kappa(gkg^{-1}) \in \kappa K \text{ for } \forall k \in K,\ \forall g \in G$$
$$\text{dvs. } \kappa K \triangleleft G^* .$$

"$\Leftarrow$" Antag $K^* \triangleleft G^*$; lad $x \in \kappa^{-1}K^*$; da vil $\kappa(gxg^{-1}) = \kappa g \kappa x (\kappa g)^{-1} \in K^*\ \forall g \in G$. Følgelig er $g(\kappa^{-1}K^*)g^{-1} \subseteq \kappa^{-1}(K^*)\ \forall g \in G$; dvs. $\kappa^{-1}(K^*) \triangleleft G$.

Hvis $K \triangleleft G$ og κ^* er den kanoniske homomorfi af G^*/K^*, hvor $K^* = \kappa(K)$, da er $\kappa^*\kappa$ en surjektiv homomorfi af G på G^*/K^* med $\operatorname{Ker}\kappa^*\kappa = K$. Homomorfisætningen giver da $G/K \simeq G^*/K^*$. □

KOMMUTATORGRUPPER.

Lad A være en delmængde i gruppen G. Med $\{A\}$ betegner vi den mindste undergruppe i G der indeholder A. $\{A\}$ vil bestå af alle elementer der kan skrives på formen ${a_1}^{n_1} \dots {a_r}^{n_r}$, $a_1, \dots, a_r \in A$, $n_1, \dots, n_r \in \mathbb{Z}$, $r \in \mathbb{N}$. (Gentagelser tilladt). $\{A\}$ kaldes undergruppen frembragt af A.

For elementer a, b i en gruppe G kaldes løsningen $x = aba^{-1}b^{-1}$ til ligningen $ab = xba$ den til a, b svarende *kommutator*. Undergruppen i G frembragt af samtlige kommutatorer $aba^{-1}b^{-1}$ kaldes G's *kommutatorgruppe* og betegnes G' (den *"afledede"* *gruppe*). Ved en vilkårlig automorfi for G vil kommutatorerne (som helhed) føres over i sig selv. Derfor vil G' ved enhver automorfi gå over i sig selv, dvs. G' er karakteristisk undergruppe, specielt er $G' \triangleleft G$.

Den følgende sætning giver en karakterisering af kommutatorgruppen.

Sætning 11. *For en normaldeler H i G gælder:*

$$H \supseteq G' \iff G/H \text{ er abelsk}.$$

Med andre ord er G' den mindste normaldeler med abelsk faktorgruppe.

Bevis. "$\Rightarrow$" Alle kommutatorer ligger i H, dvs. $aba^{-1}b^{-1} \in H$ for $\forall a, b$, hvorfor: $a\ b\ a^{-1}\ b^{-1} = e$ i G/H. (Her betegner a (resp. b) a's sideklasse, (resp. b's sideklasse) i G/H). Altså er $a\ b = b\ a$ dvs.: G/H er abelsk.

"$\Leftarrow$" Lad a og b være vilkårlige elementer i G. Da gælder for de tilsvarende sideklasser i G/H $a\ b = b\ a$, hvorfor $\overline{aba^{-1}b^{-1}} = e$ og dermed $aba^{-1}b^{-1} \in H$. H indeholder altså samtlige kommutatorer, og derfor er $H \supseteq G'$. $\square$

Bemærkning. G abelsk $\iff G' = \{e\}$.

– – – – – – – – – – – – – – – –

GRUPPER AF GIVEN ENDELIG ORDEN.

Vi vil nu udlede nogle sætninger om grupper af given orden n for visse n, der specielt tillader bestemmelsen af grupperne af orden < 12.

For ethvert $n \in \mathbb{N}$ findes mindst én gruppe af orden n, nemlig den cykliske $\mathbb{Z}_n$.

For ethvert lige tal $2n$, $n \geqq 3$, findes mindst en ikke abelsk gruppe af orden $2n$, nemlig gruppen af alle drejninger og spejlinger der fører en regulær n-kant over i sig selv. Denne gruppe kaldes *diedergruppen* af orden $2n$ og betegnes D_n.

Sætning 12. *Hvis G har en orden, der er et primtal p, da er G cyklisk.*

Bevis. Ethvert fra e forskelligt element i G vil frembringe G. $\square$

Sætning 13. *Der findes netop to (ikke-isomorfe) grupper af orden 4, nemlig den cykliske $\mathbb{Z}_4$ og "Kleins Vierergruppe". V_4, dvs. alle matricer af formen $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ med sædvanlig matrixmultiplikation.*

Bevis. Det er klart, at $\mathbb{Z}_4$ og V_4 er ikke-isomorfe grupper af orden 4. Det er derfor nok at vise, at der højst findes én ikke-cyklisk gruppe af orden 4. G ej cyklisk $\Rightarrow$ ordenen af ethvert element $= 1$ eller 2 dvs.: ifølge Sætning 2 må G være abelsk. Vælg $a, b \in G$ så $e \neq a$, $e \neq b$, $a \neq b$. Da er G's elementer $\{e, a, b, ab\}$. Derfor er der kun èn mulighed for gruppetavlen. $\square$

Sætning 14. *Lad p være et ulige primtal; da findes netop to (ikke-isomorfe) grupper af orden $2p$, nemlig den cykliske $\mathbb{Z}_{2p}$ og den (ikke-abelske) diedergruppe D_p.*

Bevis. Det er klart, at $\mathbb{Z}_{2p}$ og D_p er ikke-isomorfe grupper af orden $2p$.

For at godtgøre, at der kun findes de to nævnte grupper af orden $2p$ viser vi, at der kun findes én ikke-cyklisk gruppe G af orden $2p$.

$1°$. *G har et element af orden p.* I modsat fald ville ethvert element i G have orden 1 eller 2, specielt ville G være abelsk. Lad $a \neq e$, $a^2 = e$; $A =$ undergruppen $\{e, a\}$ af orden 2. A er normal undergruppe, da G abelsk. $|G/A| = p$ dvs.: G/A cyklisk. Lad $\textcircled{g}$ være frembringerelement, altså $\textcircled{g} \neq \textcircled{e}$, $\overline{g^p} = \textcircled{e}$; dvs.: for en repræsentant g gælder $g \notin A$, $g^p \in A$. Men ethvert kvadrat i G er e, dvs.: $g^2 = e$; følgelig $g = g^p(g^2)^{-\frac{p-1}{2}} \in A$. Modstrid!

$2°$. *G har et element af orden* 2. Vises analogt med $1°$. (Her benyttes, at en undergruppe af orden p har index 2 og derfor er normaldeler i G.)

$3°$. Lad nu a være et element af orden p og b et element af orden 2. G består netop af elementerne $e, a, a^2, a^{p-1}, b, ba, ba^2, ba^{p-1}$. ab kan derfor skrives ba^j, $1 \leq j \leq p-1$. Lad A være den cykliske undergruppe $\{e, a, \ldots, a^{p-1}\}$ af orden p. Da $[G : A] = 2$, er $A \lhd G$ og G/A cyklisk af orden 2. Sideklassen $\overline{ab}$ i G/A har orden 2, hvorfor $\mathrm{Ord}(ab)$ indenfor G er 2 eller $2p$. Her er $2p$ udelukket, da G ellers var cyklisk i strid med den gjorte antagelse. Dvs.: $(ab)^2 = e$ eller $ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{p-1}$.

Hermed fastlægges entydigt hvorledes elementerne i G multipliceres, dvs. der er kun én mulighed for G's gruppetavle. □

Vi undersøger nu grupper, hvis orden er en primtalspotens.

DEFINITION. Gruppen G kaldes en *p-gruppe*, hvis $|G|$ er en potens af primtallet p.

Inden vi viser første sætning vedrørende p-grupper bringer vi nogle generelle overvejelser, som vi også får brug for ved senere lejligheder.

I en *vilkårlig* gruppe G (her *ikke nødvendigvis en p-gruppe*) indføres følgende ækvivalensrelation: Lad a og b være elementer i G. Da defineres $a \sim b \iff \exists g \in G$ så $a = gbg^{-1}$. (Det vises let, at $\sim$ virkelig er ækvivalensrelation). $a \sim b$ læses "a *konjugeret* med b". Herved inddeles G i ækvivalensklasser. For en endelig gruppe spørger vi nu: Hvor mange elementer indeholder ækvivalensklassen $\textcircled{a}$ indeholdende a? Hertil indføres $\mathcal{C}_a = \{g \in G \mid ga = ag\}$. $\mathcal{C}_a$ er en undergruppe i G og betegnes *centralisatoren* for a.

Elementerne i $\textcircled{a}$ er $\{gag^{-1} \mid g \in G\}$. For disse gælder

$$g_1 a g_1^{-1} = g_2 a g_2^{-1} \iff g_2^{-1} g_1 a = a g_2^{-1} g_1 \iff g_2^{-1} g_1 \in \mathcal{C}_a$$

$\iff g_1 \underset{h}{\sim} g_2$ med hensyn til $\mathcal{C}_a$. Følgelig bliver de indbyrdes forskellige elementer i $\textcircled{a}$ netop $\{g_i a g_i^{-1}\}$, hvor g_i gennemløber et fuldstændigt repræsentantsystem for højresideklasserne i G m.h.t. $\mathcal{C}_a$. Antallet af elementer i $\textcircled{a}$ er altså $[G : \mathcal{C}_a]$.

Vi bemærker, at $[G : \mathcal{C}_a] = 1 \iff \mathcal{C}_a = G \iff ag = ga \; \forall g \in G \iff a \in Z(G) =$ centrum for G. Ækvivalensklassen a består altså kun af elementet a netop når a ligger i centret $Z(G)$.

Antag nu, at G er en endelig gruppe. Hvis $a \notin Z(G)$, er $[G : \mathcal{C}_a] > 1$ og ved direkte optælling fås den såkaldte "*klasseligning*"

$$|G| = |Z(G)| + \sum_{\substack{\text{visse } a \\ [G:\mathcal{C}_a]>1}} [G : \mathcal{C}_a]$$

hvor den sidste summation udstrækkes over et repræsentantsystem for de ækvivalensklasser der indeholder mere end 1 element.

Antag nu atter, at G er en p-gruppe. Hvis $[G : \mathcal{C}_a] > 1$, vil $[G : \mathcal{C}_a]$ være delelig med p. Idet $|G|$ er delelig med p, viser klasseligningen, at $p \mid |Z(G)|$, dvs. centret for G er ikke trivielt. Vi har altså vist

Sætning 15. *Centret af en p-gruppe er ikke-trivielt.*

For den efterfølgende anvendelse får vi brug for

Lemma. *Lad G være en gruppe for hvilken $G/Z(G)$ $(\simeq \mathrm{Aut}_i(G))$ er cyklisk. Da er G abelsk.*

Bevis. Antag $G/Z(G)$ er frembragt af sideklassen g. Lad x og y være to vilkårlige elementer i G. Da findes hele tal i og j så

$$\begin{aligned} x &= g^i z_1 \qquad z_1 \in Z(G) \\ y &= g^j z_2 \qquad z_2 \in Z(G)\,. \end{aligned}$$

Vi får nu

$$\begin{aligned} xy &= \; g^i z_1 g^j z_2 = g^{i+j} z_1 z_2 \\ yx &= \; g^j z_2 g^i z_1 = g^{j+i} z_2 z_1 = g^{i+j} z_1 z_2\,. \end{aligned}$$

Altså er G abelsk. $\square$

Sætning 16. *Hvis p er et primtal findes netop to ikke-isomorfe grupper af orden p^2, nemlig den cykliske $\mathbb{Z}_{p^2}$ og gruppen af diagonalmatricer af formen*

$$\begin{pmatrix} e^{\frac{2\pi i a}{p}} & 0 \\ 0 & e^{\frac{2\pi i b}{p}} \end{pmatrix}, \quad a, b \in \mathbb{Z}\,.$$

Disse er begge abelske.

Bevis. Det er klart, at de nævnte grupper af orden p^2 er ikke-isomorfe. For at vise at disse er de eneste grupper af orden p^2, er det nok at godtgøre, at der højst er én ikke-cyklisk gruppe af orden p^2.

Ifølge sætning 15 og det efterfølgende lemma må en gruppe af orden p^2 være abelsk.

Lad nu G være en ikke-cyklisk gruppe af orden p^2. Hvis a er et element $\neq e$, må a have orden p. Undergruppen $A = \{e, a, \dots, a^{p-1}\}$ har orden p. Lad b være et element der ikke ligger i A; da har undergruppen $B = \{e, b, \dots, b^{p-1}\}$ orden p. Da G er abelsk, er AB en undergruppe af orden $> p$. Da G har orden p^2, må $AB = G$. Ethvert element i G kan da entydigt skrives på formen $a^i b^j$, $0 \leqq i < p$, $0 \leqq j < p$, og der gælder $\left(a^{i_1} b^{j_1}\right)\left(a^{i_2} b^{j_2}\right) = a^{i_1+i_2} b^{j_1+j_2}$. Idet $a^p = b^p = e$, er gruppetavlen for G hermed entydigt bestemt. $\square$

Ud fra ovenstående sætninger kan vi nu udfylde skemaet

Orden	2	3	4	5	6	7	8	9	10	11
Antal grupper	1	1	2	1	2	1		2	2	1
Heraf ikke-abelske	0	0	0	0	1	0		0	1	0

For at bestemme grupperne af orden 8 angiver vi først explicit visse sådanne grupper, og viser derefter at der ikke findes andre.

Af abelske grupper findes udover I) $\mathbb{Z}_8$ følgende:

II) alle matricer af formen $\begin{pmatrix} i^a & 0 \\ 0 & \pm 1 \end{pmatrix}$ $a = 0, 1, 2, 3$ $(i = \sqrt{-1})$;

III) alle matricer af formen $\begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & \pm 1 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}$.

Af ikke-abelske grupper findes

IV) Diedergruppen D_4 (dvs.: alle drejninger og spejlinger der fører et kvadrat over i sig selv).

V) Quaterniongruppen dvs.: de quaternioner $a_0\mathbf{1} + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$, hvor én af koeefficienterne er ± 1 og de øvrige 0 dvs. $\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}$.(Se appendiks 1.)

Ved at betragte elementordenerne ses, at grupperne II) og III) ikke er isomorfe.

Elementordenerne i IV) er: 1, 2, 2, 2, 2, 2, 4, 4.

Elementordenerne i V) er: 1, 2, 4, 4, 4, 4, 4, 4.

Altså er IV) og V) ikke isomorfe. Da IV) og V) er ikke-abelske, giver I), II), III), IV), V) 5 ikke-isomorfe grupper af orden 8.

Vi viser nu, at – pånær isomorfi – er I), II), III) de eneste abelske grupper af orden 8. I analogi med tidligere beviser skal vi godtgøre, at der kun findes 2 muligheder for gruppetavlen for en ikke-cyklisk abelsk gruppe G af orden 8.

Da G ikke er cyklisk, er de mulige elementordener 1, 2, 4. Antag først at G indeholder et element a af orden 4. Lad A være den cykliske undergruppe $\{e, a, a^2, a^3\}$ af orden 4 og lad b være et element $\neq e$ i faktorgruppen G/A af orden 2. Da vil $b^2 \in A$, og idet $b^4 = e$, må gælde $b^2 = e$ eller $b^2 = a^2$. Hvis $b^2 = a^2$ er $(ba)^2 = e$ og man kan derfor ved i givet fald at erstatte b med ba (der repræsenterer samme sideklasse i G/A) antage, at $b^2 = e$. Elementerne i G bliver da $e, a, a^2, a^3, b, ba, ba^2, ba^3$. Da G abelsk, vil G's gruppetavle hermed være entydigt bestemt.

Antag dernæst, at G ikke indeholder noget element af orden 4, dvs. $g^2 = e \; \forall g \in G$. Ifl. sætning 2 er G abelsk. Vælg $a \in G$, $a \neq e$ og $b \in G$, $b \neq a$ $b \neq e$. Da er e, a, b, ab indbyrdes forskellige. Vælg endelig $c \in G$, $c \notin \{e, a, b, ab\}$. G's elementer bliver da netop $e, a, b, ba, c, ca, cb, cab$. Da G er abelsk og alle kvadrater er lig e, er G's gruppetavle hermed entydigt bestemt.

Tilbage står nu at bestemme de ikke-abelske grupper af orden 8. Vi skal godtgøre, at der kun findes to mulige gruppetavler. Lad nu G være en ikke-abelsk gruppe af orden 8.

Da G ej abelsk, findes et element a af orden 4. Den cykliske undergruppe $A = \{e, a, a^2, a^3\}$ er normal i G, da $[G : A] = 2$. Lad $b \in G/A$ være element $\neq e$ $\overline{b^2} = e$ dvs. $b^2 \in A$. Hvis b^2 var $= a$ eller a^3, ville G være cyklisk med b som frembringer i strid med, at G var antaget ikke-abelsk. Følgelig må $\underline{b^2 = e}$ eller $\underline{b^2 = a^2}$. G's elementer er $e, a, a^2, a^3, b, ba, ba^2, ba^3$. For produktet ab findes a priori følgende muligheder:

$$ab = \begin{cases} b \\ ba^2 \\ ba^3 \\ ba \end{cases}$$

Her er $ab = b$ udelukket, da $a \neq e$. $ab = ba$ ville medføre G abelsk. $ab = ba^2$ ville medføre: $a = ba^2b^{-1} \Rightarrow a^2 = ba^2b^{-1}ba^2b^{-1} = e$ modstrid! Altså er $ab = ba^3$. Følgelig findes kun to mulige gruppetavler svarende til $b^2 = e$ og $b^2 = a^2$.

Hermed er bestemmelsen af grupperne af orden 8 afsluttet.

Bemærkning. Quaterniongruppen har en bemærkelsesværdig egenskab. Den er ikke abelsk, men samtlige undergrupper er normale. (Bevisskitse: Quaterniongruppen har kun ét element af orden 2.)

Vi kan nu fuldstændiggøre skemaet angående grupper af given orden.

Orden	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Antal grupper	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1	5	1
Heraf ikke-abelske	0	0	0	0	1	0	2	0	1	0	3	0	1	0	9	0	3	0

Resultaterne for orden 12, 15 16 og 18 angivet uden bevis.

Opgave. Angiv 2 abelske grupper af orden 12. Diedergruppen D_6 og den alternerende gruppe A_4 (jfr. senere) er ikke-isomorfe ikke-abelske grupper af orden 12. Den tredie ikke-abelske gruppe af orden 12 kan fås som følger: Alle regulære (2×2)-matricer med komplekse elementer udgør en gruppe. Undergruppen heri, frembragt af matricerne

$$\underset{=}{A} = \begin{pmatrix} e^{\frac{2\pi i}{3}} & 0 \\ 0 & e^{\frac{4\pi i}{3}} \end{pmatrix} \quad \text{og} \quad \underset{=}{B} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

er en ikke-abelsk gruppe af orden 12. Elementerne er $\underset{=}{A}^{\mu}\underset{=}{B}^{\nu}$, $\mu = 0, 1, 2$, $\nu = 0, 1, 2, 3$ $\underset{=}{A}^3 = \underset{=}{B}^4 = \underset{=}{E}$ og $\underset{=}{B}\underset{=}{A}\underset{=}{B}^{-1} = \underset{=}{A}^2$. Gruppen er ikke isomorf med D_6 eller A_4.

FLYTNINGSGRUPPER.

Vi skal nu betragte visse endelige grupper der har en simpel geometrisk interpretation.

Tetraedergruppen *T*. Alle (egentlige) drejninger i rummet der fører et regulært tetraeder over i sig selv. Den består af: Identiteten + 3 drejninger på 180° (om akserne forbindende modstående kantmidtpunkter) + 8 drejninger på 120° og 240° om højderne, dvs. T har orden 12. Ved betragtning af hjørnerne ses, at $T = A_4$. Til bestemmelsen af normaldelerne i T kan vi bruge nogle almene overvejelser.

Lad M være en abstrakt mængde og G en gruppe af transformationer (dvs.: bijektive afbildninger) af M på sig selv. For $a \in M$ vil de afbildninger φ i G, der holder a invariant, dvs. $\varphi(a) = a$, udgøre en undergruppe G_a i G.

Denne undergruppe kaldes *stabilitetsgruppen* for a.

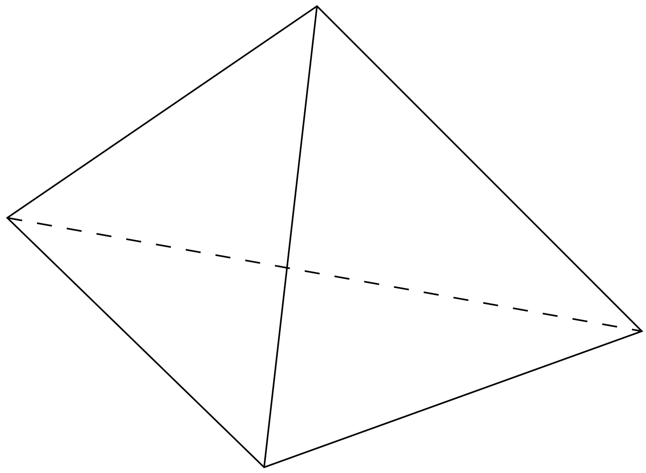
Da gælder:

Sætning 17. *Lad M være en abstrakt mængde og G en gruppe af transformationer (dvs.: bijektive afbildninger) af M på sig selv. For $a \in M$ lad G_a være stabilitetsgruppen for a. Da gælder for ethvert $\psi \in G : \psi \circ G_a \circ \psi^{-1} = G_{\psi(a)}$.*

Bevis. Lad ϕ ligge i G_a. Da er $(\psi \circ \phi \circ \psi^{-1}) \circ \psi(a) = \psi(a)$, hvilket indebærer, at $\psi \circ G_a \circ \psi^{-1} \subseteq G_{\psi(a)}$.

Lad omvendt ρ tilhøre $G_{\psi(a)}$. Da er $\rho(\psi(a)) = \psi(a)$, hvorfor $(\psi^{-1} \circ \rho \circ \psi)(a) = a$, dvs. $\psi^{-1} \circ \rho \circ \psi \in G_a$. Det betyder netop, at $\rho \in \psi \circ G_a \circ \psi$, eller $G_{\psi(a)} \subseteq \psi \circ G_a \circ \psi^{-1}$. $\square$

Ved anvendelse af denne sætning på T (M tages som hjørnerne i tetraedret) ses, at den eneste ikke-trivielle normaldeler i T er den undergruppe i T, som fører det i tetraedret indlagte treretvinklede koordinatsystem (se model/figur) over i sig selv. Denne undergruppe er isomorf med V_4.



Hexaedergruppen $\mathcal{H}$. Alle (egentlige) drejninger i rummet der fører en terning over i sig selv, orden 24, $\mathcal{H} \simeq S_4$ (betragt rumdiagonalerne). Ved overvejelser som ovenfor ses, at $\mathcal{H}$ kun indeholder to ikke-trivielle normaldelere, nemlig undergruppen i $\mathcal{H}$ bestående af de drejninger, der fører et i terningen indskrevet tetraeder over i sig selv samt undergruppen $\mathcal{K}$ bestående af de drejninger der fører akserne forbindende modstående sideflademidtpunkter over i sig selv (akseretningerne kan vendes). Sidstnævnte gruppe $\mathcal{K}$ er $\simeq V_4$, og der gælder $\mathcal{H}/\mathcal{K} \simeq S_3$.

Heraf sluttes specielt:

$$\begin{aligned} \mathcal{H}' &= T \\ \mathcal{H}'' &= T' = V_4 \\ \mathcal{H}''' &= T'' = V_4' = e\,. \end{aligned}$$

Bemærkning. Hexaedergruppen = oktaedergruppen, dvs. de drejninger der fører et regulært oktaeder over i sig selv.

Ikosaedergruppen $\mathcal{I}$. Alle (egentlige) drejninger, der fører et regulært ikosaeder over i sig selv. (Se model). Orden af $\mathcal{I}$: 60 $\mathcal{I} \simeq$ Alternerende gruppe A_5 (se model).

Ved argumenter udnyttende Sætning 17 ses, at $\mathcal{I}$ er en simpel gruppe.

Bemærkning. Man kan vise, at $\mathbb{Z}_n$, D_n, T, $\mathcal{H}$ og $\mathcal{I}$ er de eneste endelige drejningsgrupper i rummet. Anderledes udtrykt udgør disse (på nær ortogonal ækvivalens) de eneste endelige undergrupper i den egentligt ortogonale gruppe $O_3^+(\mathbb{R})$. ($O_3^+(\mathbb{R})$ kan iøvrigt vises at være simpel og er således et eksempel på en uendelig simpel gruppe.)

– – – – – – – – – – – – – – – –

PERMUTATIONSGRUPPER.

Lad Ω være en vilkårlig mængde ($\neq \emptyset$) og $S(\Omega)$ mængden af alle bijektive afbildninger af Ω på Ω. Med sammensætning som komposition udgør $S(\Omega)$ en gruppe. Hvis Ω er endelig, f.eks. $\Omega = \{1, 2, \ldots, n\}$ er $S(\Omega)$ *den symmetriske gruppe* S_n.

Ved en *permutationsgruppe på* Ω forstås en undergruppe af $S(\Omega)$. Vi bringer først nogle almene begreber og sætninger for vilkårlige Ω, og specialiserer os siden til endelige Ω.

Definition. En permutationsgruppe G på Ω kaldes *transitiv*, hvis der til ethvert par (a, b), $a, b \in \Omega$ findes et $\sigma \in G$ så $\sigma(a) = b$.

Definition. En permutationsgruppe G på Ω kaldes *dobbelt transitiv*, hvis der til vilkårlige $a, b, c, d \in \Omega$ $a \neq b$ og $c \neq d$ findes $\sigma \in G$ så $\sigma(a) = c$ og $\sigma(b) = d$.

Bemærkning. Åbenbart gælder: dobbelt transitiv $\Rightarrow$ transitiv.

Enhver gruppe kan opfattes som en permutationsgruppe, idet der gælder følgende

Cayley's sætning. *Lad G være en vilkårlig gruppe. Da findes en injektiv homomorfi φ af G på en transitiv undergruppe i $S(G)$. Specielt er en gruppe af endelig orden n isomorf med en transitiv undergruppe i den symmetriske gruppe S_n.*

Bevis. For $g \in G$ lad φ_g være følgende element i $S(G)$:

$$\varphi_g(x) = g \circ x\,, \qquad x \in G\,.$$

φ_g er en bijektiv afbildning af G på G, dvs. φ_g er et veldefineret element i $S(G)$. På grund af den associative lov for gruppemultiplikation gælder

$$\varphi_{g_1 \circ g_2} = \varphi_{g_1} \circ \varphi_{g_2}$$

dvs. φ er en homomorfi af G ind i $S(G)$.

Endvidere er

$$\mathrm{Ker}(\varphi) = \{g \in G \mid \varphi_g = Id_G\} = \{g \in G \mid g \circ x = x \; \forall x \in G\} = \{e\}\,.$$

Altså er φ injektiv.

Billedet af G ved φ er en transitiv undergruppe i $S(G)$; thi hvis a og b er vilkårlige elementer i G, da er $\varphi_g(a) = b$ for $g = ba^{-1}$. $\square$

Ofte kan en generalisering af Cayley's sætning for endelige grupper være nyttig.

Lad H være en undergruppe i gruppen G med indeks $[G : H] = n$, $n \in \mathbb{N}$, og lad $G = \bigcup_{i=1}^{n} g_i H$ være inddelingen af G i disjunkte højresideklasser m.h.t. H. Vi kan for eksempel antage $g_1 = e$.

For ethvert $g \in G$ vil $G = \bigcup_{i=1}^{n} gg_iH$ igen være inddelingen af G i disjunkte højresideklasser m.h.t. H, hvorfor

$$\begin{pmatrix} g_1H & g_2H & \cdots & g_nH \\ gg_1H & gg_2H & \cdots & gg_nH \end{pmatrix}$$

vil være en permutation af sideklasserne g_iH, $1 \leq i \leq n$, og derfor kan opfattes som element i den symmetriske gruppe S_n. Vi definerer en afbildning $\rho : G \to S_n$ ved

$$\rho g = \begin{pmatrix} g_1H & g_2H & \cdots & g_nH \\ gg_1H & gg_2H & \cdots & gg_nH \end{pmatrix}$$

og skriver $gg_iH = g_{\rho(g)[i]}H$, $1 \leq i \leq n$.

Det ses let – i analogi med det ovenstående bevis for Cayley's sætning – at ρ er en homomorfi, og at ρG er en transitiv undergruppe i S_n. Ordenen af ρG er da delelig med n (hvorfor?)

For kernen af ρ gælder

$$\operatorname{Ker}(\rho) = \bigcap_{i=1}^{n} g_iHg_i^{-1} \subseteq H \quad \text{og} \quad \operatorname{Ker}\rho \triangleleft G \quad \text{med} \quad G/\operatorname{Ker}\rho \simeq \rho G\ .$$

Åbenbart er $\operatorname{Ker}(\rho)$ den største i H indeholdte undergruppe, der er normaldeler i G.

Bemærkning. Hvis $H = \{e\}$ fås Cayley's sætning for endelige grupper.

Vi giver nu nogle små sætninger vedrørende dobbelt transitive permutationsgrupper.

Sætning 18. *Lad N være en normaldeler $\neq \{e\}$ i en dobbelt transitiv permutationsgruppe G på Ω. Da er N transitiv.*

Bevis. Lad $a, b \in \Omega$, $a \neq b$. Vi søger $\sigma \in N$ så $\sigma(a) = b$. Da $N \neq \{e\}$ findes $c \neq d$ i Ω så $\overline{\sigma}(c) = d$ for passende $\overline{\sigma} \in N$. Da G er dobbelt transitiv, findes $\tau \in G$ så $\tau(c) = a$ og $\tau(d) = b$. Men så gælder $\tau\,\overline{\sigma}\,\tau^{-1}(a) = b$. Da $N \triangleleft G$ er $\tau\,\overline{\sigma}\,\tau^{-1} \in N$ dvs.: $\tau\,\overline{\sigma}\,\tau^{-1}$ er et brugbart σ. □

Definition. Lad G være permutationsgruppe på Ω. For $a \in \Omega$ kaldes $G_a = \{\sigma \in G \mid \sigma(a) = a\}$ G's stabilitetsgruppe i Ω. (G_a ses straks at være undergruppe i G.)

Sætning 19. *Lad G være dobbelt transitiv permutationsgruppe på Ω, hvor $|\Omega| > 1$. Da er G_a en maximal undergruppe i G, dvs.: ingen undergrupper ligger strengt mellem G_a og G.*

Bevis. Lad $\mathcal{H}$ være undergruppe i G og antag $\mathcal{H} \underset{\neq}{\supset} G_a$. Vi skal da vise at $\mathcal{H} = G$. Der findes $\tau \in \mathcal{H}$ så $\tau(a) = b$, $b \neq a$. Lad ρ være vilkårlig i G, og lad $\rho(a) = c$.

Hvis $c = a$ er $\rho \in \mathcal{H}$ og vi er færdige. Vi kan derfor antage $c \neq a$. Da G er dobbelt transitiv, findes $\sigma \in G$ for hvilket $\sigma(a) = a$, $\sigma(b) = c$. Specielt er $\sigma \in G_a$. $\sigma\tau(a) = c$ hvorfor $\rho^{-1}\sigma\tau(a) = a$ dvs. $\rho^{-1}\sigma\tau \in G_a \subsetneqq \mathcal{H}$; da $\sigma, \tau \in \mathcal{H}$, ses heraf, at $\rho \in \mathcal{H}$. Da ρ var vilkårlig i G, ses at $\mathcal{H} = G$. □

Vi får nu et kriterium for simpelhed som vi ved en senere lejlighed har brug for.

Sætning 20. *Lad G være en dobbelt transitiv permutationsgruppe på Ω $(|\Omega| > 1)$. Da er G simpel, hvis*

i) *$G = G'$ (G' betegner kommutatorgruppen for G).*
ii) *Der findes $a \in \Omega$ så G_a indeholder en abelsk normaldeler K så G er frembragt af de med K konjugerede mængder $\{\sigma K \sigma^{-1} \mid \sigma \in G\}$.*

Bevis. Antag $\{e\} \neq N \lhd G$; vi skal da vise, at $N = G$. Vælg et $a \in \Omega$ så ii) gælder. G_a er maximal så $G_a N$ er $= G_a$ eller G. Da N ifølge Sætning 18 er transitiv og G_a ikke er transitiv (idet $|\Omega| > 1$) er muligheden $G_a N = G_a$ udelukket. Dvs. $G = G_a N$. Vi påstår nu, at $NK \lhd G$. (Bemærk, at NK er en undergruppe, da $N \lhd G$). Da $G = G_a N$ $(= N G_a)$, kan ethvert element i G skrives $\nu\sigma$, hvor $\nu \in N$, $\sigma \in G_a$, og vi har, da $N \lhd G$ og $K \lhd G_a$

$$\nu\sigma N K \sigma^{-1}\nu^{-1} = N\nu\sigma K \sigma^{-1}\nu^{-1} = N\nu(\sigma K \sigma^{-1})\nu^{-1} = N\nu K \nu^{-1} = NK\,.$$

Da $K \subsetneqq NK \lhd G$, gælder

$$\forall \sigma \in G : \sigma K \sigma^{-1} \subsetneqq \sigma N K \sigma^{-1} = NK\,.$$

På grund af ii) findes ingen ægte undergruppe i G indeholdende $\sigma K \sigma^{-1}$ for alle $\sigma \in G$. Følgelig fås $NK = G$.

Vi udnytter nu i): $G = G'$. Enhver kommutator kan skrives $(nk)(n_1k_1)(nk)^{-1}(n_1k_1)^{-1}$ hvor n og $n_1 \in N$, k og $k_1 \in K$. Da K er abelsk kan dette udtryk reduceres til $nkn_1k_1k^{-1}n^{-1}k_1^{-1}n_1^{-1} = nkn_1k^{-1}k_1n^{-1}k_1^{-1}n_1^{-1}$ der tilhører N, da $N \lhd G$. Men dette indebærer $G = G' \subseteq N$ dvs. $G = N$. □

Vi betragter nu nærmere tilfældet, hvor Ω er endelig og sætter $\Omega = \{1, 2, \ldots, n\}$. $S(\Omega)$ er da den symmetriske gruppe S_n. S_n har orden $n!$ De lige permutationer i S_n udgør en undergruppe A_n i S_n. A_n kaldes den *alternerende gruppe*. Dens orden er $\frac{1}{2}n!$ Åbenbart gælder: $A_n \lhd S_n$.

Definition. En permutation $\sigma \in S_n$ kaldes en *cykel*, hvis den er af formen $\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \\ a_2 & a_3 & \cdots & a_k & a_1 \end{pmatrix}$. Her er underforstået, at de fra $a_1, \ldots, a_k$ forskellige elementer er fixe ved σ. k kaldes cyklens længde. σ betegnes kort $(a_1, \ldots, a_k)$. En cykel af længde 2 er en *transposition*.

Sætning 21. *Enhver permutation $\sigma \in S_n$ kan på en og kun én måde skrives som produkt af cykler af indbyrdes disjunkte elementer.*

Bevis. **1) Eksistens**. For et $a \in \{1, 2, \dots, n\}$ betragtes elementerne $a, \sigma a, \sigma^2 a, \dots$. Hvis k er det mindste tal for hvilket $\sigma^k a = a$, er $a, \sigma a, \dots, \sigma^{k-1}a$ indbyrdes forskellige elementer. Hvis $k = n$ er σ selv en cykel $\begin{pmatrix} a & \sigma a & \cdots & \sigma^{k-1}a \\ \sigma a & \sigma^2 a & \cdots & a \end{pmatrix}$ og vi er færdige; hvis $k < n$ vælger vi $b \in \{1, \dots, n\} \setminus \{a, \sigma a, \dots, \sigma^{k-1}a\}$ og betragter $b, \sigma b, \sigma^2 b, \dots$ og tilhørende mindste ℓ for hvilket $\sigma^\ell(b) = b$. Elementerne $a, \sigma a, \dots, \sigma^{k-1}a, b, \sigma b, \dots, \sigma^{\ell-1}(b)$ er indbyrdes forskellige. Hvis $k + \ell = n$ da er

$$\sigma = \begin{pmatrix} a \cdots, \sigma^{k-1}(a) \\ \sigma a \qquad\quad a \end{pmatrix} \begin{pmatrix} b \cdots, \sigma^{\ell-1}(b) \\ \sigma b \qquad\quad b \end{pmatrix}$$

og vi er færdige. Hvis $k+\ell < n$ vælges $c \in \{1, \dots, n\} \setminus \{a, \dots, \sigma^{k-1}(a), b, \dots, \sigma^{\ell-1}(b)\}$ og vi betragter $c, \sigma c, \dots$ etc. Denne proces stopper efter endelig mange skridt.

2) Entydighed. Lad $\sigma = \tau_1 \dots \tau_s = \tau'_1 \dots \tau'_t$ være to fremstillinger af σ som produkt af indbyrdes disjunkte cykler (bemærk faktorernes rækkefølge er ligegyldig, da cykler af indbyrdes disjunkte elementer er ombyttelige). Alle cykler kan naturligvis antages at have længde > 1. Lad a være element så $\tau_1(a) \neq a$, og lad τ'_i være cyklen bl. $\tau'_1, \dots, \tau'_t$ for hvilken $\tau'_i(a) \neq a$. Hvis k er mindste tal for hvilket $\sigma^k a = a$, gælder $\tau_1 = \begin{pmatrix} a \cdots \sigma^{k-1}a \\ \sigma a \qquad a \end{pmatrix} = \tau'_i$; etc. □

Korollar. *Enhver permutation $\sigma \in S_n$ er produkt af transpositioner.*

Bevis. Det er nok at se på en cykel:

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \\ a_2 & a_3 & & a_k & a_1 \end{pmatrix} = \begin{pmatrix} a_1 & a_k \\ a_k & a_1 \end{pmatrix} \begin{pmatrix} a_1 & a_{k-1} \\ a_{k-1} & a_1 \end{pmatrix} \cdots \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}$$

□

Bemærkning. En cykel af lige længde er en ulige permutation.

En cykel af ulige længde er en lige permutation.

Sætning 22. *For $n > 2$ er centrum af S_n lig $\{e\}$.*

Bevis. Antag $\sigma \neq e$. Ved passende nummerering kan vi antage:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots \\ 2 & a & \cdots \end{pmatrix}$$

i) $a = 1$: For $\tau = \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$ gælder $\sigma\tau \neq \tau\sigma$, idet $\sigma\tau(2) = 1$ og $\tau\sigma(2) = 3$.

ii) $a \neq 1$: For $\tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ gælder $\sigma\tau \neq \tau\sigma$, idet $\tau\sigma(1) = 1$ og $\sigma\tau(1) = a$, $a \neq 1$.

Altså har vi vist: $\forall \sigma \in S_n \setminus \{e\}\ \exists \tau \in S_n$, så $\sigma\tau \neq \tau\sigma$. □

Korollar. $\mathrm{Aut}_i(S_n) = S_n$ *for* $n > 2$.

Bemærkning. Man kan vise, at for $n \neq 2$, $n \neq 6$ er S_n fuldstændig dvs.: $\mathrm{Aut}(S_n) = S_n$.

Den efterfølgende sætning er særdeles vigtig, ikke mindst med henblik på anvendelser i Galoisteori.

Sætning 23 (Galois). *For* $n \geqq 5$ *er den alternerende gruppe* A_n *simpel.*

Bevis. Lad $N \lhd A_n$, $N \neq \{e\}$. Vi skal da vise, at $N = A_n$. Da $N \lhd A_n$ vil $\tau^{-1}\sigma^{-1}\tau\sigma \in N$ for alle $\sigma \in N$ og alle $\tau \in A_n$. Vi vælger $\sigma \in N$, $\sigma \neq e$, og skelner mellem forskellige muligheder for σ's kanoniske fremstilling som produkt af indbyrdes disjunkte cykler. For hvert af tilfældene vælges et $\tau \in A_n$ som følger:

σ	τ	$\tau^{-1}\sigma^{-1}\tau\sigma$
$(abcd...)(...)$	(bcd)	(adc)
$(abc)(de...)(...)$	(bce)	$(aecbd)$
(abc)	(bcd)	$(ad)(bc)$
$(ab)(cd)(...)$	(abc)	$(ad)(bc)$

N må altså indeholde en permutation, der er produkt af to disjunkte transpositioner.

Ved passende nummerering kan vi derfor antage $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in N$.

Påstand: $\begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix} \in N$, hvor a, b, c og d er 4 vilkårlige indbyrdes forskellige blandt cifrene $\{1, \cdots, n\}$.

Betragt en vilkårlig permutation af formen $\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots \\ a & b & c & d & \cdots \end{pmatrix}$; idet

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots \\ a & b & c & d & \cdots \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots \\ b & a & c & d & \cdots \end{pmatrix}$$

kan vi antage, at

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots \\ a & b & c & d & \cdots \end{pmatrix}$$

er lige. Da er

$$\tau \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \tau^{-1} = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix} \in N\,.$$

Følgelig indeholder N samtlige produkter af to transpositioner af indbyrdes forskellige elementer. Da ethvert $\sigma \in A_n$ er produkt af et lige antal transpositioner, vil beviset være færdigt, når vi har godtgjort, at en permutation $\begin{pmatrix} x & y \\ y & x \end{pmatrix} \begin{pmatrix} y & z \\ z & y \end{pmatrix}$ er produkt af permutationer af ovennævnte art. Men dette følger af: $(xy)(yz) = (xy)(uv)(uv)(yz)$, hvor u og v er valgt forskellige fra x, y og z. (Her udnyttes $n \geqq 5$.) $\square$

Bemærkning. For $n = 2$ er $A_n = \{e\}$; for $n = 3$ er $A_n \simeq \mathbb{Z}_3$, dvs. simpel. For $n = 4$ er $A_n \simeq$ Tetraedergruppen, der – som tidligere vist – indeholder en ægte normaldeler ($\simeq V_4$) og derfor ikke er simpel.

Sætning 24. *For $n \geqq 5$ er A_n eneste ikke-trivielle normaldeler i S_n.*

Bevis. Antag $N \lhd S_n$; vi skal vise $N = \{e\}$, A_n eller S_n.

1) $N \subseteqq A_n \Rightarrow N \lhd A_n \underset{\text{(Galois'sætning)}}{\Rightarrow} N = A_n$ eller $\{e\}$.

2) $N \nsubseteqq A_n \Rightarrow NA_n \underset{\neq}{\supset} A_n \Rightarrow NA_n = S_n$.

Vi anvender Noethers 1. isomorfisætning på:

$$\begin{tikzcd}
& S_n \arrow[d, equal] & \\
& NA_n \arrow[dl, dash] \arrow[dr, dash] & \\
N \arrow[dr, dash] & & A_n \arrow[dl, dash] \\
& N \cap A_n \arrow[d, dash] & \\
& \{e\} &
\end{tikzcd}$$

$A_n \cap N \lhd A_n \Rightarrow A_n \cap N = \{e\}$ eller $A_n \cap N = A_n$. $A_n \cap N = A_n \Rightarrow A_n \subseteq N$, hvilket på grund af $N \nsubseteq A_n$ indebærer $N = S_n$. $A_n \cap N = \{e\} \Rightarrow N =$ gruppe af orden 2. Lad $g \in N$, $g \neq e$. For ethvert $\sigma \in S_n$ ville da $\sigma g \sigma^{-1} \in N$, dvs. $\sigma g \sigma^{-1} = g$ for alle $\sigma \in S_n$. Følgelig var $g \neq e$ i centrum for S_n. Men ifølge Sætning 22 har S_n trivielt centrum. $\square$

Korollar. *For $n \geqq 5$ gælder $S_n' = A_n$; $S_n'' = A_n' = A_n$.*

Bemærkning.

For $n = 2$ gælder $S_2' = e$.
For $n = 3$ gælder $S_3' = A_3$; $S_3'' = A_3' = e$.
For $n = 4$ gælder $S_4' = A_4$; $S_4'' = A_4' = V_4$; $S_4''' = A_4'' = V_4' = e$.

Eksempel. Som tidligere nævnt findes uendelige simple grupper. Ud fra det foregående giver vi endnu et eksempel. Lad $\Omega = \{1, 2, \dots\} = \mathbb{N}$ og lad $S_{\mathbb{N}}$ være undergruppen i $S(\Omega)$ bestående af alle $\sigma \in S(\Omega)$ for hvilke $\sigma(a) = a$ for alle $a > k(\sigma)$, hvor $k(\sigma)$ er et naturligt tal afhængigt af σ. Undergruppen $A_{\mathbb{N}}$ svarende til de lige permutationer er en uendelig simpel gruppe. (Skriv $A_{\mathbb{N}} = \cup_{n=1}^{\infty} A_n$ og benyt Galois' sætning).

Øvelse. Giv et eksempel på en følge $G_1 \supseteq G_2 \supseteq G_3 \supseteq \dots$ af simple grupper for hvilken $\cap_{n=1}^{\infty} G_n$ ej er simpel.

— — — — — — — — — — — — — — — —

NORMALRÆKKER.

Ved en *normalrække* i gruppen G forstås en følge af undergrupper

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{s-1} \triangleright G_s = \{e\}\,, \qquad (*)$$

hvor hver G_i er normaldeler i den foregående G_{i-1}. Faktorgrupperne G_0/G_1, G_1/G_2, $G_2/G_3, \dots, G_{s-1}/G_s = G_{s-1}$ kaldes normalrækkens *faktorer*. Antallet af faktorer, s, er normalrækkens *længde*. Normalrækken siges at være uden gentagelser hvis alle faktorerne $\neq e$. Normalrækken

$$G = G_0 \triangleright \widetilde{G}_1 \triangleright \widetilde{G}_2 \triangleright \cdots \triangleright \widetilde{G}_t = \{e\} \qquad (\dagger)$$

kaldes en *forfining* af $(*)$ hvis hvert G_i $(1 \le i \le s)$ er lig et $\widetilde{G}_j$ $(1 \le j \le t)$. Hvis $(\dagger)$ består af effektivt flere undergrupper end $(*)$ kaldes $(\dagger)$ en ægte forfining.

Definition. En normalrække i G kaldes en *kompositionsrække*, hvis den er uden gentagelser og ikke tillader nogen ægte forfining uden gentagelser.

Ved hjælp af Noethers 2. isomorfisætning vises let:

Sætning 25. *Hvis $(*)$ er en normalrække uden gentagelser, gælder*

$$(*) \text{ er kompositionsrække} \iff \text{faktorerne er simple grupper}.$$

Desuden gælder trivielt

Sætning 26. *G endelig $\Rightarrow G$ har en kompositionsrække.*

Bemærkning. Ovenstående sætning kan ikke vendes om, da der findes uendelige simple grupper.

Imidlertid gælder:

Sætning 27. *For abelske grupper G gælder: G endelig $\iff$ G har kompositionsrække.*

Bevis. Benyt, at en simpel abelsk gruppe er endelig (endda af primtalsorden). $\square$

Eksempel. $\mathbb{Z}_6 \supset 2\mathbb{Z}_6 \supset 0$ og $\mathbb{Z}_6 \supset 3\mathbb{Z}_6 \supset 0$ er "væsentlig" ens normalrækker. (Faktorerne er de samme $\mathbb{Z}_2$, $\mathbb{Z}_3$ og $\mathbb{Z}_3$, $\mathbb{Z}_2$).

Definition. To normalrækker uden gentagelser kaldes isomorfe, hvis faktorerne på nær rækkefølgen er isomorfe.

Bemærkning. Ved hjælp af Sætning 25 ses, at en normalrække uden gentagelser, der er isomorf med en kompositionsrække, selv er en kompositionsrække.

Vi viser nu nogle klassiske sætninger.

Jordan–Hölders sætning. *Hvis en gruppe G har en kompositionsrække er alle kompositionsrækker i G indbyrdes isomorfe.*

Schreier's Forfiningssætning. *To vilkårlige normalrækker i en gruppe har isomorfe forfininger.*

Klart, at Schreier's forfiningssætning $\Rightarrow$ Jordan–Hölders sætning.
For at vise Schreier's forfiningssætning benytter vi

Zassenhaus Lemma. *Lad H_1, H_2, K og K_2 være undergrupper i gruppen G. Lad $H_1 \triangleleft H_2$, $K_1 \triangleleft K_2$. Da er $H_1(H_2 \cap K_1)$, $H_1(H_2 \cap K_2)$, $K_1(H_1 \cap K_2)$ og $K_1(H_2 \cap K_2)$ undergrupper i G, og der gælder*

(i) $H_1(H_1 \cap K_1) \triangleleft H_1(H_2 \cap K_2)$

(ii) $K_1(H_1 \cap K_2) \triangleleft K_1(H_2 \cap K_2)$

og

(iii) $H_1(H_2 \cap K_2)/H_1(H_2 \cap K_1) \simeq K_1(H_2 \cap K_2)/K_1(H_1 \cap K_2)$.

Bevis. At $H_1(H_2 \cap K_1)$, etc. er undergrupper følger af $H_1 \triangleleft H_2$ og $K_1 \triangleleft K_2$.

Et element i $H_1(H_2 \cap K_1)$ kan skrives hx, $h \in H_1$; $x \in H_2 \cap K_1$ og et element i $H_1(H_2 \cap K_2)$ kan skrives $\widetilde{h}y$, $\widetilde{h} \in H_1$; $y \in H_2 \cap K_2$. Elementet

$$(\widetilde{h}y)(hx)\widetilde{h}y)^{-1} = \widetilde{h}(yhy^{-1})(yxy^{-1})\widetilde{h}^{-1} \in H_1(H_2 \cap K_1)$$

idet $yhy^{-1} \in H_1$ og $yxy^{-1} \in H_2 \cap K_1$. Dette godtgør (i). ((ii) vises analogt).

$(H_2 \cap K_2)$ og $H_1(H_2 \cap K_1)$ er undergrupper i $H_1(H_2 \cap K_2)$ og $H_1(H_2 \cap K_1) \triangleleft H_1(H_2 \cap K_2)$. Vi anvender Noethers 1. isomorfisætning på:

$$\begin{tikzcd}[column sep=small]
 & H_1(H_2 \cap K_2) \arrow[dl, dash] \arrow[dr, dash] & \\
H_2 \cap K_2 \arrow[dr, dash] & & H_1(H_2 \cap K_1) \arrow[dl, dash] \\
 & (H_1 \cap K_2)(H_2 \cap K_1) &
\end{tikzcd}$$

hvor man let efterviser, at $(H_2 \cap K_2)H_1(H_2 \cap K_1) = H_1(H_2 \cap K_2)$ og $(H_2 \cap K_2) \cap (H_1(H_2 \cap K_1)) = (H_1 \cap K_2)(H_2 \cap K_1)$. Vi har derfor isomorfien:

$$H_1(H_2 \cap K_2)/H_1(H_2 \cap K_1) \simeq H_2 \cap K_2/H_1 \cap K_2)(H_2 \cap K_1) \tag{†}$$

Højre side er symmetrisk i H og K hvorfor man får:

$$K_1(H_2 \cap K_2)/K_1(H_1 \cap K_2) \simeq H_2 \cap K_2/(H_1 \cap K_2)(H_2 \cap K_1) \tag{††}$$

(†) og (††) giver den ønskede isomorfi i (iii). $\square$

Vi er nu istand til at vise Schreier's forfiningssætning: Lad

$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_s = \{e\} \tag{$*$}$$

og

$$G = K_0 \triangleright K_1 \triangleright \cdots \triangleright K_t = \{e\} \tag{$**$}$$

være to vilkårlige normalrækker i G,

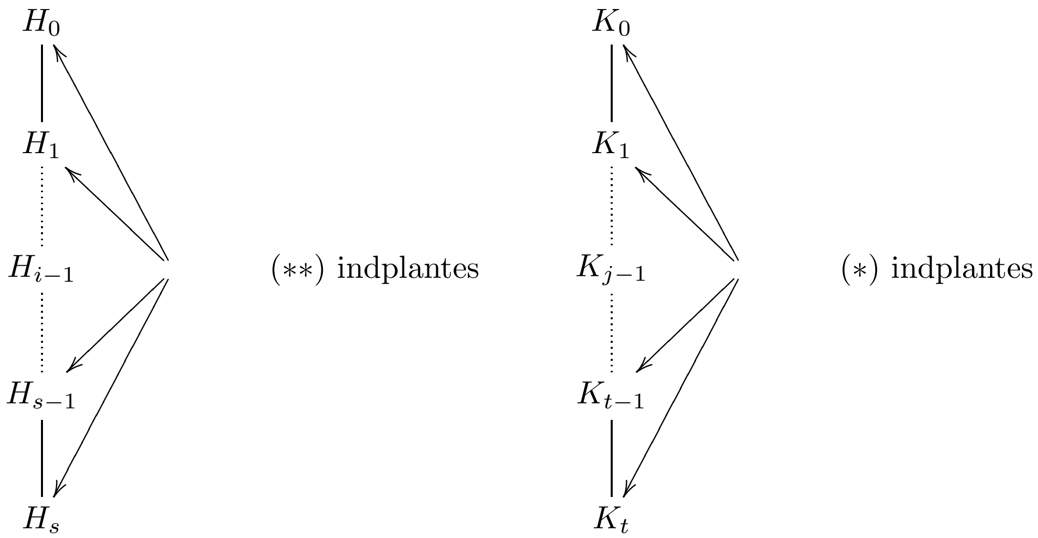
Vi angiver nu følgende forfining af $(*)$ idet $(**)$ "indplantes" mellem H_{i-1} og H_i for alle $i = 1, \ldots, s$:

$$\begin{tikzcd}
H_{i-1} \arrow[dddd, dash] & = & H_i(H_{i-1} \cap K_0) \arrow[d, dotted, dash] \\
 & & H_i(H_{i-1} \cap K_{j-1}) \arrow[d, dash] \\
 & & H_i(H_{i-1} \cap K_j) \arrow[d, dotted, dash] \\
 & & \vdots \\
H_i & = & H_i(H_{i-1} \cap K_t)
\end{tikzcd}$$

Omvendt "indplantes" $(**)$ i $(*)$:

$$
\begin{array}{ccc}
K_{j-1} & = & K_j(H_0 \cap K_{j-1}) \\
\Big| & & \vdots \\
 & & K_j(H_{i-1} \cap K_{j-1}) \\
\Big| & & \Big| \\
 & & K_j(H_i \cap K_{j-1}) \\
\Big| & & \vdots \\
K_j & = & K_j(H_s \cap K_{j-1})
\end{array}
$$

De to skraverede faktorgrupper bliver isomorfe ifølge Zassenhaus' Lemma. De nedenfor antydede normalrækker er da isomorfe forfininger af $(*)$ og $(**)$



Som før nævnt er Jordan–Hölders sætning et umiddelbart korollar af Schreier's forfiningssætning. Vi angiver endnu nogle simple konsekvenser af forfiningssætningen:

Korollar 1. *Hvis en gruppe har en kompositionsrække, kan enhver normalrække (uden gentagelser) forfines til en kompositionsrække.*

Korollar 2. *Hvis en gruppe har en kompositionsrække af længden s, er længden af enhver normalrække (uden gentagelser) $\leqq s$, og $= s$ netop når normalrækken er en kompositionsrække.*

Opgave. Angiv en kompositionsrække for en cyklisk gruppe $\mathbb{Z}_n$. Hvilken kendt talteoretisk sætning fås ved anvendelse af Jordan–Hölders sætning?

OPLØSELIGHED.

DEFINITION. Gruppen G siges at være *opløselig*, hvis der findes en normalrække i G med abelske faktorer.

Vi giver først en karakterisering af opløselige grupper udtrykt ved kommutatorgrupperne og de højere afledede.

Sætning 28. *Lad G være en vilkårlig gruppe. Da gælder:*

$$G \text{ opløselig} \iff G^{(n)} = \{e\} \text{ for passende } n \in \mathbb{N}\,.$$

Bevis. "⇒" Lad $G \rhd G_1 \rhd \cdots \rhd G_s = \{e\}$ være normalrække med abelske faktorer. Da G/G_1 er abelsk, er (jfr. karakteriseringen af kommutatorgruppen) $G' \subseteqq G_1$. Analogt fås

$$G_1' \subseteqq G_2 \Rightarrow G'' \subseteqq G_1' \subseteqq G_2 \text{ og helt alment:}$$
$$G^{(i)} \subseteqq G_i \text{ og følgelig } G^{(s)} = \{e\}\,.$$

"⇐"

$$G' \lhd G \text{ og } G/G' \text{ abelsk}$$
$$G'' \lhd G' \text{ og } G'/G'' \text{ abelsk}\,.$$

Dvs.: $G \rhd G' \rhd G'' \rhd \cdots \rhd G^{(n)} = \{e\}$ er en normalrække med abelske faktorer. □

BEMÆRKNING. Det ses let, at alle de afledede grupper $G^{(i)}$ er karakteristiske undergrupper i G, specielt normaldelere i G. Ovenstående sætning viser derfor, at G opløselig ⇒ G har en "absolut" normalrække (dvs.: Undergrupperne er normaldelere ikke blot i foregående gruppe, men i hele G) med abelske faktorer.

Sætning 29.

G opløselig ⇒ enhver undergruppe i G er opløselig.
G opløselig ⇒ ethvert homomorft billede af G er opløselig.

Bevis. Den første implikation fås af ovenstående Sætning 28 ved at bemærke, at for en undergruppe H i en gruppe G vil kommutatorgruppen H' for H være en undergruppe i G' og tilsvarende for de højere afledede grupper.

Den anden implikation fås af ovenstående Sætning 28 ved at bemærke, at for en homomorfi f fra en gruppe G til en gruppe H vil $f(G')$ være en undergruppe i H' og tilsvarende for de højere afledede grupper. □

Sætning 30. *Lad G være en vilkårlig gruppe. Hvis G indeholder en opløselig normaldeler N så G/N er opløselig, da er G opløselig.*

Bevis. Vælg en normalrække med abelske faktorer for N og en normalrække med abelske faktorer for G/N. Sidstnævnte normalrække "indplantes" mellem N og G ved hjælp af Noethers 2. isomorfisætning. Sammenstykning giver da en normalrække i G med abelske faktorer dvs.: G er opløselig. □

Vi giver nu en beskrivelse af kompositionsrækkerne i en endelig opløselig gruppe. Vi får brug følgende hjælpesætning.

Sætning 31. *En simpel opløselig gruppe er cyklisk af primtalsorden.*

Bevis. Hvis G er simpel, er $G \rhd \{e\}$ den eneste ikke-trivielle normalrække. Når G er opløselig, må faktorgruppen $G/\{e\} \simeq G$ være abelsk. Men en abelsk simpel gruppe er cyklisk af primtalsorden (jfr. Opgave p.1.6). □

Sætning 32. *For en endelig gruppe G er følgende betingelser ækvivalente:*
i) G er opløselig.
ii) Der findes en kompositionsrække for G, hvis faktorer er cykliske af primtalsorden.
iii) Faktorerne i enhver kompositionsrække for G er cykliske af primtalsorden.

Bevis. Da det er klart, at *iii*) $\Rightarrow$ *ii*) $\Rightarrow$ *i*), er det nok at godtgøre *i*) $\Rightarrow$ *iii*).

Sætning 29 medfører, at faktorerne i en vilkårlig kompositionsrække for G er opløselige. Ifølge Sætning 25 er faktorerne i en kompositionsrække simple. Sætning 31 medfører nu, at faktorerne må være cykliske af primtalsorden. □

Sætning 33. *Enhver p-gruppe er opløselig.*

Bevis. Lad p-gruppen G have orden p^n. Beviset føres ved induktion efter n.

$n = 1$ klar (G er da cyklisk).

Antag sætningen vist for p-grupper af orden $< p^n$. Ifølge sætning 15 har centret $Z(G)$ orden $\geqq p$. Nu er $Z(G) \lhd G$ og $G/Z(G)$ er en p-gruppe af orden $< p^n$. Ifølge induktionsantagelsen er $G/Z(G)$ derfor opløselig.

$Z(G)$ er abelsk og dermed opløselig. Sætning 30 viser nu, at G er opløselig. □

Sætning 34. *Den symmetriske gruppe S_n er opløselig for $n \leqq 4$ og ikke-opløselig for $n \geqq 5$.*

Bevis. $n = 1, 2$ triviel, $\underline{n = 3}$, $S_3' = A_3$, $S_3'' = A_3' = \{e\}$, $\underline{n = 4}$ $S_4 \simeq \mathcal{H}$, $S_4''' = \{e\}$: S_n opløselig for $n \leqq 4$. For $n \geqq 5$ er A_n simpel og ikke-abelsk, hvorfor A_n og dermed S_n ikke er opløselig. □

BEMÆRKNING. At S_n ikke er opløselig for $n \geqq 5$ kan bevises direkte (uden brug af Galois' sætning). Nok at vise $A_n = A_n'$ for $n \geqq 5$. Hertil godtgør vi:

1) Enhver 3-cykel er en kommutator,
2) 3-cyklerne frembringer hele A_n.

Ad 1) (abc) givet; da $n \geqq 5$ findes d og e så a, b, c, d, e er indbyrdes forskellige:

$$(abc) = (dba)^{-1}(aec)^{-1}(dba)(aec)\,.$$

Ad 2) Enhver permutation i A_n er produkt af par af transpositioner. To tilfælde:

$$\begin{aligned}&(ab)(bc) = (abc)\\&(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)\,.\end{aligned}$$

□

I bemærkning p.1.27 så vi, at G opløselig $\Rightarrow$ G har "absolut" normalrække med abelske faktorer.

DEFINITION. Gruppen G kaldes *overopløselig*, hvis G har en absolut normalrække med cykliske faktorer.

Klart, at overopløselig $\Rightarrow$ opløselig.

EKSEMPEL. Tetraedergruppen $\simeq A_4$ er opløselig, men ej overopløselig.

DEFINITION. G kaldes *nilpotent*, hvis G har en absolut normalrække

$$G_n = e \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G\,,$$

hvor G_{i-1}/G_i er indeholdt i Centrum (G/G_i).

EKSEMPEL. S_3 er overopløselig, men ej nilpotent.

Beviset for Sætning 32 kan modificeres til at godtgøre at enhver p-gruppe er nilpotent.

For *endelige* grupper gælder (ej trivielt): nilpotent $\Rightarrow$ overopløselig, og man har derfor implikationerne (for endelige grupper)

$$\text{abelsk} \;\Rightarrow\; \text{nilpotent} \;\Rightarrow\; \text{overopløselig} \;\Rightarrow\; \text{opløselig}\,,$$

hvor alle implikationerne er "ægte".

I analogi med kompositionsrækker (og Jordan–Hölders sætning) kan man betragte maximale kæder af undergrupper. Her gælder en overraskende sætning af Iwasawa ifølge hvilken en endelig gruppe er overopløselig, hvis og kun hvis alle maximale kæder af undergrupper har samme længde.

Sylows Gruppesætninger.

Definition. Lad G være en endelig gruppe og p en primdivisor i $|G|$. Antag $|G| = p^r \cdot m$, $p\nmid m$. En undergruppe i G af orden p^r kaldes en p-Sylowgruppe.

Inden Sylows sætninger et lille lemma.

Lemma. *Lad G være en endelig abelsk gruppe og p en primdivisor i $|G|$. Da findes et element i G af orden p.*

Bevis. Sæt $|G| = n$. Induktion efter n. For $n = 2, 3$ er udsagnet klart. Antag lemmaet bevist for grupper af orden $< n$.

Vælg $a \neq e$ i G og lad A være den cykliske undergruppe frembragt af a. $|A| = \operatorname{Ord} a = t$, $t > 1$. Vi skelner mellem to tilfælde.

i) $p|t$; da er $a^{\frac{t}{p}}$ et element af orden p.
ii) $p\nmid t$; da vil $p|\frac{n}{t} = |G/A|$.

Ifølge induktionsantagelsen findes et element b i G/A af orden p, (idet $|G/A| < n$). For en repræsentant b for b gælder $b^p \in A$, $b \notin A$ og derfor $b^p = a^i$ for passende i. Da $\operatorname{ord} a = t$ er $b^{pt} = e$ eller $(b^t)^p = e$. Følgelig nok at vise, at $b^t \neq e$. Men $b^t = e$ ville medføre $b^t = e$ og dermed $p|t$ i strid med antagelsen ii). $\square$

Sylows 1. Sætning. *Lad G være en endelig gruppe og p en primdivisor i $|G|$. Da findes en p-Sylowgruppe i G.*

Bevis. Induktion efter $|G|$. For "små" ordener er sætningen triviel. Antag sætningen vist for grupper af orden $< |G|$. To muligheder:

1) $\exists$ ægte undergruppe H i G så $p \nmid [G : H]$
2) For alle ægte undergrupper H i G gælder $p|[G : H]$.

Ad 1) Ifølge induktionsantagelsen findes en p-Sylowgruppe i H. Denne vil – da $p \nmid [G : H]$ – også være en p-Sylowgruppe i G.

Ad 2) Vi inddeler elementerne i G i ækvivalensklasser m.h.t. konjugering. Da gælder klasseligningen (jfr. p.1.13)

$$|G| = |Z(G)| + \sum_{\substack{\text{visse } a \\ [G:\mathcal{C}_a]>1}} [G : \mathcal{C}_a]$$

hvoraf sluttes, at $p \mid |Z(G)|$. Ifølge lemmaet findes et element $a \in Z(G)$ af orden p. Den af a frembragte cykliske undergruppe A er normaldeler i G. Vi betragter nu den kanoniske afbildning κ af G på $G/A(=G^*)$

$$\begin{tikzcd}
G \arrow[r, "\kappa"] \arrow[d, dash] & G^* \arrow[d, dash] \\
P \arrow[r, dotted, dash] \arrow[d, dash] & P^* \arrow[d, dash] \\
A \arrow[r] \arrow[d, dash] & \{e^*\} \\
\{e\} &
\end{tikzcd}$$

Hvis $|G| = p^r m$, $p \nmid m$, er $|G^*| = p^{r-1}m$. Dersom $r = 1$, vil A være en p-Sylowgruppe i G. Dersom $r > 1$, vil G^*, der har mindre orden end G, på grund af induktionsantagelsen have en p-Sylowgruppe P^*. Ifølge Noethers 2. isomorfisætning er $P = \kappa^{-1}(P^*)$ en undergruppe i G så $P/A \simeq P^*$, dvs.: $|P| = p^{r-1}p = p^r$. P er altså en p-Sylowgruppe i G. □

Korollar 1. (Cauchy). *Hvis p er en primdivisor i ordenen af en endelig gruppe G, da findes et element i G af orden p.*

Bevis. Lad a være et fra det neutrale element forskelligt element i en p-Sylowgruppe i G. Ordenen af a må være en potens p^t af p. Elementet $a^{p^{t-1}}$ må da have orden p. □

Korollar 2. *Lad G være en gruppe af orden $2p^n$, hvor p er et primtal. Da er G opløselig.*

Bevis. Hvis $p = 2$ følger udsagnet umiddelbart af sætning 33. Hvis $p \neq 2$ vil en p-Sylowgruppe P have indeks 2 i G og derfor være en normaldeler i G. Da P ifl. sætning 33 er opløselig og faktorgruppen G/P er cyklisk af orden 2, specielt opløselig, medfører sætning 30, at G er opløselig. □

Inden Sylows 2. sætning indfører vi for en undergruppe H i G *normalisatoren* N_H som $N_H = \{g \in G \mid gHg^{-1} = H\}$. N_H bliver en undergruppe i G, og det er klart, at $H \lhd N_H$. (I øvrigt ses let, at N_H er den største undergruppe i G der indeholder H som normaldeler).

To undergrupper H_1 og H_2 i G kaldes *konjugerede*, hvis $gH_1g^{-1} = H_2$ for et passende $g \in G$. Man ser let, at "konjugeret" er en ækvivalensrelation. I analogi med et tidligere argument (p.1.12) ses, at antallet af med H konjugerede undergrupper er $[G : N_H]$.

Det er klart, at hvis P er en p-Sylowgruppe, er enhver med P konjugeret undergruppe også en p-Sylowgruppe. En art omvending er givet i:

Sylows 2. sætning. *Lad G være en endelig gruppe og p en primdivisor i $|G|$. Alle p-Sylowgrupper i G er indbyrdes konjugerede, og enhver p-undergruppe i G er indeholdt i en p-Sylowgruppe.*

Bevis. Lad P være en p-Sylowgruppe i G, og S en vilkårlig p-undergruppe i G. Lad $\{P_i\}$ være de med P konjugerede undergrupper, hvis antal er $[G : N_P]$. P_i kaldes S-ækvivalent med P_j hvis $P_i = sP_js^{-1}$ for et passende $s \in S$. Antallet af med P_i S-ækvivalente undergrupper er $[S : (S \cap N_{P_i})]$.

I nedenstående lemma viser vi, at $S \cap P_i = S \cap N_{P_i}$.

Ved optælling (jfr. udledelsen af klasseligningen p.1.12) fås derfor en relation

$$[G : N_P] = \sum_{\text{visse i}} [S : (S \cap P_i)]$$

$[S : (S \cap P_i)] =$ potens af p (evt. 1). $p \nmid [G : N_P]$ indebærer derfor $[S : (S \cap P_i)] = 1$ for mindst et i og dermed $S \subseteq P_i$. Hvis S selv er en Sylowgruppe, vil $S = P_i$, da grupperne S og P_i har samme elementantal. Beviset er derfor afsluttet modulo:

Lemma. *Hvis P er p-Sylowgruppe i G og S er p-undergruppe i G, da er $S \cap N_P = S \cap P$.*

Bevis. Sæt $S_1 = S \cap N_P$. Det er klart, at $S_1 \supseteq S \cap P$, $P \triangleleft N_P$ og at S_1P er en undergruppe i N_P. Noethers 1. isomorfisætning anvendes:

$$\begin{tikzcd}[column sep=small] & S_1P \arrow[dl, dash] \arrow[dr, dash] & \\ S_1 \arrow[dr, dash] & & P \arrow[dl, dash] \\ & S_1 \cap P & \end{tikzcd} \qquad S_1P/P \simeq S_1/S_1 \cap P$$

Specielt er $[S_1P : P] = [S_1 : (S_1 \cap P)]$. Da $p \nmid [S_1P : P]$ og da $[S_1 : (S_1 \cap P)]$ er divisor i en potens af primtallet p er $[S_1 : (S_1 \cap P)] = 1$ dvs.: $S_1 = S_1 \cap P$ og følgelig $S \cap N_P = S \cap P$. $\square$

Sylows 3. sætning. *Lad G være en endelig gruppe og p en primdivisor i $|G|$. Antallet af p-Sylowgrupper i G er en divisor i $|G|$ og $\equiv 1 \pmod p$.*

Bevis. Antallet af p-Sylowgrupper er $[G : N_P]$, hvor P er en vilkårlig, men fast p-Sylowgruppe. Som i beviset for Sylows 2. sætning fås:

$$[G : N_P] = \sum_{\text{visse i}} [P : (P \cap P_i)] \qquad (*)$$

Her har vi: $p \nmid [G : N_P]$ og $[P : (P \cap P_i)] =$ potens af p (evt. 1)

Endvidere gælder: $[P : (P \cap P_i)] = 1 \iff P = P_i$ (da $|P| = |P_i|$).

Følgelig forekommer på højre side af $(*)$ netop én addend 1, mens resten er delelige med p. Følgelig fås: $[G : N_P] \equiv 1 \pmod p$. □

Bemærkning. Lad P være p-Sylowgruppe i G. Da gælder åbenbart: $P \lhd G \iff [G : N_P] = 1 \iff$ netop én p-Sylowgruppe i G.

Opgave. Vis, at i ovenstående situation gælder: $P \lhd G \Rightarrow P$ karakteristisk undergruppe i G.

Anvendelser.

Sætning 35. *En gruppe G af orden pq, hvor p og q er primtal, er opløselig.*

Bevis. Vi kan antage (hvorfor ?) $p \neq q$ f.eks. $p > q$. Ifølge ovenstående bemærkning findes netop én p-Sylowgruppe, der er normaldeler og sammen med G og $\{e\}$ udgør en normalrække med abelske faktorer. □

Sætning 36. *Lad p og q være forskellige primtal for hvilke $p \not\equiv 1 \pmod q$ og $q \not\equiv 1 \pmod p$. Da er enhver gruppe G af orden pq cyklisk.*

Bevis. Ved anvendelse af Sylows 3. sætning ses, at G indeholder netop én undergruppe P af orden p og netop én undergruppe Q af orden q. Der er derfor netop $(p-1)$ elementer af orden p og netop $(q-1)$ elementer af orden q. Desuden er der netop ét element af orden 1. Da elementordnerne må være blandt tallene $1, p, q$ og pq, og $pq - (p-1) - (q-1) - 1 = (p-1)(q-1) > 0$, må der findes et element i G af orden pq, dvs. G er cyklisk. □

Sætning 37. *Hvis gruppen G har orden p^2q, hvor p og q er primtal, er G opløselig.*

Bevis. Vi kan antage $p \neq q$ (hvorfor ?). Det er nok at vise, at der enten kun findes én p-Sylowgruppe eller kun én q-Sylowgruppe. Hvis $p > q$ giver Sylows 3. sætning umiddelbart, at der er netop én p-Sylowgruppe. I tilfældet $p < q$ føres beviset indirekte. Antag, at såvel antallet af p-Sylowgrupper som antallet af q-Sylowgrupper er > 1. Der må da findes (mindst) q p-Sylowgrupper og p^2 q-Sylowgrupper. To forskellige q-Sylowgrupper har kun e fælles. To forskellige p-Sylowgrupper har højst p elementer fælles. Følgelig måtte G have mindst $p^2(q-1) + (p^2-1) + (p^2-p) + 1 = p^2q + p^2 - p$ elementer. Modstrid! □

Ved et analogt optællingsargument fås:

Sætning 38. *Hvis gruppen G har orden pqr, hvor p, q og r er primtal, er G opløselig.*

I næste afsnit skal vi vise: $|G|$ kvadratfri $\Rightarrow G$ opløselig.

Ved brug af mere dybtliggende metoder kan vises

Sætning. (Burnside). *Hvis gruppen G har orden $p^a \cdot q^b$, p og q primtal, da er G opløselig.*

Sætning. (Feit & Thompson, Pac. J. Math. 1963, 775-1029 (!)). *Enhver gruppe af ulige orden er opløselig.*

Opgave. Lad n være af formen $p \cdot a$, $p > a$, p et primtal. Vis, at enhver undergruppe af orden p^a i den symmetriske gruppe S_n er abelsk.

VERLAGERUNG OG ANVENDELSER HERAF.

Vi stiler nu mod at vise en generel sætning af Burnside, der bl.a. indebærer, at en gruppe af kvadratfri orden (dvs.: produkt af indbyrdes forskellige primtal) er opløselig.

Hertil studerer vi først begrebet “Verlagerung”.

Lad G være en endelig gruppe og H en abelsk undergruppe i G. Vi definerer nu en afbildning “Verlagerung” $\mathrm{Ver}(x)$, $x \in G$, fra G til H. Lad $g_1, \dots, g_n$ være et fuldstændigt repræsentantsystem for højresideklasserne til H, altså:

$$G = \bigcup_{i=1}^{n} g_i H \qquad \text{(disjunkt forening)}\,.$$

For ethvert $x \in G$ er også $xg_1, \dots, xg_n$ et fuldstændigt repræsentantsystem for højresideklasserne til H, dvs. $\forall_{g_i}\ \exists! g_j\,,\ j = x(i)$, så $xg_iH = g_jH$ eller $xg_i = g_{x(i)} \cdot h_{x,i}$ hvor $h_{x,i} \in H$ og $i \to x(i)$ er en permutation af $\{1, 2, \dots, n\}$.

Vi sætter nu:

$$\mathrm{Ver}(x) = \prod_{i=1}^{n} h_{x,i}$$

Da H er abelsk, er produktet uafhængig af faktorernes rækkefølge. Denne definition er tillige uafhængig af valget af repræsentantsystemet for højresideklasserne til H. Ethvert andet repræsentantsystem kan skrives $g_1\widetilde{h}_1, \dots, g_n\widetilde{h}_n$, hvor $\widetilde{h}_1, \dots, \widetilde{h}_n \in H$. For hvert i, $1 \le i \le n$, fås

$$x(g_i\widetilde{h}_i) = g_{x(i)}h_{x,i}\widetilde{h}_i = (g_{x(i)}\widetilde{h}_{x(i)}) \cdot (\widetilde{h}_{x(i)}^{-1}h_{x,i}\widetilde{h}_i)\,,$$

således at

$$\prod_{i=1}^{n}\left(\widetilde{h}_{x(i)}^{-1}h_{x,i}\widetilde{h}_i\right) = \prod_{i=1}^{n}\widetilde{h}_{x(i)}^{-1}\prod_{i=1}^{n}h_{x,i}\prod_{i=1}^{n}\widetilde{h}_i = \prod_{i=1}^{n}h_{x,i}$$

hvor vi at udnyttet, at H er abelsk, og $i \to x(i)$ er en permutation af indexmængden $\{1, \dots, n\}$.

Vi viser nu, at Ver *er en homomorfi fra G ind i H*. Lad $g_1, \dots, g_n$ være et fuldstændigt repræsentantsystem for højresideklasserne til H og lad x og y være vilkårlige elementer i G.

Hvis

$$xg_i = g_{x(i)}h_{x,i}; \text{ og } \ yg_i = g_{y(i)}h_{y,i} \quad (1 \le i \le n)$$

vil

$$xyg_i = xg_{y(i)}h_{y,i} = g_{x(y(i))}h_{x,y(i)}h_{y,i} \quad (1 \le i \le n)$$

hvorfor

$$\operatorname{Ver}(xy) = \prod_{i=1}^{n} \left(h_{x,y(i)} h_{y,i}\right) = \prod_{i=1}^{n} h_{x,y(i)} \cdot \prod_{i=1}^{n} h_{y,i} = \operatorname{Ver}(x) \cdot \operatorname{Ver}(y)\,.$$

I stedet for højresideklasser kunne vi have betragtet venstresideklasserne

$$G = \bigcup_{i=1}^{n} Hg_i\,, \qquad \text{(disjunkt forening)}$$

og have indført $\widehat{\operatorname{Ver}}(x) = \prod_{i=1}^{n} \widehat{h}_{x,i}$, når $g_i x = \widehat{h}_{x,i} g_{x(i)}$ for entydigt bestemt $x(i) \in \{1, \ldots, n\}$ og $\widehat{h}_{x,i} \in H$. $\widehat{\operatorname{Ver}}$ vil da som før være veldefineret og en homomorfi fra G til H. Vi hævder, at

$$\operatorname{Ver}(x) = \widehat{\operatorname{Ver}}(x)\ \forall x \in G\,;$$

thi når $G = \bigcup_{i=1}^{n} Hg_i$ (disjunkt forening), vil $G = \bigcup_{i=1}^{n} g_i^{-1} H$ (disjunkt forening). Af $g_i x = \widehat{h}_{x,i} g_{x(i)}$ følger $x^{-1} g_i^{-1} = g_{x(i)}^{-1} \cdot \widehat{h}_{x,i}^{-1}$ og derfor

$$\operatorname{Ver}(x^{-1}) = \prod_{i=1}^{n} \widehat{h}_{x,i}^{-1} = \left(\prod_{i=1}^{n} \widehat{h}_{x,i}\right)^{-1} = (\widehat{\operatorname{Ver}}(x))^{-1}$$

Da Ver er en homomorfi, fås heraf $\operatorname{Ver}(x) = \widehat{\operatorname{Ver}}(x)$.

Ver er altså en veldefineret homomorfi fra G til H, uafhængig af valget af repræsentanter for sideklasserne, uafhængig af højre og venstre.

Alternativ beregning af Verlagerung

Endelig viser vi, at for ethvert $x \in G$ kan $\operatorname{Ver}(x)$ skrives $\operatorname{Ver}(x) = \prod_{k=0}^{r} y_k^{-1}\, x^{t_k}\, y_k$, hvor $y_0 = e$, $y_k \in G$, $t_k \in \mathbb{N}$, $(0 \leq k \leq r)$ og $\sum_{t=0}^{r} t_k = [G : H]$ og $y_k^{-1} x^{t_k} y_k \in H$, $\forall k\ (0 \leq k \leq r)$.

Hertil angiver vi først et bestemt (af x afhængigt) repræsentantsystem for højresideklasserne for H. Lad t_0 være mindste naturlige tal med $x^{t_0} \in H$. Da er $H, xH, \ldots, x^{t_0-1}H$ indbyrdes forskellige højresideklasser. Hvis $t_0 = [G : H]$, er disse samtlige sideklasser. Hvis $t_0 < [G : H]$, vælges $y_1 \in G$, $y_1 \notin \bigcup_{j=0}^{t_0-1} x^j H$. Lad t_1 være mindste naturlige tal med $x_1^{t_1} y_1 \in y_1 H$. Da er $H, xH, \ldots, x^{t_0-1}H$, $y_1 H$, $xy_1 H, \ldots, x^{t_1-1} y_1 H$ indbyrdes forskellige højresideklasser. Hvis $t_0 + t_1 = [G : H]$, er disse samtlige sideklasser. Hvis $t_0 + t_1 < [G : H]$, vælges

$$y_2 \in G\,, y_2 \notin \cup x^j H \cup x^j y_1 H\,.$$

Lad da t_2 være mindste naturlige tal med $x^{t_2}y_2 \in y_2H$. Da er

$$H, xH, \ldots, x^{t_0-1}H, y_1H, \ldots, x^{t_1-1}y_1H, y_2H, \ldots, x^{t_2-1}y_2H$$

indbyrdes forskellige sideklasser etc. Alt i alt fås repræsentantsystem

$$e, x, \ldots, x^{t_0-1}, y_1, xy_1, \ldots, x^{t_1-1}y_1, \ldots, y_r, xy_r, \ldots, x^{t_r-1}y_r$$

hvor $t_0 + t_1 + \cdots + t_r = [G : H]$. For dette repræsentantsystem ses let, at

$$\mathrm{Ver}(x) = x^{t_0}\left(y_1^{-1}x^{t_1}y_1\right)\ldots\left(y_r^{-1}x^{t_r}y_r\right) .$$

Vi vender nu tilbage til Sylowgrupperne. Først et

Lemma. *Lad G være en endelig gruppe og P en abelsk p-Sylowgruppe (p en primdivisor i $|G|$). Hvis to elementer a og $b \in P$ er konjugerede i G, da er de også konjugerede inden for normalisatoren N_P.*

Bevis. Da P er abelsk, er $P \subseteq \mathcal{C}_a$ og $P \subseteq \mathcal{C}_b$. Da a og b er konjugerede i G, er $b = xax^{-1}$ for passende $x \in G$. Heraf fås:

$$\mathcal{C}_b = x\mathcal{C}_a\, x^{-1}$$

Af $P \subseteq \mathcal{C}_a$ følger $xPx^{-1} \subseteq x\mathcal{C}_a x^{-1} = \mathcal{C}_b$.

Da P og xPx^{-1} begge er p-Sylowgrupper i $\mathcal{C}_b$, er de ifl. Sylows 2. sætning konjugerede indenfor $\mathcal{C}_b$, dvs. der findes $y \in \mathcal{C}_b$ så $P = y(xPx^{-1})y^{-1}$. Dette viser, at $yx \in N_P$. Men ligningen $b = yby^{-1} = y(xax^{-1})y^{-1} = (yx)a(yx)^{-1}$ viser, at a og b er konjugerede indenfor N_P. □

Burnsides Verlagerungssætning. *Lad G være en endelig gruppe og P en p-Sylowgruppe, hvor p er en primdivisor i $|G|$. Hvis P er indeholdt i centrum for normalisatoren N_P, da findes en normaldeler N i G så $G/N \simeq P$.*

Bevis. Da P er indeholdt i centrum for N_P, er P abelsk. Vi kan derfor betragte Verlagerung $\mathrm{Ver} : G \to P$. Sæt $N = \mathrm{Ker}(\mathrm{Ver})$, da er $N \triangleleft G$. Sætningen er bevist, når vi har godtgjort, at $\mathrm{Ver}(G) = P$; vi viser endda $\mathrm{Ver}(P) = P$.

Lad $x \in P$. Ved den ovenfor nævnte alternative beregningsmetode for Verlagerung, fås

$$\mathrm{Ver}(x) = \prod_{k=0}^{r} y_k\, x^{t_k}\, y_k^{-1}\,,\ y_k \in G\,,\ y_k\, x^{t_k}\, y_k^{-1} \in P\,,\ \sum_{k=0}^{r} t_k = [G : P]\,.$$

De i P liggende faktorer $y_k\, x^{t_k}\, y_k^{-1}$ er indenfor G konjugerede med x^{t_k} og derfor ifølge det foregående lemma også konjugerede med x^{t_k} indenfor N_P; dvs. der findes $z_k \in N_P$ så

$$y_k\, x^{t_k}\, y_k^{-1} = z_k\, x^{t_k}\, z_k^{-1}$$

Men $x \in P$ og $P \subseteq$ centrum for N_P, hvorfor $z_k\, x^{t_k}\, z_k^{-1} = x^{t_k}$. Alt i alt er $\mathrm{Ver}(x) = x^{\sum t_k} = x^{[G:P]}$ for alle $x \in P$. Da P er p-Sylowgruppe, er $|P|$ og $[G : P]$ indbyrdes primiske. Der findes da hele tal α og β så $\alpha|P| + \beta[G : P] = 1$. Heraf fås for $x \in P$

$$x = x^{|P|\cdot\alpha} \cdot x^{\beta\cdot[G:P]} = \mathrm{Ver}(x^{\beta})\,.$$

Altså er $P = \mathrm{Ver}(P)$. □

Inden vi giver anvendelser af Burnsides Verlagerungssætning, indfører vi et nyt begreb. Lad H være en undergruppe i en gruppe G. *Centralisatoren* $\mathcal{C}_H$ defineres som $\mathcal{C}_H = \{x \in G \mid xh = hx\ \forall h \in H\}$. Det er klart, at $\mathcal{C}_H$ er en undergruppe i G og at $\mathcal{C}_H$ er indeholdt i normalisatoren N_H. Hvis specielt $H = G$ er centralisatoren lig gruppens centrum.

Lemma A. *Lad G være en endelig gruppe og P en undergruppe. Da er $[N_P : \mathcal{C}_P]$ en divisor i $|\mathrm{Aut}(P)|$.*

Bevis. For hvert $g \in N_P$ er afbildningen $\varphi_g : P \to P$ defineret ved $\varphi_g(x) = gxg^{-1}$, $x \in P$, en automorfi for P. Afbildningen $\varphi : N_P \to \mathrm{Aut}(P)$ $(g \to \varphi_g)$ er en homomorfi hvis kerne netop er $\mathcal{C}_P$. Følgelig er $N_P/\mathcal{C}_P$ isomorf med en undergruppe i $\mathrm{Aut}(P)$, hvoraf lemma A følger. □

Lemma B. *Lad P være en abelsk p-Sylowgruppe i gruppen G. Hvis $(|\mathrm{Aut}(P)|, [G : P]) = 1$, da findes en normaldeler N i G, for hvilken G/N er isomorf med P.*

Bevis. Ifølge Lemma A er $[N_P : \mathcal{C}_P]$ en divisor i $|\mathrm{Aut}(P)|$. Da P er abelsk, er $P \subseteq \mathcal{C}_P$. Vi har derfor inklusionskæden $P \subseteq \mathcal{C}_P \subseteq N_P \subseteq G$, hvorfor $[N_P : \mathcal{C}_P]$ også er en divisor i $[G : P]$. Dette indebærer ifølge forudsætningen i Lemma B, at $[N_P : \mathcal{C}_P] = 1$, dvs. $\mathcal{C}_P = N_P$.

Dette betyder, at P er indeholdt i centret for N_P. Ifølge Burnsides Verlagerungssætning vil der derfor findes en normaldeler N i G for hvilken G/N er isomorf med P. □

Vi er nu i stand til at vise

Sætning 39. *Hvis alle Sylowgrupper i en endelig gruppe G er cykliske, da er G opløselig.*

Bevis. Lad os skrive $|G| = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, hvor $p_1, \dots, p_r$ er indbyrdes forskellige primtal. Beviset føres ved induktion efter r.

For $r = 1$ er sætningen triviel.

Antag sætningen vist for grupper, hvis orden højst er delelig med $r-1$ forskellige primtal.

Lad p_1 være den mindste primdivisor i $|G|$ og lad P være en p_1-Sylowgruppe. P er da cyklisk af orden $p_1^{\alpha_1}$. Idet P er isomorf med $(\mathbb{Z}_{p_1{}^{\alpha_1}}, +)$ ses let, at $\mathrm{Aut}(P) \simeq$ (den multiplikative gruppe af de primiske restklasser modulo $p_1^{\alpha_1}$) og $\mathrm{Aut}(P)$ har derfor orden $p_1^{\alpha_1} - p_1^{\alpha_1 - 1} = p_1^{\alpha_1-1}(p_1 - 1)$. Da $[G : P] = p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ og p_1 er den mindste primdivisor i $|G|$, er $|\mathrm{Aut}(P)|$ og $[G : P]$ indbyrdes primiske, hvorfor Lemma B medfører,at der findes en normaldeler N i G så $G/N \simeq P$. Idet $|N| = p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ vil enhver Sylowgruppe i N også være en Sylowgruppe i G og derfor være cyklisk. Ifølge induktionsantagelsen er N således opløselig. Eftersom N og $G/N \simeq P$ er opløselige, er G opløselig ifølge sætning 30. $\square$

Bemærkning. En alternativ formulering af sætningen er: En endelig gruppe G er opløselig, hvis der til enhver primtalspotens p^α, som går op i $|G|$, findes et element i G af orden p^α.

Korollar til Sætning 39. *En endelig gruppe af kvadratfri orden er opløselig.*

Endnu en lille anvendelse:

Sætning 40. *Lad G være endelig gruppe af orden $2 \cdot n$ hvor n er ulige. Da findes én og kun én undergruppe af orden n.*

Bevis. Ovenstående bevis giver umiddelbart eksistensen af en undergruppe $N \lhd G$ så $G/N \simeq \mathbb{Z}_2$ dvs.: $|N| = n$.

At N er eneste sådanne undergruppe følger af, at N kan karakteriseres som mængden $\{g^2 \mid g \in G\}$ af kvadrater i G. $\square$

Sætning 41. *Lad G være en endelig simpel ikke-cyklisk gruppe. Hvis $|G|$ er lige, er $|G|$ delelig med 8 eller 12.*

Bevis. Skriv $|G| = 2n$. Hvis n var ulige, viser ovenstående sætning, at der findes $N \lhd G$ så $G/N \simeq \mathbb{Z}_2$. Dette strider mod, at G er simpel, men ej cyklisk. Altså må $4 \mid |G|$, dvs. $|G| = 4k$, $k \in \mathbb{N}$. Vor opgave er at vise k ulige $\Rightarrow 3|k$.

Lad P være en $2-$Sylowgruppe i G. Da k er forudsat ulige, må P have orden 4. P kan ikke være cyklisk, da G ellers ifølge Lemma B indeholdt en normaldeler N med $G/N \simeq \mathbb{Z}_4$ i strid med, at G er simpel. Altså må P være isomorf med Kleins Vierergruppe V_4. Da $\mathrm{Aut}(V_4) = S_3$ (hvorfor ?) må $[N_P : \mathcal{C}_P]$ ifølge lemma A være divisor i 6. Da $2 \nmid [N_P : \mathcal{C}_P]$, er $[N_P : \mathcal{C}_P] = 1$ eller 3.

$[N_P : \mathcal{C}_P] = 1$ ville indebære (Lemma B), at G indeholdt normaldeler N, så $G/N \simeq V_4$ i strid med, at G er simpel. Altså er $[N_P : \mathcal{C}_P] = 3$ hvorfor $3 \mid |G|$ og derfor $3|k$. $\square$

Bemærkning. Ovenstående sætning skyldes Burnside. Han formodede, at forudsætningen "$|G|$ er lige" kunne undværes. Dette blev bekræftet i 1963 af Feit-Thompson. *Enhver* endelig simpel ikke-cyklisk gruppe har således orden delelig med

8 eller 12. Man kan vise, at ordenen af en endelig simpel ikke-cyklisk gruppe er delelig med 12, 16 eller 56.

*Opgave.** Vis, at en endelig gruppe G er opløselig, såfremt enhver ægte undergruppe i G er abelsk.

Abelske grupper og lineære grupper

I dette afsnit vil vi under ét behandle en fundamental struktursætning for abelske grupper og – ved videreudvikling af metoderne hertil – visse lineære grupper, hvorved vi specielt lærer en ny familie af simple grupper at kende.

For abelske grupper skriver vi kompositionen additivt med $+$. Det neutrale element bliver da 0, det inverse til a, $-a$ og vi definerer for $n \in \mathbb{Z}$

$$na = \begin{cases} a + \cdots + a \ n \text{ addender} & (\text{for } n > 0) \\ 0 & \text{for } n = 0 \\ -(-na) & \text{for } n < 0\,. \end{cases}$$

Da gælder:

$$\begin{aligned} &(n+m)a = na + ma && \forall n, m \in \mathbb{Z} \\ &n(ma) = (nm)a \\ &n(a+b) = na + nb && (\leftarrow \text{ her benyttes kommutativiteten}) \end{aligned}$$

For en abelsk gruppe G defineres *torsionen* G_T ved $G_T = \{g \in G \mid ng = 0 \text{ for passende } n \in \mathbb{Z} \setminus \{0\}\}$, dvs. G_T = elementerne i G af endelig orden. Det ses let, at G_T er en undergruppe i G. Hvis $G = G_T$ kaldes G en *torsionsgruppe*. Hvis $G_T = 0$ kaldes G *torsionsfri*.

Eksempel. G endelig $\Rightarrow$ G torsionsgruppe $(\mathbb{Z}, +)$ og $(\mathbb{R}, +)$ er torsionsfri.

Bemærkning. For enhver gruppe G gælder $(G/G_T)_T = 0$.

Definition. Endelig mange elementer i en abstrakt gruppe G $a_1, \dots, a_n$ kaldes *uafhængige*, hvis

$$h_1 a_1 + \cdots + h_n a_n = 0 \ h_1 \dots h_n \in \mathbb{Z} \Rightarrow h_1 = \cdots = h_n = 0\,.$$

En vilkårlig mængde af elementer i G $\{a_i\}$ kaldes uafhængig hvis enhver endelig delmængde af $\{a_i\}$ er uafhængig i henhold til ovenstående.

Definition. En delmængde $S \subseteq G$ kaldes et *frembringersystem* for G, hvis ethvert element i G kan skrives som $\mathbb{Z}$-linearkombination af endelig mange elementer i S. G kaldes *endelig frembragt*, hvis G har et endeligt frembringersystem.

Definition. G kaldes *fri*, hvis der findes et uafhængigt frembringersystem for G, dvs. en familie af elementer $\{e_i\}$ så ethvert element i G entydigt kan skrives som $\mathbb{Z}$-linearkombination af endelig mange elementer i $\{e_i\}$. Ethvert sådant uafhængigt frembringersystem kaldes en *basis* for G.

Eksempel. $\mathbb{Z}^n$, dvs. alle ordnede n-tupler af hele tal med komponentvis addition, udgør fri abelsk gruppe.

Bevis. En endelig gruppe $\neq 0$ er aldrig fri. Dette følger af

Sætning 42. *G abelsk gruppe. Da gælder G fri $\Rightarrow G$ torsionsfri.*

Bevis. Simpel øvelse.

Eksempel. $(Q, +)$ er torsionsfri men ej fri.

Opgave. Er den multiplikative gruppe $(Q^+, \cdot)$ af positive rationale tal fri? (Vink: Tænk på den entydige primfaktoropløsning i ringen $\mathbb{Z}$.)

Er den multiplikative gruppe $(\mathbb{R}^+, \cdot)$ af positive reelle tal fri?

Eksempel. Mængden af alle følger af hele tal, der er 0 fra et vist trin (afhængigt af den enkelte følge) udgør med komponentvis addition en fri abelsk gruppe. Man kan vise (ej trivielt), at mængden af *samtlige* følger af hele tal med komponentvis addition udgør en ikke-fri abelsk gruppe. Ved argumenter kendt fra den lineære algebra i Mat 1 fås let:

Sætning 43. *Alle baser for en given abelsk gruppe har samme elementantal. Dette fælles elementantal kaldes G's rang.*

Sætning 44. *Lad G være fri med en basis $u_1, \ldots, u_n$. Da gælder for n vilkårlige elementer $v_1, \ldots, v_n \in G$, der på grund af basisegenskaben for $u_1, \ldots, u_n$ (entydigt) kan skrives*

$$\begin{pmatrix} v_1 \\ v_n \end{pmatrix} = \underline{\underline{A}} \begin{pmatrix} u_1 \\ u_n \end{pmatrix}, \quad \underline{\underline{A}}\ (n \times n) \text{ Matrix med heltalselementer}$$

at $v_1 \ldots v_n$ er basis for $G \iff$ $\det \underline{\underline{A}} = \pm 1$.

Bevis. "$\Rightarrow$" $v_1, \ldots, v_n$ basis medfører eksistensen af en heltalsmatrix $\underline{\underline{B}}$ så

$$\begin{pmatrix} u_1 \\ u_n \end{pmatrix} = \underline{\underline{B}} \begin{pmatrix} v_1 \\ v_n \end{pmatrix}, \quad \text{hvoraf} \begin{pmatrix} u_1 \\ u_n \end{pmatrix} = \underline{\underline{B}}\,\underline{\underline{A}} \begin{pmatrix} u_1 \\ u_n \end{pmatrix}$$

dvs. $\underline{\underline{B}}\,\underline{\underline{A}} = E$. Følgelig er $(\det \underline{\underline{B}}) \cdot (\det \underline{\underline{A}}) = 1$ og dermed $\det \underline{\underline{A}} = \pm 1$.

"$\Leftarrow$" Da $\det A \neq 0$ er $v_1 \ldots v_n$ uafhængige. Da $\det \underline{\underline{A}} = \pm 1$ vil $\underline{\underline{A}}^{-1}$ have heltallige elementer. Følgelig er $\begin{Bmatrix} u_1 \\ u_n \end{Bmatrix} = A^{-1} \begin{Bmatrix} v_1 \\ v_n \end{Bmatrix}$ dvs. $v_1, \ldots, v_n$ er tillige frembringersæt for G og dermed basis for G.

Bemærkning. En heltals matrix med determinant ± 1 kaldes "unimodulær". Disse matricer udgør en gruppe kaldet $\mathrm{GL}(n, \mathbb{Z})$.

Sætning 45. *Lad G være en fri abelsk gruppe af (endelig) rang n. Da er enhver undergruppe A af G fri med rang $\leqq n$.*

Bevis. Induktion efter n.

$n = 0$: Intet at bevise.

Hvis $n = 1$ er $G \simeq \mathbb{Z}$ og enhver undergruppe har formen $\mathbb{Z}\,a$, dvs. fri af rang 1 (hvis $a \neq 0$) eller af rang 0 (hvis $a = 0$).

$n-1 \to n$: Lad $u_1, \dots, u_n$ være basis for G. Ethvert $a \in A$ kan entydigt skrives $a = h_1 u_1 + \cdots + h_n u_n, h_1, \dots, h_n \in \mathbb{Z}$. Når a gennemløber A vil de tilsvarende koefficienter h_n udgøre en undergruppe i $\mathbb{Z}$. Lad denne have formen $\mathbb{Z}\,\gamma$, $\gamma \in \mathbb{Z}$. Vi skelner nu mellem to tilfælde:

" 1)" $\gamma = 0$; da er $A \subseteq \mathbb{Z}\,u_1 + \cdots + \mathbb{Z}\,u_{n-1}$; iflg. induktionsantagelsen er A fri af rang $\leqq n-1 < n$.

" 2)" $\gamma \neq 0$. Lad v være et element i A så $v = h_1' u_1 + \cdots + h_{n-1} u_{n-1}' + \gamma u_n$. Ifølge induktionsantagelsen er $A \cap (\mathbb{Z}\,u_1 + \cdots + \mathbb{Z}\,u_{n-1})$ fri af rang $\rho \leqq n-1$. Lad $v_1, \dots, v_\rho$ være en basis for $A \cap (\mathbb{Z}\,u_1 + \cdots + \mathbb{Z}\,u_{n-1})$. Beviset afsluttes ved at godtgøre, at $v_1, \dots, v_\rho$, v en basis for A.

i) $v_1, \dots, v_\rho\,,\ v$ *frembringer* A; thi lad $a \in A$ have fremstillinger $a = h_1'' u_1 + \cdots + h_{n-1}'' u_{n-1} + h\gamma u_n$. Da er $a - hv \in A \cap (\mathbb{Z}\,u_1 + \cdots + \mathbb{Z}\,u_{n-1})$ dvs.: $a - hv$ er $\mathbb{Z}$-linearkombination af $v_1, \dots, v_\rho$. Dermed er a en $\mathbb{Z}$-linearkombination af $v_1, \dots, v_\rho\,,\ v$.

ii) $v_1, \dots, v_\rho\,,\ v$ *er uafhængige*; thi antag $k_1 v_1 + \cdots + k_\rho v_\rho + kv = 0$, hvor $k_1, \dots, k_\rho$, $k \in \mathbb{Z}$. Ved at skrive $v_1, \dots, v_\rho\,,\ v$ som $\mathbb{Z}$-linearkombination af $u_1, \dots, u_n$ og se på koefficienterne til u_n ses, da $\gamma \neq 0$, at $k = 0$. Da $v_1, \dots, v_\rho$ er uafhængige, må $k_1 = \cdots = k_\rho = 0$. Altså er $v_1, \dots, v_\rho\,,\ v$ en basis for A. Antallet er $\rho + 1 \le (n-1) + 1 = n$.

Bemærkning. Lad F være fri undergruppe i den fri gruppe G. Rang F = rang G medfører *ikke* at $F = G$ (modeksempel ?)

Den næste sætning er fundamental for både abelske grupper og lineære grupper.

Elementærdivisorsætningen. *Lad F være fri abelsk gruppe af endelig rang n og G en (ifølge foregående sætninger nødvendigvis) fri undergruppe af rang $m (\leqq n)$. Lad $u_1, \dots, u_n$ være basis for F, $v_1, \dots, v_m$ basis for G. Lad med passende $(m \times n)$ heltalsmatrix $\underline{\underline{A}}$*

$$\begin{Bmatrix} v_1 \\ v_m \end{Bmatrix} = \underline{\underline{A}} \begin{Bmatrix} u_1 \\ u_n \end{Bmatrix}.$$

Ved basisskifte for F og G kan opnås at transformationsmatricen $\underline{\underline{A}}$ herved føres over i en diagonalmatrix (dvs.: Nuller uden for diagonalen). Alternativ formulering: Der findes unimodulære $(m \times m)$, resp. $(n \times n)$ matricer $\underline{\underline{P}}$ resp. $\underline{\underline{Q}}$ så (jvf. sætning 44)

$$\underline{\underline{P}}\,\underline{\underline{A}}\,\underline{\underline{Q}} = \begin{Bmatrix} \varepsilon_1 & 0 & \\ & & \underline{\underline{0}} \\ 0 & \varepsilon_m & \end{Bmatrix} \quad \textit{for passende hele tal } \varepsilon_1, \dots, \varepsilon_m$$

Bevis. Vi viser, at $\underline{\underline{A}}$ kan bringes på den ønskede form ved successiv anvendelse af følgende to operationer:

1) erstatte u_i med $u_i + \gamma u_j$ $(i \neq j)$, $\gamma \in \mathbb{Z}$. Dette svarer til, at man i $\underline{\underline{A}}$ subtraherer γ (i^{te} søjle) fra den j^{te} søjle.
2) erstatte v_i med $v_i + \gamma v_j$ $(i \neq j)$, $\gamma \in \mathbb{Z}$. Dette svarer til, at man i $\underline{\underline{A}}$ adderer γ (j^{te} række) til den i^{te} række.

Uden indskrænkning kan $\underline{\underline{A}}$ antages $\neq 0$. Betragt nu alle de matricer der fås ud fra $\underline{\underline{A}}$ ved successiv anvendelse af 1) og 2). Lad ε være det numerisk mindste hele tal $\neq 0$, der på nogen plads optræder i en af disse matricer. Ved 1) og 2) kan ε føres op på 1^{ste} række og 1^{ste} søjle. Ved yderligere anvendelse af 1) og 2) kan man opnå, at alle øvrige elementer i 1^{ste} række og 1^{ste} søjle er 0. (Ved denne og den foregående reduktion benyttes Euklids algoritme på velkendt måde).

$\underline{\underline{A}}$ kan således føres over i en matrix af formen

$$\begin{pmatrix} \varepsilon & 0 & \cdots & 0 \\ 0 & & & \\ & & \underline{\underline{A}}_1 & \\ 0 & & & \end{pmatrix}$$

hvor $\underline{\underline{A}}_1$ er $(m-1) \times (n-1)$ heltalsmatrix. Ovennævnte proces gentages på $\underline{\underline{A}}_1$ der føres over i en matrix af formen,

$$\begin{pmatrix} \varepsilon_1 & 0 & \cdots & 0 \\ 0 & & & \\ & & \underline{\underline{A}}_2 & \\ 0, & & & \end{pmatrix}$$

hvor $\underline{\underline{A}}_2$ er en $(m-2) \times (n-2)$ heltalsmatrix; dernæst anvendes processen på $\underline{\underline{A}}_2$ etc. Efter endelig mange skridt føres $\underline{\underline{A}}$ herved over i en matrix af den ønskede form.

Vi bringer to anvendelser af elementærdivsorsætningen: Hovedsætningen om endelig frembragte abelske grupper og bestemmelsen af kommutatorgrupper for visse lineære grupper, hvorved en ny familie simple grupper findes. Vi tager sidstnævnte anvendelse først.

Vi bemærker først, at matricen der bevirker basisskiftet ved 1) i ovenstående bevis er $\underline{\underline{E}} + \gamma \underline{\underline{E}}_{ij}$, hvor $\underline{\underline{E}}_{i,j}$ er matricen, der har 1 på $(i,j)^{\text{te}}$ plads og ellers lutter nuller. Tilsvarende for basisskiftet 2). Matricer af denne form $(i \neq j)$ kaldes *elementære*. De har åbenbart determinant 1.

I kraft af ovenstående bemærkning og (beviset for) elementærdivisorsætningen fås således:

Sætning 46. *Lad $\underline{\underline{A}}$ være vilkårlig $(m\times n)$ heltalsmatrix. Da findes elementære $(m\times m)$ matricer $\underline{\underline{E}}'_1,\dots,\underline{\underline{E}}'_\mu$ og elementære $(n\times n)$ matricer $\underline{\underline{E}}''_1,\dots,\underline{\underline{E}}''_\nu$ så*

$$\underline{\underline{E}}'_1,\dots,\underline{\underline{E}}'_\mu\,\underline{\underline{A}}\,\underline{\underline{E}}''_1\dots\underline{\underline{E}}''_\nu = \textit{diagonalmatrix}\begin{pmatrix}\varepsilon_1 & 0 & \\ & & \underline{0} \\ 0 & \varepsilon_m & \end{pmatrix}.$$

Tilføjelse. Ovennævnte gælder også (beviset endda kun lidt simplere), hvis vi i stedet for frie abelske grupper betragter vektorrum over et vilkårligt legeme. Specielt gælder ovenstående sætning for matricer med elementer i et legeme.

De to følgende lemmaer viser vi generelt for en vilkårlig kommutativ ring med et et-element for ikke at skulle skelne mellem gruppetilfældet og vektorrumstilfældet. Begrebet "elementær matrix" overføres uden videre til matricer over en vilkårlig kommutativ ring med et-element.

Lemma 1. *Lad a og b være invertible elementer i ringen R. Da kan $\begin{pmatrix} a & 0 \\ 0 & b\end{pmatrix}$ ved multiplikation af elementær matricer (fra venstre og højre) føres over i matricen $\begin{pmatrix} 1 & 0 \\ 0 & ab\end{pmatrix}$.*

Bevis.

$$\begin{pmatrix} 1 & 0 \\ 0 & ab\end{pmatrix} = 1\begin{pmatrix} 1 & 0 \\ ab-b & 1\end{pmatrix}\begin{pmatrix} 1 & \frac{1}{b} \\ 0 & 1\end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b\end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1-a & 1\end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1\end{pmatrix}$$

Ved successiv anvendelse af dette lemma fås umiddelbart

Lemma 2. *Lad $a_1,\dots,a_n$ være invertible elementer i ringen R. Da kan*

$$\begin{pmatrix} a_1 & 0 & 0 & \cdots & 0 \\ 0 & a_2 & 0 & & 0 \\ 0 & 0 & & & \\ 0 & & & & a_n \end{pmatrix}$$

ved multiplikation af elementære matricer (fra venstre og højre) føres over i matricen

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots\dots\dots & & 0 \\ 0 & 0 & 1 & 0 & \dots & \\ 0 & & & 0 & a_1a_2 \quad \dots & a_n \end{pmatrix}.$$

For en vilkårlig kommutativ ring R med et element defineres den generelle lineære gruppe af Grad n, $\mathrm{GL}(n,R)$, *som gruppen (med sædvanlig matrixmultiplikation) af alle $(n\times n)$ matricer med elementer i R og determinant et invertibelt element i R.*

Den specielle lineære gruppe

Den specielle lineære gruppe af grad n defineres som undergruppen i $\mathrm{GL}(n,R)$ bestående af matricerne med determinant 1.

Ved determinantafbildningen $\mathrm{GL}(n,R) \xrightarrow{\det} R^*$, hvor R^* er gruppen af invertible elementer i R, ses (idet $\mathrm{SL}(n,R) = \mathrm{Ker}(\det)$) at $\mathrm{SL}(n,R) \triangleleft \mathrm{GL}(n,R)$ og $\mathrm{GL}(n,R)/\,\mathrm{SL}(n,R) \simeq R^*$.

Heraf følger, at kommutatorgruppen $\mathrm{GL}(n,R)'$ er indeholdt i $\mathrm{SL}(n,R)$.

Vi vil nu vise at for $R = \mathbb{Z}$ eller et vilkårligt legeme gælder $\mathrm{GL}(n,R)' = \mathrm{SL}(n,R)$ (på nær en enkelt undtagelse). Vi viser først:

Sætning 47. *Hvis $R = \mathbb{Z}$ eller et vilkårligt legeme kan enhver matrix $\underline{\underline{A}} \in \mathrm{SL}(n,R)$ skrives som produkt af elementære matricer. Med andre ord er $\mathrm{SL}(n,R)$ frembragt af mængden af elementære matricer.*

Bevis. På grund af sætning 45 (og tilføjelsen) findes elementære matricer $\underline{\underline{E}}'_1 \dots \underline{\underline{E}}'_\mu$, $\underline{\underline{E}}''_1, \dots, E''_\nu$ så

$$\underline{\underline{E}}'_1 \dots \underline{\underline{E}}'_\mu \,\underline{\underline{A}}\, E''_1 \dots E''_\nu = \begin{pmatrix} a_1 & 0 \\ 0 & a_n \end{pmatrix}$$

hvor $1 = \det \underline{\underline{A}} = a_1 \dots a_n$.

Ifølge Lemma 2, kan $\begin{pmatrix} a_1 & 0 \\ 0 & a_n \end{pmatrix}$ ved multiplikation med elementære matricer føres over i

$$\begin{pmatrix} 1 & 0 & & \\ & 1 & & \\ 0 & a_1 & \vdots & a_n \end{pmatrix} = \underline{\underline{E}}\,.$$

Da den reciprolle matrix af en elementær matrix selv er elementær (bemærk at $(\underline{\underline{E}} + \gamma \underline{\underline{E}}, j)^{-1} = \underline{\underline{E}} - \gamma \underline{\underline{E}}_{ij}$) følger heraf, at $\underline{\underline{A}}$ er produkt af elementære matricer.

Sætning 48. *Hvis $R = \mathbb{Z}$ eller et vilkårligt legeme gælder for $n \geqq 3$, at $\mathrm{SL}(n,R) = \mathrm{SL}(n,R)'$. Specielt er $\mathrm{GL}(n,R)' = \mathrm{SL}(n,R)$ for $n \geqq 3$.*

Bevis. På grund af foregående sætning er det nok at godtgøre, at enhver elementær matrix tilhører $\mathrm{SL}(n,R)'$. Vi viser endda, at enhver elementær matrix er en kommutator i $\mathrm{SL}(n,R)$. Lad $\underline{\underline{E}} + \gamma \underline{\underline{E}}_{i,k}$ være en vilkårlig elementær matrix $1 \le i,k \le n$ $i \neq k$. Da $n \geq 3$ findes j $1 \leqq j \leqq n$ så i, j og k er indbyrdes forskellige. For et sådant j gælder:

$$(\underline{\underline{E}} + \gamma \underline{\underline{E}}_{i,j})(\underline{\underline{E}} + \underline{\underline{E}}_{i,k})(\underline{\underline{E}} + \gamma E_{i,j})^{-1}(\underline{\underline{E}} + \underline{\underline{E}}_{i,k})^{-1} = \underline{\underline{E}} + \gamma \underline{\underline{E}}_{j,k}$$

Sætning 49. *Hvis R er et legeme med mindst 3 elementer gælder* $\mathrm{GL}(2,R)' = \mathrm{SL}(2,R)$.

Bevis. Skal blot godtgøre, at $\mathrm{SL}(2,R) \leq \mathrm{GL}(2,R)'$. Ved samme argument som i foregående sætning er det nok at vise, at enhver elementær (2×2) matrix er en kommutator i $\mathrm{GL}(2,R)$. Da R har mindst 3 elementer findes et element $u \neq \begin{cases} 0 \\ 1 \end{cases}$. For et vilkårligt $\gamma \in R$ gælder nu:

$$\begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -\frac{\gamma}{1-u} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & \frac{-\gamma}{1-u} \\ 0 & 1 \end{pmatrix}^{-1}$$

og tilsvarende for $\begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}$.

Opgave. Vis, at for $R = \mathbb{Z}/\mathbb{Z}2$ (legemet med 2 elementer) er $\mathrm{GL}(2,R) = \mathrm{SL}(2,R) \simeq S_3$ og $\mathrm{SL}(2,R)' = \mathrm{GL}(2,R)'$ dermed en ægte undergruppe i $\mathrm{GL}(2,R) = \mathrm{SL}(2,R)$. Forudsætningen i foregående sætning angående R er således nødvendig.

Sætning 50. *Hvis R er et legeme med mindst 4 elementer gælder* $\mathrm{SL}(2,R)' = \mathrm{SL}(2,R)$.

Bevis. Da R har mindst 4 elementer findes et $b \in R$, så $b \neq 0$, $b^2 \neq 1$. Vi er

$$\begin{pmatrix} b & 0 \\ 0 & \frac{1}{b} \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & \frac{1}{b} \end{pmatrix}^{-1} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a(b^2-1) \\ 0 & 1 \end{pmatrix}$$

for ethvert $a \in R$. Da $b^2 - 1 \neq 0$ gennemløber $a(b^2-1)$, $a \in R$, elle elementerne i R. Følgelig er enhver elementær matrix kommutator i $\mathrm{SL}(2,R)$.

Opgave. Vis, at for $R = \mathbb{R}$, de reelle tals legeme, og $n = 2$ er $-\underline{\underline{E}} \in \mathrm{SL}(2,\mathbb{R})'$ men $-\underline{\underline{E}}$ kan ikke skrives som en kommutator (dvs.: $-\underline{\underline{E}} \neq A\,B\,A^{-1}\,B^{-1}$ for alle $\underline{\underline{A}}, \underline{\underline{B}} \in \mathrm{SL}(2,\mathbb{R})$).

Vi er her i stand til at give en ny familie af simple grupper. Lad nu R være et kommutativt legeme K. En enkelt udregning viser, at centrum $(\mathrm{SL}(n,K)) =$ matricerne

$$\begin{pmatrix} \lambda & 0 & 0 & \vdots \\ 0 & \lambda & 0 & \vdots \\ 0 & \cdots & \cdots & \lambda \end{pmatrix}, \quad \lambda \in K\,,\ \lambda^n = 1\,.$$

(Benyt, at matricerne i centrum kommuterer med alle elementære matricer). Den projektive specielle lineære gruppe $\mathrm{PSL}(n,K)$ af grad n over K defineres som $\mathrm{SL}(n,K)/$ centrum $(\mathrm{SL}(n,K))$.

Vi stiler mod at vise, at $\mathrm{PSL}(n,K)$ er simpel for $n \geqq 3$ og alle K og simpel for $n = 2$ når K har mindst 4 elementer. Vi indføjer nu et par bemærkninger om det projektive rum $P(n,K)$. For et kommutativt legeme K lad $V(n+1,K)$ være det $(n+1)$-dimensionale vektorrum over K. I $V(n+1,K) \setminus \{0\}$ defineres en ækvivalensrelation ved $\underline{a} \sim \underline{b} \iff \exists \lambda \in K \setminus \{0\}$ så $\underline{a} = \lambda \underline{b}$. Mængden af ækvivalensklasser kaldes n-dimensionale projektive rum $P(n,K)$. Dette kan intuitivt beskrives som mængden af "udprikkede" rette linier gennem 0 i $V(n+1,K)$.

Enhver matrix $\underline{\underline{A}} \in \mathrm{SL}(n+1,K)$ inducerer på oplagt vis en permutation $\rho_{\underline{\underline{A}}}$ i $P(n,K)$. Kernen for afbildningen $\underline{\underline{A}} \to \rho_{A}$ ses let at være skalarmatricerne $\lambda \underline{\underline{E}} \in \mathrm{SL}(n+1,K)$ dvs. centrum for $\mathrm{SL}(n+1,K)$.

Følgelig kan $\mathrm{PSL}(n+1,K)$ opfattes som en permutationsgruppe på $P(n,K)$. Vi påstår nu

Lemma. $\mathrm{PSL}(n+1,K)$ *er en dobbelt-transitiv permutationsgruppe på* $P(n,K)$.

Bevis. Lad $\overline{\underline{a}_1}$, $\overline{\underline{a}_2}$ og $\overline{\underline{b}_1}$, $\overline{\underline{b}_2}$ være punktpar i $P(n,K)$ $\overline{\underline{a}_1} \neq \overline{\underline{a}_2}$ og $\overline{\underline{b}_1} \neq \overline{\underline{b}_2}$. For repræsentanter a_1, a_2, b_1, b_2 gælder $\underline{a}_1$ og $\underline{a}_2$ ej proportionale, $\underline{b}_1$ og $\underline{b}_2$ ej proportionale. Derfor findes $\underline{\underline{A}} \in \mathrm{SL}(n+1,K)$ så $\underline{\underline{A}}\,\underline{a}_1 = \underline{b}_1$ $\underline{\underline{A}}\,a_2 = \lambda b_2$ for passende $\lambda \in K \setminus \{0\}$. Følgelig er $\rho_{\underline{\underline{A}}}(\overline{\underline{a}_1}) = \overline{\underline{b}_1}$ og $\rho_{\underline{\underline{A}}}\overline{\underline{a}_2} = \lambda\overline{\underline{b}_1} = \overline{\underline{b}_2}$.

Vi kan nu vise

Sætning 51. *Grupperne* $\mathrm{PSL}(n,K)$ *er simple for alle* $n \geq 2$ *og alle legemer* K *undtagen for* $n = 2$ *og* $K =$ *legemet med 2 eller 3 elementer.*

Bevis. På nær i de to nævnte undtagelsestilfælde er $\mathrm{SL}(n,K) = \mathrm{SL}(n,K)'$ ifølge Sætning 48 og Sætning 50. Da gælder også $\mathrm{PSL}(n,K) = \mathrm{PSL}(n,K)'$ og $\mathrm{PSL}(n,K)$ er en dobbelt-transitiv permutationsgruppe på $P(n-1,K)$.

Vi ønsker nu at anvende simpelhedskriteriet i Sætning 20. For et punkt @ $\in P(n-1,K)$ skal vi angive en abelsk normaldeler $\mathcal{K}$ i stabilisatorgruppen for @ så $\mathrm{PSL}(n,K)$ er frembragt af de med $\mathcal{K}$ konjugerede grupper. I $V(n,K)$ betragter vi følgende lineære afbildninger: Lad $\underline{a} \in V(n,K)\setminus\{0\}$ og μ en fra 0 forskellig linearform på $V(n,K)$ der forsvinder på $\underline{a}$. Vi betragter de såkaldte transvektioner T, der er lineære afbildninger defineret ved

$$T_{\mu,\underline{a}}\underline{v} = \underline{v} - \mu(\underline{v})a \quad v \in V(n,K) \tag{$*$}$$

Man bemærker, at den til en elementær matrix svarende lineære afbildning er en transvektion. Specielt vil transvektionerne frembringe hele $\mathrm{SL}(n,K)$ (jfr. Sætning 47).

For fast $\underline{a}$ udgør transvektionerne $\{T_{\mu,\underline{a}} | \mu \text{ lineærform}, \mu(\underline{a}) = 0\}$ en undergruppe i $\mathrm{SL}(n,K)$. Denne undergruppe $\widetilde{\mathcal{K}}$ er abelsk, idet $T_{\mu,\underline{a}}$, $T_{v,\underline{a}} = T_{\mu+v,\underline{a}}$.

For ethvert $\underline{\underline{S}} \in \mathrm{SL}(n,K)$ gælder

$$\underline{\underline{S}}\, T_{\mu,\underline{a}}\, \underline{\underline{S}}^{-1} = T_{\mu \underline{a}^{-1}, \underline{\underline{S}}\, \underline{a}}\,,$$

hvoraf ses:

i) $\widetilde{\mathcal{K}}$ er normaldeler i stabilisatorgruppen for $\underline{a}$;

ii) Enhver transvektion er konjugeret med en transvektion i $\widetilde{\mathcal{K}}$.

Foreningsmængden af de med $\widetilde{\mathcal{K}}$ konjugerede undergrupper frembringer således hele $\mathrm{SL}(n,K)$.

Den tilsvarende gruppe $\mathcal{K}$ i $\mathrm{PSL}(n,K)$ kan derfor anvendes i det omtalte simpelhedskriterium, hvorved sætningen er bevist.

Bemærkning. For $n = 2$, $K = \mathbb{Z}/2\mathbb{Z}$ er $\mathrm{PSL}(2,K) \simeq S_3$, og for $n = 2$, $K = \mathbb{Z}/3\mathbb{Z}$ er $\mathrm{PSL}(2,K) \simeq A_4$.

Ingen af disse er som bekendt simple.

For at finde de endelige grupper blandt den nye familie af simple grupper får vi brug for sætninger om endelige legemer som vi får i næste kapitel. Vi nævner dem her:

1. Ethvert endeligt legeme har orden p^m, hvor p er et primtal, $m \in \mathbb{N}$.
2. Til enhver primtalspotens p^m findes et – pånær isomorfi – kun et legeme med p^m elementer.

Endvidere får vi senere i dette kapitel

3. Et endeligt legemes multiplikative gruppe er cyklisk

For en primtalspotens q betegner vi med $\mathrm{GL}(n,q)$, $\mathrm{SL}(n,q)$ og $\mathrm{PSL}(n,q)$ grupperne $\mathrm{GL}(n,K)$, $\mathrm{SL}(n,K)$, $\mathrm{PSL}(n,K)$, hvor K er det entydigt bestemte legeme med q elementer.

Ved et elementært kombinatorisk argument findes

$$|\,\mathrm{GL}(n,q)| = (q^n - 1)(q^n - q)(q^n - q^2)\dots(q^n - q^{n-1})$$

og herved

$$|\,\mathrm{SL}(n,q)| = \frac{|\,\mathrm{GL}(n,q)|}{q-1} = (q^n - 1)(q^n - q)\dots(q^n - q^{n-2})q^{n-1}$$

Fra definition af PSL er det klart, at

$$|\,\mathrm{PSL}(n,q)| = \frac{|\,\mathrm{SL}(n,q)|}{\begin{array}{l}(\text{ antallet af rødder til } x^n = 1\\ \text{inden for } K)\end{array}}$$

Idet K's multiplikative gruppe af fra 0 forskellige elementer er cyklisk (jfr. 3) bliver antallet af rødder til ligningen $x^n = 1$ i K netop $(n, q-1)$, hvor alment (a,b) betegner største fælles mål af a og b. Dette følger af:

Lemma. *I en cyklisk gruppe af orden m har ligningen $x^n = \ell$ netop (m,n) løsninger.*

Bevis. Lad u være en brembringer for gruppen u^a, $a \in \mathbb{Z}$ er løsning til ligningen $x^n = \ell$ hvis og kun hvis $na \equiv 0 \pmod{m}$. Sidstnævnte kongruens har præcis (m,n) løsninger.

Korollar. $|\operatorname{PSL}(n,q)| = \frac{(q^n-1)(q^n-q)\ldots(q^n-q^{n-2})q^{n-1}}{(n,q-1)}$.

Man kan vise, at de eneste isomorfier der består mellem grupperne $\operatorname{PSL}(n,q)$ og de alternerende grupper og symmetriske grupper er:

(1) $\operatorname{PSL}(2,2) = \operatorname{SL}(2,2) = \operatorname{GL}(2,2) \simeq S_3$.
(2) $\operatorname{PSL}(2,3) \simeq A_4$.
(3) $\operatorname{PSL}(2,4) \simeq \operatorname{PSL}(2,5) \simeq A_5$.
(4) $\operatorname{PSL}(2,7) \simeq \operatorname{PSL}(3,2)$.
(5) $\operatorname{PSL}(4,2) \simeq A_8$.
(6) $\operatorname{PSL}(2,9) \simeq A_5$.

Bemærk, at $|\operatorname{PSL}(3,4)| = |A_8| = \frac{1}{2} \times 8!$.

$\operatorname{PSL}(3,4)$ og A_8 er således simple, ikke-isomorfe grupper af samme orden!

Hovedsætningen om endelig frembragte abelske grupper

Først en definition

Definition. Lad $A_1, A_2, \ldots, A_n$ være n abelske grupper. Alle ordnede n-tripler $(a_1, a_2, \ldots, a_n)$, $a_i \in A_i$, $1 \le i \le n$, udgør en abelsk gruppe med komponentvis addition. Denne kaldes *den (ydre) direkte sum* af $A_1, A_2, \ldots, A_n$ og betegnes $A_1 \oplus A_2 \oplus \cdots \oplus A_n$. Hvis alle A_i, $1 \le i \le n$, er samme gruppe A, skrives kort A^n.

Et vigtigt eksempel er givet i

Sætning 52. *Lad $n = {p_1}^{a_1} \ldots {p_r}^{a_r}$, hvor $p_1 \ldots p_r$ er indbyrdes forskellige primtal. Da er $\mathbb{Z}_n \simeq \mathbb{Z}_{p_1}a_1 \oplus \cdots \oplus \mathbb{Z}_{p_r}a_r$.*

Bevis. Definer homomorfi $\varphi : \mathbb{Z} \to \mathbb{Z}_{p_1}a_1 \oplus \cdots \oplus \mathbb{Z}_{p_r}a_r$ ved $\varphi(h) = (h_{p_1}a_1, \ldots, h_{p_r}a_r)$. Her er $\operatorname{Ker}\varphi \simeq n\mathbb{Z}$, hvorfor ifølge homomorfisætningen $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n \simeq \varphi\mathbb{Z} \subseteq \mathbb{Z}_{p_1}a_1 \oplus \cdots \oplus \mathbb{Z}_{p_r}a_r$. Da $\varphi\mathbb{Z}$ og $\mathbb{Z}_{p_1}a_1 \oplus \cdots \oplus \mathbb{Z}_{p_r}a_r$ således har samme orden $n = {p_1}^{a_1} \ldots {p_r}^{a_r}$, må $\varphi\mathbb{Z} = \mathbb{Z}_{p_1}a_1 \oplus \cdots \oplus \mathbb{Z}_{p_r}a_r$.

Sætning 53. *Enhver endelig frembragt abelsk gruppe A er (isomorf med) en direkte sum af cykliske grupper.*

Bevis. Antag $a_1, \ldots, a_n$ frembringer A. Lad $F = \mathbb{Z}^n$ være den fri abelske gruppe med basis $\ell_1 = (1, 0, \ldots, 0), \ldots, \ell_n = (0, \ldots, 0, 1)$ og lad φ være den ved $\varphi(h_1, \ldots, h_n) = h_1a_1 + \cdots + h_na_n$ definerede homomorfi fra $\mathbb{Z}^n$ til A. $K = \operatorname{Ker}\varphi$ er undergruppe i F og derfor (Sætning 45) fri af rang $m \leqq n$. Ifølge elementærdivisorsætningen findes baser $u_1, \ldots, u_n$, $v_1, \ldots, v_m$ for F, henholdsvis K, så

$$\begin{aligned} v_1 &= \varepsilon_1 u_1 \\ v_m &= \varepsilon_m u_m \,. \end{aligned}$$

Ethvert element x i F kan entydigt skrives $x = h_1u_1 + \cdots + h_nu_n$, $h_1, \ldots, h_n \in \mathbb{Z}$. Vi definerer en homomorfi ψ fra F til

$$G = \mathbb{Z}_{\varepsilon_1} \oplus \cdots \oplus \mathbb{Z}_{\varepsilon_m} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \quad (n-m) \text{ eksemplarer}$$

ved

$$\psi(x) = ([h_1]_{\varepsilon_1}, \ldots, [h_m]_{\varepsilon_m}\,, \quad h_{m+1}, \ldots, h_n)$$

ψ er oplagt surjektiv.

$$\operatorname{Ker}\psi = \{x \in F | h_1 \equiv 0 \mod \varepsilon_1, \ldots, h_m \equiv 0 \mod \varepsilon_m\,,\ h_{m+1} = \cdots = h_n = 0\} = K\,.$$

Ifølge homomorfisætningen har vi derfor

$$G \simeq F/\operatorname{Ker}\psi = F/K = F/\operatorname{Ker}\varphi \simeq A\,,$$

dvs. $A \simeq G$, der er direkte sum af cykliske grupper.

Korollar. *Hvis A er en endelig frembragt torsionsfri abelsk gruppe, da er A fri.*

BEMÆRKNING. Forudsætningen A endelig frembragt er vigtig (modeksempel $(Q, +)$).
Kombination af de viste sætninger giver umiddelbart

Hovedsætning. *Enhver endelig frembragt abelsk gruppe A er (isomorf med) den direkte sum af eksemplarer af $\mathbb{Z}$ og af cykliske grupper af primtalspotens, dvs.*

$$A \simeq \mathbb{Z}^n \oplus \sum_{i,j} \oplus \mathbb{Z}_{p_i{}^j}^{\ell_{i,j}} \tag{$*$}$$

for passende n og $\ell_{i,j} \geq 0$ og visse (endelig mange) primtal p_i. Eksponenterne n og $\ell_{i,j}$ er entydigt bestemte ved A.

Bevis. Eksistensudsagnet følger af det foregående. Entydighedsudsagnet er en simpel konsekvens af følgende generelle

Forkortningssætning. *Lad G og H være vilkårlige abelske grupper, F en endelig frembragt abelsk gruppe. Hvis $F \oplus G \simeq F \oplus H$, da er $G \simeq H$.*

Inden beviset for denne sætning omtaler vi begrebet "indre direkte sum". Lad $A_1, \ldots, A_n$ være undergrupper i en given abelsk gruppe A. A siges at være *indre direkte sum* af $A_1, \ldots, A_n$, hvis ethvert element $a \in A$ på entydig måde kan skrives $a = a_1 + \cdots + a_n$, $a_1 \in A_1, \ldots, a_n \in A_n$. I så fald skriver man $A = A_1 \oplus \cdots \oplus A_n$. Forbindelsen mellem den tidligere indførte (ydre) direkte sum og den indre direkte sum er:

Lad $A = A_1 \oplus \cdots \oplus A_n$ (indre direkte sum), da er $A \simeq A_1 \oplus \cdots \oplus A_n$ (ydre direkte sum). En isomorfi fra den ydre til den indre direkte sum er givet ved

$$(a_1, \ldots, a_n \mid\!\!\longrightarrow (a_1 + \cdots + a_n))\,.$$

Omvendt. lad A være ydre direkte sum $A = A_1 \oplus \cdots \oplus A_n$ (ydre direkte sum). Undergrupperne $A_i' = \{(0, \ldots, a_i, 0, \ldots, 0) | a_i \in A_i\}$ er isomorfe med A_i og man ser let, at $A = A_1' \oplus \cdots \oplus A_n'$ (indre direkte sum). Lad A være undergruppe i den abelske gruppe B. A siges at være *en direkte summand i B*, hvis der findes undergruppe $K \subseteq B$ så $B = A \oplus K$ (indre direkte sum). Når et sådant K findes, må $K \simeq B/A$.

Lemma. *Lad A være undergruppe i B. Hvis $B/A \simeq \mathbb{Z}$, er A direkte summand i B.*

Bevis. Lad κ være den kanoniske homomorfi: $B \to B/A$ og lad $c \in B$ være et element så $\kappa\, c$ frembringer $B/A \simeq \mathbb{Z}$. For den cykliske undergruppe K i B frembragt af c gælder nu

$$B = A \oplus K \quad \text{(indre direkte sum)}$$

Thi for etjver $b \in B$ findes helt tal h så $\kappa\, b = h\, \kappa\, c$ dvs.: $b - hc \in \operatorname{Ker} \kappa = A$ dvs.: $b =$ (element i A) $+$ (element i K). Endvidere, hvis $0 = a + hc$, $a \in A$, $h \in C$, da må $0 = \kappa\, a + h\, c = h\, \kappa\, c \Rightarrow h = 0 \Rightarrow a = 0$. Altså er $B = A \oplus K$ (indre direkte sum).

Inden beviset for forkortningssætningen endnu et (isoleret stående)

Lemma. *Lad G være en abelsk gruppe, g et element i G hvis orden er en primtalspotens p^n. Lad V være den cykliske undergruppe i G frembragt af g og H en vilkårlig undergruppe i G. Da gælder $V \cap H \neq \{0\} \Leftrightarrow p^{n-1}g \in H$.*

Bevis. "$\Leftarrow$" klart.

"$\Rightarrow$" $V \cap H \neq \{0\}$ medfører, at der findes et multiplum bg. $b \in \mathbb{Z}$, $p^n \nmid b$ så $bg \in H$. b kan skrives $b = p^i a$, $0 \leq i < n \quad p \nmid a$. Da $p \nmid a$ findes $x, y \in \mathbb{Z}$ så $ax + p^n y = 1$, hvoraf $p^{n-1}ax + p^{2n-1}y = p^{n-1}$ og dermed $p^{n-1}axg + p^{2n-1}yg = p^{n-1}g$. Vi behøver nu blot at bemærke, at $p^{n-1}axg \in H$ og $p^{2n-1}yg = 0$.

Nu bevis for forkortningssætningen. På grund af eksistensudsagnet i hovedsætningen er det åbenbart tilstrækkeligt at vise forkortningssætningen i tilfældet hvor F er uendelig cyklisk (dvs.: $\simeq \mathbb{Z}$) eller er cyklisk af primtalspotensorden.

Oversat til indre direkte summer skal vi vise:

Lad E være abelsk gruppe så $E = A \oplus B \oplus H$ (indre direkte summer) og enten $A \simeq B \simeq \mathbb{Z}$ eller $A \simeq B \simeq \mathbb{Z}p^n$ (p^n er primtalspotens), da er $G \simeq H$.

1) Lad os først betragte tilfældet $A \simeq B \simeq \mathbb{Z}$. Sæt $D = G \cap H$; ifølge Noether's 1. isomorfisætning gælder:

$$G/D \simeq G + H/H\,;\ G + H/H \ \text{ er undergruppe i } \ E/H \simeq B \simeq \mathbb{Z}$$

hvorfor $G/D = 0$ eller $\simeq \mathbb{Z}$. Følgelig er $G = D$ eller $G = D \oplus U$, $U \simeq \mathbb{Z}$ (jfr. lemmaet).

Analogt gælder $H = D$ eller $H = D \oplus V$, $V \simeq \mathbb{Z}$.

Beviset fuldføres ved at godtgøre, at kombinationerne $G = D \ \wedge \ H = D \oplus V$ og $G = D \oplus U \ \wedge \ H = D$ ikke kan indtræffe. Af symmetrigrunde nok at vise, at $G = D$ er uforenelig med $H = D \oplus V$. $G = D \ \wedge \ H = D \oplus V$ ville indebære $E = A \oplus D = B \oplus D \oplus V$ og dermed $E/D \simeq A \simeq B \oplus V$ eller $\mathbb{Z} \simeq \mathbb{Z} \oplus \mathbb{Z}$, hvilket umuligt (jfr. Sætning 42).

2) Nu tilfældet $A \simeq B \simeq \mathbb{Z}_{p^n}$, hvor p^n er en printalspotens. Vi viser først, at der findes et element u i E af orden p^u så $U \cap G = U \cap H = 0$, hvor U er den cykliske undergruppe frembragt af u. Lad a, resp. b, være frembringer for A, resp. B.

$$\begin{array}{c} \text{Hvis } \ A \cap H = 0 \ \text{ kan } \ a \ \text{ bruges som } \ u\,. \\ \text{Hvis } \ B \cap G = 0 \ \text{ kan } \ b \ \text{ bruges som } \ u\,. \end{array}$$

Antag derfor $A \cap H \neq \{0\}$ og $B \cap G \neq \{0\}$. Ifølge lemmaet er da $p^{n-1}a \in H$ og $p^{n-1}b \in G$. For $a + b$ gælder:

$$\begin{array}{lclclcl} p^n(a+b) = 0\,, \quad p^{n-1}(a+b) & = & (p^{n-1}a & + & p^{n-1}b) & \notin H \\ & & \in H & & \notin H & \notin G \\ & & \notin G & & \in G & \end{array}$$

hvorfor $a + b$ er brugbart som u.

For det således konstruerede u og tilsvarende cykliske undergruppe U af orden p^n gælder:

$$U+G/G \simeq U/U\cap G \simeq U_j \quad |U+G/G| = p^n\,.$$

Idet $G \subseteq U+G \subseteq A+G = E$ og $U+G/G \subseteq A+G/G \simeq A$ ses, at $U+G/G = A?G/G$, da $|A+G/G| = |E/G| = p^n$. Følgelig er $E = U+G$ og idet $U\cap G = 0$ er $U+G = U\oplus G$. Altså er $E = U\oplus G$.

Analogt fås $E = U\oplus H$, hvoraf $G \simeq E/U \simeq H$.

Forkortningssætningen er nu fuldstændigt bevist.

Bemærkning. Forudsætningen F endelig frembragt er væsentlig for forkortningssætningens rigtighed (modeksempel ?)

Vi afslutter afsnittet om abelske grupper med nogle anvendelser af hovedsætningen om endelig frembragte abelske grupper. Først en umiddelbar konsekvens om antallet af ikke-isomorfe abelske grupper. Lad $\mathcal{A}(n)$ være antallet af ikke-isomorfe abelske grupper af orden n. Lad $n = {p_1}^{a_1}\dots {p_r}^{a_r}$ være n's primfaktoropløsning. Da giver hovedsætningen, at $\mathcal{A}(n) = \mathcal{A}({p_1}^{a_1})\dots\mathcal{A}({p_r}^{a_r})$ og for en primtalspotens p^a gælder: $\mathcal{A}(p^a) = p(a)$, hvor $p(a)$ er antallet af "partitioner" af a dvs.: Antallet af måder a kan skrives som sum af naturlige tal.

Endelig et kriterium for cykliske grupper.

Sætning 54. *Lad G være en endelig abelsk gruppe. Da er følgende betingelser ækvivalente:*

(i) *G er cyklisk.*
(ii) *For ethvert primtal p har ligningen $px = 0$ højst p løsninger x i G.*
(iii) *For ethvert primtal $p, p \mid |G|$, har ligningen $px = 0$ netop p løsninger x i G.*

Bevis. (i) $\Rightarrow$ (ii) umiddelbar, da $G \simeq \mathbb{Z}_n$ for passende n.

(ii) $\Rightarrow$ (iii) her bemærkes blot, at for $p|G|$ findes elementer af orden p (benyt enten p. ? eller hovedsætningen om endeligt frembragte abelske grupper).

(iii) $\Rightarrow$ (i) indebærer, at for ethvert primtal p_i, der går op i $|G|$, findes netop ét j, for hvilket $\ell_{i,j} \neq 0$ i fremstillingen $(*)$ i hovedsætningen og dette $\ell_{i,j} = 1$. Sætning 51 viser da, at G er cyklisk.

Korollar. *Enhver endelig undergruppe G i et (kommutativt) legemes multiplikative gruppe (dvs.: Gruppen af elementerne $\neq 0$) er cyklisk.*

Bevis. Ligningen $x^p = 1$ har højst p rødder. (Et polynomium over et legeme har højst så mange rødder som graden angiver).

Korollaret viser specielt, at et endeligt legemes multiplikative gruppe er cyklisk.

Kapitel II. Ringe og polynomier

LIDT ALMENT OM RINGE OG IDEALER.

En *ring* R er en ikke-tom mængde med to kompositioner $+$ og $\cdot$, så

1) $(R, +)$ er en abelsk gruppe;
2) $(R, \cdot)$ er associativ;
3) $a \cdot (b + c) = a \cdot b + a \cdot c$
   $(a + b) \cdot c = a \cdot c + b \cdot c.$

Hvis $(R, \cdot)$ er kommutativ, kaldes R *kommutativ.* Et neutralt element m.h.t. $\cdot$ er entydigt bestemt og kaldes *ételementet* og betegnes i reglen med 1 (undertiden dog e) . Vi skal i det følgende kun betragte kommutative ringe med etelement.

Vi minder om nogle definitioner og sætninger, der er kendt fra Mat 2AL.

DEFINITION. En additiv undergruppe I i $(R, +)$, hvor R er en kommutativ ring med ételement, kaldes et *ideal*, hvis $RI \subseteq I$.

En kommutativ ring R kaldes et *integritetsområde*, hvis nulreglen gælder i R, dvs. et produkt af to elementer i R kan kun være 0, hvis mindst en af faktorerne er 0.

En kommutativ ring R kaldes et *legeme*, hvis ethvert fra 0 forskelligt element a i R har et inverst, dvs. et element $a^{-1} \in R$, så $aa^{-1} = 1$.

Ethvert legeme er specielt et integritetsområde.

DEFINITION. Et ideal I i R kaldes *hovedideal*, hvis I har formen $I = Ra$ for et passende element $a \in I$.

DEFINITION. R kaldes en *hovedidealring*, hvis ethvert ideal er hovedideal.

DEFINITION. R kaldes et *hovedidealområde*, hvis R er et integritetsområde og ethvert ideal i R er et hovedideal. Vi skriver: R er PID ("principal ideal domain").

DEFINITION.Et ideal I i ringen R, $I \neq R$, kaldes et *primideal*, hvis det for vilkårlige to elementer a og b i R gælder at $ab \in I \Rightarrow a \in I$ eller $b \in I$.

Sætning 1. *(RNG 2.12 i Mat 2AL) Et ideal I i ringen R er et primideal hvis og kun hvis R/I er et integritetsområde.*

DEFINITION. Idealet I i R, $I \subsetneq R$, kaldes *maksimalt*, hvis I er maksimalt blandt de fra R forskellige idealer i R.

Sætning 2. *(RNG 2.12 i Mat 2AL) Et ideal I i ringen R er et maksimalt ideal hvis og kun hvis R/I er et legeme.*

EKSEMPEL: I ringen $R = \mathbb{Z}[X]$ er $I = \{f(x) \in \mathbb{Z}[X] \mid f(0) = 0\}$ et ikke-maksimalt primideal.

Vi minder endvidere om begrebet ”ring med entydig faktoropløsning”, betegnet UFD:

R kaldes UFD , hvis R er et integritetsområde, hvori ethvert ikke-invertibelt element på “væsentlig entydig” måde kan skrives som produkt af irreducible elementer.

I Mat 2AL er bevist: R PID $\Rightarrow$ R UFD og R PID $\Rightarrow$ ethvert primideal $\neq 0$ i R er maksimalt.

FAKTORISERINGER AF POLYNOMIER.

Vi betragter nu polynomiumsringen $R[X]$, hvor R enten er et legeme eller PID, (specielt ringen af sædvanlige hele tal).

Hertil er det følgende ofte hensigtsmæssigt: Lad φ være en homomorfi af R på R^*, (hvor R og R^* er kommutative ringe). Ved $\Phi(r_0 + r_1x + \cdots + r_nx^n) = \varphi(r_0) + \varphi(r_1)x + \cdots + \varphi(r_n)x^n$ defineres da en homomorfi Φ af $R[X]$ på $R^*[X]$. $\square$

Definition. Lad $f(x) = a_0 + \cdots + a_nx^n \in \mathbb{Z}[X]$. $f(x)$ kaldes *primitivt*, hvis største fælles divisor $(a_0, \ldots, a_n) = 1$.

Sætning 3. (Gauss). *Produktet af to primitive polynomier $f(x)$ og $g(x)$ er primitivt.*

Bevis. Indirekte. Antag $f(x) \cdot g(x)$ ikke var primitivt, dvs.: der fandtes et primtal p så p gik op i alle koefficienter til $f(x)g(x)$.

Ved homomorfien $\varphi : \mathbb{Z} \to \mathbb{Z}_p$[1] gælder $\Phi(f) \neq 0$ og $\Phi(g) \neq 0$, men $\Phi(f \cdot g) = 0$, hvilket strider mod at Φ er en homomorfi og $\mathbb{Z}_p[X]$ er et integritetsområde. $\square$

Lemma. *Lad $f(x)$ være primitivt polynomium i $\mathbb{Z}[X]$, og $q \in \mathbb{Q}$. Da gælder $qf(x) =$ primitivt polynomium $\Rightarrow q = \pm 1$.*

Bevis. Skriv $q = \frac{r}{s}$, $(r, s) = 1$. Lad $f(x) = a_0 + \cdots + a_nx^n$. $\frac{r}{s}(a_0 + \cdots + a_nx^n) = \frac{ra_0}{s} + \cdots + \frac{ra_n}{s}x^n \in \mathbb{Z}[X] \Rightarrow s|ra_i\ \forall i \Rightarrow s|a_i\ \forall i \Rightarrow s = \pm 1$ (da $f(x)$ primitivt). $\frac{r}{s}f(x) = r\left(\frac{a_0}{s} + \cdots + \frac{a_n}{s}x^n\right)$ primitivt $\Rightarrow r = \pm 1$. $\square$

Bemærkning. De invertible elementer i $\mathbb{Z}[X]$ er ± 1.

Sætning 4. *Lad $f(x)$ være et polynomium i $\mathbb{Z}[X]$. Da gælder*

i) *Grad $f(x) = 0$: $f(x)$ irreducibel $\Leftrightarrow f(x) = \pm p$, p primtal;*

ii) *Grad $f(x) > 0$: $f(x)$ irreducibel i $\mathbb{Z}[X] \Leftrightarrow f(x)$ primitivt og $f(x)$ irreducibel i $\mathbb{Q}[X]$.*

Bevis. i) klart.

ii) $\Leftarrow$ antag $f(x)$ havde ikke-triviel faktoropløsning $f(x) = g(x)h(x)$, $g(x)$ og $h(x) \in \mathbb{Z}[X]$. $g(x)$, $h(x)$ ej invertible i $\mathbb{Z}[X]$.

[1] $\mathbb{Z}_p$ betegner her restklasseringen modulo p, der er et legeme med p elementer

Da $f(x)$ primitiv må Grad $g(x) > 0$ og Grad $h(x) > 0$, dvs. $f(x)$ havde ikke-triviel spaltning indenfor $\mathbb{Q}[X]$. Modstrid!

$\Rightarrow$ klart at $f(x)$ må være primitiv. Antag $f(x)$ have ikke-triviel spaltning indenfor $\mathbb{Q}[X]$: $f(x) = g(x)h(x)$, $g(x)$ og $h(x)$ ej konstanter.

Vælg rationale tal q_1 og q_2 så $q_1 g(x)$ og $q_2 h(x)$ er primitive.

$$q_1 q_2 f(x) = [q_1 g(x)][q_2 h(x)] .$$

Ifølge Gauss' sætning er $q_1 q_2 f(x)$ primitiv. Da $f(x)$ er primitiv, er på grund af lemmaet $q_1 q_2 = \pm 1$, og herved

$$f(x) = (\pm\, q_1 g(x)) \cdot (q_2 h(x))$$

dvs.: $f(x)$ skulle havde ikke-triviel spaltning indenfor $\mathbb{Z}[X]$. Følgelig må $f(x)$ være irreducibel som element i $\mathbb{Q}[X]$. □

Sætning 5. $\mathbb{Z}[X]$ *er* UFD.

Bevis. 1) Ethvert $f(x) \in \mathbb{Z}[X]$ er produkt af irreducible. Det er klart.(Hvorfor?)

2) For beviset af entydigheden er det nok at godtgøre, at hvis $p(x)$ er irreducibel i $\mathbb{Z}[X]$, da vil
$p(x)|f(x) \cdot g(x)$, $f(x), g(x) \in \mathbb{Z}[X] \Rightarrow p(x)|f(x)$ eller $p(x)|g(x)$.

Der er to muligheder for $p(x)$:

i) $p(x) = \pm p$, p primtal.

ii) $p(x)$ positiv grad, $p(x)$ primitiv og irreducibel i $\mathbb{Q}[X]$.

ad i) $p|f(x)g(x)$; betragt

$$\begin{array}{lll} \text{homomorfien} & \varphi : \mathbb{Z} \to \mathbb{Z}_p & \text{og} \\ \text{homomorfien} & \Phi : \mathbb{Z}[X] \to \mathbb{Z}_p[X] & \end{array}$$

$0 = \Phi(f(x)g(x)) = \Phi(f(x)) \cdot \Phi(g(x))$.

Idet $\mathbb{Z}_p[X]$ er et integritetsområde, må $\Phi(f(x))$ eller $\Phi(g(x))$ være 0, dvs.: $p|f(x)$ eller $p|g(x)$.

ad ii) $p(x)|f(x)g(x)$ indenfor $\mathbb{Z}[X]$ medfører $p(x)|f(x)g(x)$ indenfor $\mathbb{Q}[X]$.

Da $p(x)$ er irreducibel i $\mathbb{Q}[X]$ og $\mathbb{Q}[X]$ er UFD, vil $p(x)|f(x)$ eller $p(x)|g(x)$ indenfor $\mathbb{Q}[X]$. Antag f.eks. $p(x)|f(x)$ indenfor $\mathbb{Q}[X]$. Vi har altså

$$f(x) = p(x)h(x)\,, \quad h(x) \in \mathbb{Q}[X]\,.$$

Vælg $q \in Q$ så $qh(x)$ er primitiv. Følgelig er

$$qf(x) = p(x) \cdot (qh(x))\,.$$

Som før (Gauss) må $qf(x)$ være primitiv. Skriv $q = \frac{r}{s}$, $(r,s) = 1$, $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. $\forall i : \frac{r}{s} a_i \in \mathbb{Z} \Rightarrow s|ra_i \Rightarrow s|a_i \Rightarrow r|\frac{a_i r}{s}$. Da $qf(x)$ primitiv må $r = \pm 1$ dvs.: $h(x) = (\pm s)qh(x) \in \mathbb{Z}[X]$, og dermed $p(x)|f(x)$ indenfor $\mathbb{Z}[X]$. □

Bemærkning. Ved ovenstående bevis er om $\mathbb{Z}$ i det væsentlige kun udnyttet at $\mathbb{Z}$ er UFD. Dvs.: alment gælder

Sætning 6. *R UFD $\Rightarrow R[X]$ UFD.*

Korollar til sætning 6. *K legeme $\Rightarrow K[X_1, \ldots, X_n]$ UFD.*

Sætning 7 (Schönemann-Eisensteins irreducibilitetskriterium). *Ethvert polynomium $f(x) \in \mathbb{Z}[X]$ af formen $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, hvor for et vist primtal p, $p|a_{n-1}, \ldots, p|a_1$, $p|a_0$, $p^2 \nmid a_0$, er irreducibelt i $\mathbb{Q}[X]$.*

Bevis. Ifølge Sætning 4 er det nok at vise, at $f(x)$ er irreducibelt i $\mathbb{Z}[X]$.

Antag $f(x) = g(x) \cdot h(x)$, hvor $g(x)$ og $h(x) \in \mathbb{Z}[X]$ og $g(x)$ og $h(x)$ af grad $< n$.

Vi kan antage, at $g(x)$ og $h(x)$ har højeste koefficienter $= 1$. Vi betragter homomorfien $\mathbb{Z} \xrightarrow[\varphi]{} \mathbb{Z}_p$ og den herved inducerede homomorfi $\mathbb{Z}[X] \xrightarrow[\Phi]{} \mathbb{Z}_p[X]$.

Vi får da:

$$\Phi(f(x)) = x^n = \Phi(g(x)) \cdot \Phi(h(x)) \Rightarrow \Phi(g(x)) = x^m\,;\ \Phi(h(x)) = x^{n-m}$$

for et passende m, $1 \le m \le n-1$. Dette medfører, at alle koefficienter i $g(x)$ og $h(x)$ på nær de øverste er delelige med p, specielt vil $p|g(0)$ og $p|h(0)$ og dermed $p^2|g(0)h(0) = f(0) = a_0$. Modstrid! $\square$

Eksempel. $\frac{x^n-1}{x-1}$ er irreducibel i $\mathbb{Q}[X] \Leftrightarrow n =$ primtal.

Bevis. $\Rightarrow$ antag n sammensat $n = n_1 n_2$, $1 < n_1 < n$. Da er

$$\frac{x^n - 1}{x-1} = \frac{x^{n_1 n_2} - 1}{x-1} = \frac{x^{n_1} - 1}{x-1}\left[(x^{n_1})^{n_2-1} + \cdots + x^{n_1} + 1\right] \quad \text{reducibelt.}$$

$\Leftarrow$ antag $n =$ primtal p; $f(x) = \dfrac{x^p - 1}{x-1}$, $f(x)$ irreducibelt $\Leftrightarrow f(x+1)$ irreducibelt,

$$f(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1}.$$

Da p er et primtal, vil $p\big|\binom{p}{j}$ for $1 \le j \le p-1$, og $p^2 \nmid \binom{p}{p-1} = p$, hvorfor ovenstående kriterium viser irreducibiliteten af $\frac{x^p-1}{x-1}$. $\square$

Bemærkning. Ovennævnte kriterium kan uden vanskelighed overføres til UFD.

Lad R være UFD og K brøklegemet for R. Lad π være irreducibelt element i R, og $f(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_0$ polynomium i $R[X]$ så $\pi | r_i$, $0 \le i \le n-1$, mens r_0 ikke er delelig med π^2, da er $f(x)$ irreducibelt i $K[X]$,(specielt irreducibelt i $R[X]$).

Eksempel. $f(x,y) = x^p + y^p - 1$ opfattet som polynomium i $K[x,y]$ hvor K er et givet legeme og p er et primtal, er irreducibelt $\Leftrightarrow$ karakteristikken af K er $\neq p$.

$\Rightarrow$ klart, da $\operatorname{Kar} K = p \Rightarrow f(x,y) = (x+y-1)^p$

$\Leftarrow$ betragt $f(x, y+1)$ som element i $(K[Y])[X]$.

Eksempel. $f(x) = \Pi_{i=1}^n (x - a_i) - 1$, hvor $a_1, \ldots, a_n$ er indbyrdes forskellige tal i $\mathbb{Z}$, er irreducibelt i $\mathbb{Q}[X]$. (Gælder tilsvarende for $\Pi_{i=1}^n (x - a_i) + 1$?)

SYMMETRISKE POLYNOMIER.

Lad K være et legeme. Et polynomium $f(X_1, ..., X_n) \in K[X_1, ..., X_n]$ kaldes symmetrisk, hvis det er invariant under enhver permutation af de variable $X_1, ...X_n$, dvs. hvis

$$f(X_1, ..., X_n) = f(X_{\sigma(1)}, ..., X_{\sigma(n)})$$

for enhver permutation $\sigma \in S_n$.

Eksempler. Polynomierne

$s_1 = X_1 + \cdots + X_n$ $\binom{n}{1}$ led

$s_2 = X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n$ $\binom{n}{2}$ led

$s_3 = X_1X_2X_3 + \cdots + X_{n-2}X_{n-1}X_n$ $\binom{n}{3}$ led

...

$s_n = X_1X_2 \cdots X_n$ $\binom{n}{n}$ led

er symmetriske.

Dette ses enten direkte eller ved at betragte polynomiet

$$(T - X_1)(T - X_2) \cdots (T - X_n) = T^n - s_1T^{n-1} + s_2T^{n-2} + \cdots + (-1)^n s_n$$

der er invariant under enhver permutation af $X_1, ..., X_n$, hvorfor alle koefficienterne også er invariante under enhver permutation af $X_1, ..., X_n$.

Disse polynomier $s_1, ..., s_n$ kaldes de *elementær-symmetriske polynomier* i $X_1, ..., X_n$.

Det er klart, at ethvert polynomium i de elementær-symmetriske polynomier er symmetrisk i $X_1, ..., X_n$.

Der gælder en art omvending, nemlig følgende vigtige

Hovedsætningen om symmetriske polynomier.

Ethvert symmetrisk polynomium $f(X_1, ..., X_n) \in K[X_1, ..., X_n]$, hvor K er et vilkårligt legeme, kan på én og kun én måde skrives som et polynomium (med koefficienter i K) i de elementær-symmetriske polynomier $s_1, ..., s_n$. Anderledes udtrykt: til ethvert symmetrisk polynomium $f(X_1, .., X_n) \in K[X_1, ..., X_n]$ findes ét og kun ét polynomium $g(Y_1, ..., Y_n) \in K[Y_1, ..., Y_n]$, så

$$f(X_1, ..., X_n) = g(X_1 + \cdots + X_n, X_1X_2 + \cdots, ..., X_1 \cdots X_n).$$

Inden beviset bringer vi nogle almene bemærkninger om polynomier i flere variable.

Ethvert polynomium i $X_1, ..., X_n$ kan skrives

$$f(X_1, ..., X_n) = \sum_{i_1, \ldots, i_n} a_{i_1, \ldots, i_n} X_1^{i_1} ... X_n^{i_n}$$

hvor $a_{i_1,\cdots,i_n}$ er elementer i K.

Ved *graden* af et led $a_{i_1,\ldots,i_n}X_1^{i_1}\ldots X_n^{i_n}$, $a_{i_1,\ldots,i_n} \neq 0$ forstås $i_1 + \cdots + i_n$.

Ved *graden* af et egentligt polynomium f forstås den højeste forekommende grad af et led ($\neq 0$) i f.

For polynomier i mere end én variabel er graden af leddene ikke nok til at bestemme en ordning af disse. Derfor indføres begrebet *signatur.* Ved signaturen af et led $a_{i_1,\ldots,i_n}X_1^{i_1}\cdots\ldots X_n^{i_n}$ forstås talsættet $\mathbf{i} = (i_1, \ldots, i_n)$.

Mængden af signaturer ordnes ved, at man først ordner efter graden og derefter indenfor led af samme grad ordner leksikografisk, dvs. for to forskellige signaturer $(i_1, \ldots, i_n)$ og $(j_1, \ldots, j_n)$ haves

$$(i_1, \ldots, i_n) \prec (j_1, \ldots, j_n)$$

hvis enten $i_1 + \cdots + i_n < j_1 + \cdots + j_n$ eller $i_1 + \cdots + i_n = j_1 + \cdots + j_n$ og $i_\nu < j_\nu$ for det mindste ν for hvilket $i_\nu \neq j_\nu$.

Lemma. *Produktet af to egentlige polynomier i $K[X_1, \ldots, X_n]$, hvor K er et legeme, er egentligt, og leddet af højeste signatur i produktet er produktet af leddene af højeste signatur i de to polynomier.*

Bevis. Øvelse.

Vi vender nu tilbage til beviset for hovedsætningen.

Først *eksistensen:*

Lad $f \in K[X_1, \ldots, X_n]$ være symmetrisk. Vi kan antage $f \neq 0$.

Lad $cX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ være leddet i f af højeste signatur.

Da f er symmetrisk, må $i_1 \geq i_2 \geq \ldots \geq i_n$. (Hvorfor?).

Betragtes specielt de elementær-symmetriske polynomier $s_1, s_2, \ldots, s_n$ har disse som led af højeste signatur henholdsvis X_1, X_1X_2,..., $X_1X_2\cdots X_n$.

På grund af lemmaet vil for vilkårlige hele ikke-negative tal $j_1, j_2, \ldots, j_n$ potensproduktet $s_1^{j_1}s_2^{j_2}\cdots s_n^{j_n}$ som polynomium i $X_1, X_2, \ldots, X_n$ have

$$X_1^{j_1}(X_1X_2)^{j_2}\cdots(X_1X_2\cdots X_n)^{j_n}$$

som led af højeste signatur. Denne signatur er

$$(j_1 + j_2 + \cdots + j_n, j_2 + \cdots + j_n, \ldots, j_n)$$

Vælger vi nu $j_1 = i_1 - i_2, j_2 = i_2 - i_3, \ldots, j_{n-1} = i_{n-1} - i_n$ og $j_n = i_n$, (der p.gr.af ovenstående bemærkning bliver ikke-negative tal), bliver denne signatur netop $(i_1, i_2, \ldots, i_n)$.

Differensen $f - cs_1^{j_1}s_2^{j_2}\ldots s_n^{j_n}$ vil derfor enten være nulpolynomiet eller et symmetrisk polynomium ($\neq 0$) hvis led af højeste signatur har signatur mindre end $(i_1, i_2, \ldots, i_n)$. Hvis differensen er nulpolynomiet er vi færdige ; ellers anvendes ovenstående procedure på $f - cs_1^{j_1} s_2^{j_2} ... s_n^{j_n}$ etc.. Man vil derved sluttelig nå til nulpolynomiet, da der kun findes endelig mange signaturer mindre end et givet.

Nu *entydighedsudsagnet*:

Det er åbenbart nok at vise, at for $g(Y_1, ..., Y_n) \in K[Y_1, ..., Y_n], g(Y_1, ..., Y_n) \neq 0$ vil $g(s_1, ..., s_n) = g(X_1 + X_2 + \cdots + X_n, X_1X_2 + \cdots, ..., X_1X_2 \cdots X_n)$ være $\neq 0$.

Lad $dY_1^{t_1} Y_2^{t_2} ... Y_n^{t_n}, d \neq 0$ være et led i g. Indsættes heri for $Y_1, Y_2, ..., Y_n$ de elementær-symmetriske polynomier $s_1, s_2, ... s_n$ fås ifl. det foregående et polynomium i $X_1, X_2, ..., X_n$ i hvilket leddet af højeste signatur er

$$dX_1^{t_1} (X_1X_2)^{t_2} \cdots (X_1X_2 \cdots X_n)^{t_n}.$$

Signaturen af dette led er

$$(t_1 + t_2 + \cdots + t_n, t_2 + \cdots + t_n, ..., t_n).$$

Betragtes nu først de led i g for hvilke $t_1 + t_2 + \cdots + t_n$ er størst, derefter blandt disse de led for hvilke $t_2 + \cdots + t_n$ er størst, o.s.v. , får vi i g udskilt et bestemt led $dY_1^{t_1} Y_2^{t_2} ... Y_n^{t_n}$ med den egenskab, at dette og kun dette ved indsætning af de elementær-symmetriske polynomier fører til et led med den nævnte signatur $(t_1 + t_2 + \cdots + t_n, t_2 + \cdots + t_n, ..., t_n)$.

Dette led kan ikke forkortes væk mod noget andet led, hvorfor $g(X_1 + X_2 + \cdots + X_n, X_1X_2 + \cdots ..., ..., X_1X_2 \cdots X_n)$ ikke er nulpolynomiet. $\square$

ALGEBRAISKE UDVIDELSER.

Lad K være et dellegeme af legemet L, $K \subseteq L$. For et element $\alpha \in L$ betegner vi med $K[\alpha]$ *den mindste delring af* L *indeholdende* K *og* α. $K[\alpha]$ består af alle elementer i L der kan skrives på formen $k_0 + k_1\alpha + \cdots + k_n\alpha^n$, $k_i \in K$, $n \in \mathbb{N}$.

Med $K(\alpha)$ *betegner vi det mindste dellegeme af* L *indeholdende* K *og* α. $K(\alpha)$ består af alle elementer i L der kan skrives på formen

$$\frac{k_0 + k_1\alpha + \cdots + k_n\alpha^n}{k_0' + k_1'\alpha + \cdots + k_n'\alpha^n},$$

k_i, $k_i' \in K$, $n \in \mathbb{N}$ og nævneren $\neq 0$.

$K(\alpha)$ er åbenbart brøklegemet for $K[\alpha]$.

For givet $\alpha \in L$, $L \supseteqq K$ betragtes homomorfien $\Phi : K[X] \to K[\alpha]$ defineret ved $\Phi(f(x)) = f(\alpha)$. Φ er øjensynligt surjektiv.

Nu to muligheder:

1) $\operatorname{Ker}\Phi = 0$, dvs. $K[\alpha] \simeq K[X]$, der ikke er et legeme. I dette tilfælde er $K(X) \simeq K(\alpha)$ og vi siger, at α er er *transcendent over* K.

2) $\operatorname{Ker}\Phi \neq 0$. Da $\operatorname{Ker}\Phi$ er et ideal i $K[X]$ og $K[X]$ er PID, er $\operatorname{Ker}\Phi =$ hovedidealet $K[X]p(X)$ frembragt af et polynomium $p(X) \neq 0$. Ifølge homomorfisætningen/isomorfisætningen for ringe (se 2AL, p.190) gælder

$$K[X]/\operatorname{Ker}\Phi \simeq K[\alpha].$$

$\operatorname{Ker}\Phi$ er derfor et primideal $\neq 0$. Da $K[X]$ er PID, er $\operatorname{Ker}\Phi$ (ifølge RNG 5.7) maksimalt dvs.: $K[\alpha]$ er et legeme og dermed også $K(\alpha) = K[\alpha]$.

I dette tilfælde 2) kaldes α *algebraisk over* K. At α er algebraisk over K betyder altså, at α er rod i et egentligt polynomium (dvs. et fra nulpolynomiet forskelligt polynomium) med koefficenter i K.

Nu er $\operatorname{Ker}\Phi = K[X]p(x)$, hvor $p(x)$ er entydigt bestemt pånær et invertibelt element i $K[X]$, dvs.: pånær en konstant i K. Det entydigt bestemte normerede (dvs.: øverste koefficient = 1) polynomium i $K[X]$ der frembringer $\operatorname{Ker}\Phi$ betegnes $\operatorname{Irr}(\alpha, K)$. Dette er irreducibelt i $K[X]$.

Lad $f(x) \in K[X]$ være et polynomium for hvilket $f(\alpha) = 0$. Da er $f(x) = \operatorname{Irr}(\alpha, K) \cdot g(x)$. Dette indebærer, at $\operatorname{Irr}(\alpha, K)$ *kan karakteriseres som det entydigt bestemte normerede irreducible polynomium i* $K[X]$ *der har* α *som rod.* $\operatorname{Irr}(\alpha, K)$ kan også karakteriseres som det entydigt bestemte normerede polynomium af laveste grad der har α som rod. $\operatorname{Irr}(\alpha, K)$ betegnes derfor ofte som α's minimalpolynomium m.h.t. K.

Som det fremgår af ovenstående, vil et polynomium i $K[X]$ have α som rod hvis og kun hvis det er deleligt med $\operatorname{Irr}(\alpha, K)$.

Ifølge divisionsalgoritmen kan ethvert polynomium $f(x) \in K[X]$ entydigt skrives

$$f(x) = \mathrm{Irr}(\alpha, K) \cdot g(x) + r(x)\,, \quad \operatorname{grad} r(x) < \operatorname{grad} \mathrm{Irr}(\alpha, K) = n$$

Indsætter vi i denne ligning α for x, fås, at $f(\alpha) = r(\alpha)$ dvs.: ethvert element i $K[\alpha]$ kan skrives på formen

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\,, \quad a_0, \ldots, a_{n-1} \in K\,.$$

Denne fremstilling er entydig. Thi antag et element β i $K[\alpha]$ havde fremstillingerne

$$\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

og

$$\beta = a'_0 + a'_1\alpha + \cdots + a'_{n-1}\alpha^{n-1},$$

hvor $a_0, a_1, ..., a'_0, a'_1, ...$ ligger i K, da ville α være rod i polynomiet $a_0 - a'_0 + (a_1 - a'_1)x + \cdots + (a_{n-1} - a'_{n-1})x^{n-1}$. Men α er ikke rod i noget egentligt polynomium i $K[X]$ af grad $< n$, hvorfor $a_0 - a'_0 = a_1 - a'_1 = \cdots = a_{n-1} - a'_{n-1} = 0$ og dermed $a_0 = a'_0, a_1 = a'_1, \cdots, a_{n-1} = a'_{n-1}$.

Ethvert element i $K[\alpha] = K(\alpha)$ kan altså på entydig måde skrives som en K-linearkombination af $1, \alpha, \ldots, \alpha^{n-1}$. Vi kan udtrykke dette ved at sige, at $K[\alpha] = K(\alpha)$ som vektorrum over K har $1, \alpha, \ldots, \alpha^{n-1}$ som basis, specielt har dette vektorrum dimension n. Denne dimension betegnes $[K(\alpha) : K]$ og bliver altså $\operatorname{grad}(\mathrm{Irr}(\alpha, K))$, der kaldes α's *grad m.h.t. K*.

Definition. En udvidelse $L \supseteq K$ (L og K legemer) kaldes *algebraisk*, hvis ethvert element i L er algebraisk over K. Man skriver kort: L/K algebraisk.

Inden vi går videre, bringer vi nogle almene bemærkninger, som vi i det følgende gang på gang vil få brug for.

Hvis L er et udvidelseslegeme af K, og $\alpha_1, \cdots, \alpha_s$ er elementer i L, betegner vi med $K(\alpha_1, \ldots, \alpha_s)$ det mindste dellegeme af L indeholdende K og $\alpha_1, \ldots, \alpha_s$. Det er da klart, at $K(\alpha_1, \ldots, \alpha_s) = K(\alpha_1)\ldots(\alpha_s)$.

Et udvidelseslegeme L af K kan betragtes som et vektorrum over K og har som sådant en dimension (dvs. antallet af elementer i en basis for L over K), der betegnes $[L : K]$. Hvis denne dimension er et endeligt tal n, vil hvilkesomhelst m elementer $\omega_1, \ldots, \omega_m$, $m > n$, være lineært afhængige over K, dvs. der findes elementer $k_1, \cdots, k_m \in K$, ikke alle 0, så $k_1\omega_1 + \cdots + k_m\omega_m = 0$.

Sætning 8. *Lad L være en legemsudvidelse af K, således at L betragtet som vektorrum over K har endelig dimension. Da er L/K algebraisk.*

Bevis. Antag $[L : K] = n$. For ethvert element α i L er elementerne $1, \alpha, \alpha^2, \ldots, \alpha^n$ lineært afhængige over K, dvs. der findes elementer $k_0, k_1, \ldots, k_n$ i K, ikke alle 0, så

$$k_0 + k_1\alpha + \cdots + k_n\alpha^n = 0\,.$$

Følgelig er α rod i det egentlige polynomium

$$k_0 + k_1 X + \cdots + k_n X^n \in K[X]\,.$$

Altså er ethvert element α i L algebraisk over K. $\square$

Sætning 9. (Transitivitetssætningen). *Antag* $K \subseteqq L \subseteqq M$*; da gælder* $[M:K] = [M:L]\,[L:K]$*, når* $[M:L]$ *og* $[L:K]$ *forudsættes endelige.*

Bevis. Hvis $\alpha_1, \alpha_2, \dots, \alpha_s$ er en K-basis for L og $\beta_1, \beta_2, \dots, \beta_t$ er en L-basis for M, da er $\alpha_i\beta_j$, $1 \leqq i \leqq s$, $1 \leqq j \leqq t$, en K-basis for M. Hertil skal vises to ting:

i) Elementerne $\alpha_i\beta_j$, $1 \leqq i \leqq s$, $1 \leqq j \leqq t$, er lineært uafhængige over K.

ii) Ethvert element i M kan skrives som en K -linearkombination af elementerne $\alpha_i\beta_j$, $1 \leqq i \leqq s$, $1 \leqq j \leqq t$.

ad i) Antag

$$\sum_{i,j} k_{ij}\alpha_i\beta_j = 0,$$

hvor k_{ij} tilhører K. Denne ligning omskrives til

$$\sum_j \Big(\sum_i k_{ij}\alpha_i\Big)\beta_j = 0$$

For hvert j er den inderste sum et element i L. Da $\beta_j, 1 \leqq j \leqq n$, er uafhængige over L, må

$$\sum_i k_{ij}\alpha_i = 0$$

for ethvert j, $1 \leqq j \leqq n$.

Da elementerne $\alpha_i, 1 \leqq i \leqq s$, er uafhængige over K, sluttes dernæst, at $k_{ij} = 0$ for alle $i, 1 \leqq i \leqq s$ og alle $j, 1 \leqq j \leqq t$.

ad ii) Lad ξ være et element i M. Da $\beta_j, 1 \leqq j \leqq t$ er en L-basis for M, kan ξ skrives

$$\xi = \sum_j \ell_j\beta_j,$$

hvor hvert ℓ_j ligger i L. Da $\alpha_i, 1 \leqq i \leqq s$, er en K-basis for L, kan hvert ℓ_j skrives som

$$\ell_j = \sum_i k_{ij}\alpha_i,$$

hvor hvert k_{ij} ligger i K. Heraf fås:

$$\xi = \sum_{i,j} k_{ij}\alpha_i\beta_j,$$

hvorved ii) er godtgjort. □

Bemærkning. Transitivitetssætningen er særdeles vigtig for udregninger i eksplicitte eksempler.

Sætning 10. *Antag $K \subsetneqq L$. Lad α og β være elementer i L, der er algebraiske over K, da er $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$ og α/β, $(\beta \neq 0)$, også algebraiske over K.*

Bevis. $K(\alpha) = K[\alpha]$ er et endeligdimensionalt vektorrum over K. Da β specielt er algebraisk over $K(\alpha) = K[\alpha]$, er $(K(\alpha))(\beta) = K(\alpha, \beta)$ endeligdimensionalt over $K(\alpha)$. På grund af transitivitetssætningen er $K(\alpha, \beta)$ endeligdimensionalt over K, hvorfor $K(\alpha, \beta)$ ifølge sætning 8 er algebraisk over K.

Idet $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$ og α/β, $(\beta \neq 0)$, ligger i $K(\alpha, \beta)$, vil disse elementer være algebraiske over K. □

Definition. Lad L være en legemsudvidelse af K. Delmængden af L bestående af de over K algebraiske elementer, der ifølge ovenstående sætning er et dellegeme af L, kaldes K's *algebraiske hylster* i L og betegnes $\overline{K}$.

Eksempel. Der findes uendeligdimensionale algebraiske legemsudvidelser. Lad $L = \mathbb{R}$ og $K = \mathbb{Q}$. For ethvert naturligt tal n er (ifølge Eisenstein's kriterium) $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$, hvorfor $\mathbb{Q}$'s algebraiske hylster i $L = \mathbb{R}$ har uendelig dimension over $\mathbb{Q}$.

Sætning 11. *Lad $K \subseteq L \subseteq M$ være legemer. Hvis L/K er algebraisk, er ethvert element $\xi \in M$, der er algebraisk over L også algebraisk over K.*

Bevis. ξ er rod i et egentligt polynomium i $L[X]$:

$$\xi^n + a_0\xi^{n-1} + \cdots + a_{n-1} = 0\,, \quad a_0, \ldots, a_{n-1} \in L\,.$$

Da a_0 er algebraisk over K, er $[K(a_0) : K]$ endelig.

Da a_1 er algebraisk over K, specielt over $K(a_0)$, er $[K(a_0, a_1) : K(a_0)]$ endelig.

Da a_2 er algebraisk over K, specielt over $K(a_0, a_1)$, er $[K(a_0, a_1, a_2) : K(a_0, a_1)]$ endelig.

etc.

Da a_{n-1} er algebraisk over K, specielt over $K(a_0, \ldots, a_{n-2})$, er $[K(a_0, \ldots, a_{n-1}) : K(a_0, \ldots, a_{n-2})]$ endelig.

Da ξ er algebraisk over $K(a_0, \ldots, a_{n-1})$, er $K(\xi, a_0, \ldots, a_{n-1}) : K(a_0, \ldots, a_{n-1})]$ endelig.

Ved successiv anvendelse af transitivitetssætningen fås, at $[K(\xi, a_0, \ldots, a_{n-1}) : K]$ er endelig, hvorfor sætning 8 indebærer, at ξ er algebraisk over K. □

Korollar 1. (Transitivitet for algebraiske udvidelser). *Lad $K \subseteq L \subseteq M$ være legemer. Da gælder: M/L algebraisk $\wedge$ L/K algebraisk $\Rightarrow$ M/K algebraisk.*

Korollar 2. *Lad $K \subseteq L$ være legemer.* $\overline{\overline{K}} = \overline{K}$.

Opgave. Lad α og β være komplekse tal, der er algebraiske over $\mathbb{Q}$ af grad p, henh.q. Vis, at $\alpha + \beta$ er algebraisk over $\mathbb{Q}$ af grad pq, såfremt p og q er forskellige primtal.

– – – – – – – – – – – – – – – –

ADJUNKTION AF ROD TIL ET POLYNOMIUM. SPALTNINGSLEGEMER.

Hidtil har vi betragtet foreliggende legemsudvidelser og set på polynomier forsvindende på visse elementer. Nu betragter vi omvendt et legeme K og et polynomium $p(x) \in K[X]$ og søger udvidelser af K hvori $p(x)$ har en rod.

Sætning 12. Eksistenssætning vedrørende adjunktion af en rod til et irreducibelt polynomium. *Lad K være et vilkårligt legeme og $p(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ et irreducibelt normeret polynomium i $K[X]$. Da findes et legeme L^* indeholdende et dellegeme K^* med følgende egenskaber:*

1) *der findes et element α^* i L^*, der er algebraisk over K^*, så $L^* = K^*(\alpha^*)$;*
2) *der findes en isomorfi φ af K på K^*, så $\mathrm{Irr}(\alpha^*, K^*) = \Phi(p(x))$, hvor Φ er den af φ inducerede isomorfi af $K[X]$ på $K^*[X]$.*

Bevis. Lad L^* være restklasseringen $K[X]/K[X]p(x)$, som er et legeme, da $p(x)$ er irreducibelt og $K[X]$ er PID. For et polynomium $f(x) \in K[X]$ betegner $\overline{f(x)}$ den tilsvarende restklasse i L^*. Da gælder:

$$\begin{aligned} L^* &= \{\overline{k_0 + k_1 x + \cdots + k_{n-1}x^{n-1}} \mid k_0, k_1, \ldots, k_{n-1} \in K\} \\ &= \{\overline{k}_0 + \overline{k}_1\overline{x} + \cdots + \overline{k}_{n-1}\overline{x}_{n-1} \mid k_0, k_1, \ldots, k_{n-1} \in K\}\,. \end{aligned}$$

Vi sætter $K^* = \{\overline{k} \mid k \in K\}$, der bliver et dellegeme af L^*. Den ved $\varphi(k) = \overline{k}$ definerede afbildning fra K på K^* bliver en isomorfi. Nu er $\overline{x}$ rod i polynomiet

$$\overline{a}_0 + \overline{a}_1 x + \cdots + \overline{a}_{n-1}x^{n-1} + x^n$$

der er irreducibelt i $K^*[X]$, dvs.

$$\mathrm{Irr}(\overline{x}, K^*) = \overline{a}_0 + \overline{a}_1 x + \cdots + \overline{a}_{n-1}x^{n-1} + x^n = \Phi(p(x)).$$

Sætningen er dermed vist, idet $\overline{x}$ kan bruges som α^*. □

Bemærkning til sætning 12. Ved at identificere K med K^* kan L^* opfattes som et udvidelseslegeme af K, hvori $p(x)$ har en rod. En udvidelse (i ordets mere umiddelbare forstand) med denne egenskab kan fås ved at betragte den disjunkte mængdeteoretiske forening af K og $L^* \setminus K^*$ og via ovenstående konstruktion "indplante" regneoperationerne addition og multiplikation; herved fås et legeme indholdende K som dellegeme og indeholdende en rod til $p(x)$.

Sætning 13. Entydighedssætning vedrørende adjunktion af en rod til et irreducibelt polynomium. *Antag vi har legemer L, K, L^*, K^*, så $L \supseteq K$, $L^* \supseteq K^*$, $L = K(\alpha)$, $L^* = K^*(\alpha^*)$, hvor α er algebraisk over K og α^* algebraisk over K^*. Antag endvidere, at der findes en isomorfi φ fra K på K^*, så $\Phi\,\mathrm{Irr}(\alpha, K) = \mathrm{Irr}(\alpha^*, K^*)$, hvor Φ betegner den af φ inducerede isomorfi af $K[X]$ på $K^*[X]$. Da findes en entydigt bestemt isomorfi $\widetilde{\varphi}$ fra L på L^* så*

1) $\widetilde{\varphi}_{\mathrm{Res},K} = \varphi$;
2) $\widetilde{\varphi}(\alpha) = \alpha^*$.

Bevis. Lad $p(x) = \mathrm{Irr}(\alpha, K)$ og $p^*(x) = \mathrm{Irr}(\alpha^*, K^*)$ og antag disse polynomier har grad n.

Vi viser først entydigheden af $\widetilde{\varphi}$. Åbenbart er

$$L = \{k_0 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1} \mid k_0, k_1, \ldots, k_{n-1} \in K\}\,.$$

Hvis der findes en isomorfi $\widetilde{\varphi}$ med egenskaberne 1) og 2), da må

$$\widetilde{\varphi}(k_0 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1}) = \varphi(k_0) + \varphi(k_1)\alpha^* + \cdots + \varphi(k_{n-1})(\alpha^*)^{n-1}.$$

Der er altså højest én mulighed for $\widetilde{\varphi}$.

Dernæst viser vi eksistensen af $\widetilde{\varphi}$.

Der findes en isomorfi

$$\varphi_1 : K[X]/(p(x)) \to L$$

defineret ved $\varphi_1(\overline{f(x)}) = f(\alpha)$, $f(x) \in K[X]$ og en isomorfi

$$\varphi_2 : K^*[X]/(p^*(x)) \to L^*$$

defineret ved $\varphi_2(\overline{g(x)}) = g(\alpha^*)$, $g(x) \in K^*[X]$. Endvidere inducerer isomorfien

$$K[X] \xrightarrow{\Phi} K^*[X]$$

en isomorfi

$$K[X]/(p(x)) \xrightarrow{\widetilde{\Phi}} K^*[X]/(p^*(x))$$

ved

$$\widetilde{\Phi}(\overline{f(x)} \;\text{ modulo }\; p(x)) = \overline{\Phi f(x)} \;\text{ modulo }\; p^*(x)\,,$$

dvs. vi har specielt

$$\widetilde{\Phi}((\overline{x}) \;\text{ modulo }\; p(x)) = \overline{x} \;\text{ modulo }\; p^*(x)\,.$$

Den sammensatte afbildning $\varphi_2 \circ \widetilde{\Phi} \circ \varphi_1^{-1}$ fra L på L^* kan bruges som $\widetilde{\varphi}$, idet

$$\varphi_2 \circ \widetilde{\Phi} \circ \varphi_1^{-1}(\alpha) = \alpha^*\,,$$

og $\varphi = \mathrm{Res}_K(\varphi_2 \circ \widetilde{\Phi} \circ \varphi_1^{-1})$. □

Ved successiv anvendelse af eksistenssætningen fås

Sætning 14. *Lad K være et legeme og $f(x)$ et vilkårligt polynomium i $K[X]$ af positiv grad. Da eksisterer et udvidelseslegeme M af K, hvori $f(x)$ spaltes til bunds i 1-ste gradsfaktorer.*

Bevis. Vi fører beviset ved induktion efter graden n af det foreskrevne polynomium. Hvis $n = 1$ er udsagnet klart: Man kan bruge K selv.

Lad nu n være > 1. Hvis $f(x)$ spaltes i 1-ste gradsfaktorer inden for $K[X]$, er der intet at bevise. Ellers maa $f(x)$ være deleligt med mindst et i $K[X]$ irreducibelt polynomium $p(x)$ af grad > 1. Ifølge sætning 12 findes et udvidelseslegeme L af K, hvori $p(x)$ og dermed også $f(x)$ har en rod α. Indenfor $L[X]$ kan $f(x)$ derfor skrives $f(x) = (x - \alpha)g(x)$, hvor $g(x)$ er et polynomium i $L[X]$ af grad $n - 1$. Ifølge induktionsantagelsen findes da et udvidelseslegeme M af L, hvori $g(x)$ spaltes til bunds i 1-ste gradsfaktorer. Men da er M jo også et udvidelseslegeme af K, og i dette spaltes $f(x)$ til bunds i 1-ste gradsfaktorer. □

Hvis $f(x)$ er et polynomium i $K[X]$ af positiv grad n, vil et udvidelseslegeme af K, hvori $f(x)$ spaltes til bunds i 1-ste gradsfaktorer, indeholde elementer $\alpha_1, \ldots, \alpha_n$, så $f(x)$ pånær en konstant i K er lig produktet $(x - \alpha_1) \cdots (x - \alpha_n)$. Det af disse elementer over K frembragte legeme er et udvidelseslegeme $M = K(\alpha_1, \ldots, \alpha_n)$ af K med følgende to egenskaber:
1) $f(x)$ spaltes til bunds i 1-ste gradsfaktorer inden for $M[X]$.
2) I intet ægte dellegeme af M indeholdende K spaltes $f(x)$ til bunds i 1-ste gradsfaktorer.

Definition. Lad K være et legeme og $f(x)$ et polynomium $K[X]$. Et udvidelseslegeme M af K kaldes et *spaltningslegeme* for $f(x)$ over K, hvis $f(x)$ spaltes til bunds i 1.gradsfaktorer indenfor $M[X]$, mens intet ægte dellegeme af M indeholdende K har denne egenskab.

Sætning 14 medfører eksistensen af et spaltningslegeme for ethvert polynomium (af positiv grad) over et vilkårligt legeme.

Bemærkning. I almindelighed vil der være en ægte delmængde $\{\alpha_1, \ldots, \alpha_t\}$, af rødderne til $f(x)$, så et spaltningslegeme bliver lig $K(\alpha_1, \ldots, \alpha_t)$. Til dannelse af et spaltningslegeme kan altså nogle af rødderne være overflødige i den forstand, at de "automatisk følger med" ved adjunktion af de øvrige rødder. Hvis graden n af $f(x)$ er > 1, er summen af rødderne $\alpha_1 + \alpha_2 + \cdots + \alpha_n = -$ (koefficienten til x^{n-1}) , og således et element i grundlegemet K. Derfor er $K(\alpha_1, \ldots, \alpha_{n-1}) = K(\alpha_1, \ldots, \alpha_n)$. Ofte kan endnu flere rødder være overflødige. Hvis f.eks. $f(x) = x^4 - 2$, fås det tilsvarende spaltningslegeme (over $\mathbb{Q}$) ved blot at adjungere rødderne $\sqrt[4]{2}$ og $\sqrt[4]{2} \cdot i$, hvor $i = \sqrt{-1}$.

Vi viser nu entydighed af spaltningslegemer:

Sætning 15. *Lad K være et legeme, $f(x) \in K[X]$, M et spaltningslegeme for $f(x)$ over K. Lad K^* være legeme isomorft med K og lad $\varphi : K \to K^*$ være en isomorfi.*

Lad $f^*(x) = \Phi(f(x))$, hvor Φ er den af φ inducerede isomorfi af $K[X]$ på $K^*[X]$, og lad M^* være et spaltningslegeme for $f^*(x)$ over K^*. Da kan φ fortsættes til en isomorfi af M på M^*.

Bevis. Ved induktion efter antallet af rødder i differensmængden: {spaltningslegemet $\setminus$ grundlegemet}.

Antag først, at dette antal er $= 0$. Da spaltes $f(x)$ i 1.gradsfaktorer indenfor K, dvs.: $M = K$ og $f^*(x)$ spaltes i 1.gradsfaktorer indenfor K^* dvs.: $M^* = K^*$.

Antag nu sætningen bevist, når antallet af rødder i differensmængden { spaltningslegemet $\setminus$ grundlegemet } er $< n$. Vi skal da vise, at sætningen gælder hvis dette antal er $= n$.

Antag nu, at antallet af rødder i $M \setminus K$ er n.

Lad $\alpha \in M \setminus K$, α rod i $f(x)$. Da er $p(x) = \mathrm{Irr}(\alpha, K)$ en divisor i $f(x)$ dvs.: $f(x) = p(x) \cdot h(x)$, hvor $\mathrm{grad}(p(x)) > 1$. Indenfor $K^*[X]$ fås tilsvarende opspaltning:

$$f^*(x) = p^*(x) \cdot h^*(x)\,, \quad p^*(x) \text{ irreducibel af grad} = \mathrm{grad}(p(x))\,.$$

Lad $\alpha^* \in M^*$ være rod i $p^*(x)$. Ifølge entydighedssætningen vedrørende adjunktion af rod i et irreducibelt polynomium findes (endda netop én) fortsættelse φ' af φ : $K(\alpha) \xrightarrow[\varphi']{} K^*(\alpha^*)$ så $\varphi'(\alpha) = \alpha^*$.

Indenfor $K(\alpha)[X]$ er $x - \alpha$ divisor i $f(x)$:

$$f(x) = (x - \alpha) \cdot \cdots \cdots \,.$$

Analogt gælder indenfor $K^*(\alpha^*)[X]$:

$$f^*(x) = (x - \alpha^*) \cdot \cdots \cdots \,.$$

Nu er:

$$M \;\text{ et spaltningslegeme for } f(x) \text{ over } K(\alpha) \text{ og}$$
$$M^* \;\text{ et spaltningslegeme for } f^*(x) \text{ over } K^*(\alpha^*)\,.$$

Antallet af rødder til $f(x)$ i $(M \setminus K(\alpha)) <$ antallet af rødder til $f(x)$ i $(M \setminus K)$. Ved den til φ' svarende isomorfi Φ' af $K(\alpha)[X]$ på $K^*(\alpha^*)[X]$ gælder åbenbart $\Phi'(f(x)) = f^*(x)$.

Vi kan nu anvende induktionsantagelsen på $f(x)$ over $K(\alpha)$ og får herved, at φ' kan fortsættes til isomorfi fra M på M^*. $\square$

Eksempel. Vi vil ved hjælp af eksistenssætningen for spaltningslegemer give et "algebraisk" bevis for *algebraens fundamentalsætning*. Det eneste vi benytter fra analysen, er sætningen om kontinuert variation af en kontinuert funktion, specielt at ethvert polynomium med reelle koefficienter af ulige grad, har mindst én reel rod.

Vi skal vise, at ethvert $f(x) \in \mathbb{C}[X]$, $\mathrm{grad}\, f(x) \geqq 1$ har mindst én rod i $\mathbb{C}$. Det er nok at vise, at ethvert $f(x) \in \mathbb{R}[X]$, $\mathrm{grad}\, f(x) \geqq 1$ har mindst én rod i $\mathbb{C}$. [Lad

$g(x) \in \mathbb{C}[X]$, da vil $g(x) \cdot \overline{g}(x)$ ligge i $\mathbb{R}[X]$, hvor $^-$ betegner kompleks konjugering. Hvis α er en (kompleks) rod i dette polynomium, vil $g(\alpha) \cdot \overline{g}(\alpha)$ være 0, hvorfor $g(\alpha) = 0$ eller $\overline{g}(\alpha) = 0$, dvs. $g(\alpha) = 0$ eller $g(\overline{\alpha}) = 0$.]

Hvis grad $f(x)$ er ulige, har $f(x)$ endda en rod i $\mathbb{R}$.

Alment skrives $\mathrm{grad}(f(x)) = 2^r \cdot u$, hvor $u =$ ulige tal.

Vi fører nu beviset ved induktion efter r.

For $r = 0$ er udsagnet klart ifølge ovenstående. Dernæst for $r > 0$:

$r-1 \to r$ $\;f(x) \in \mathbb{R}[X] \subset \mathbb{C}[X]$. Lad M være spaltningslegemet for $f(x)$ over $\mathbb{C}$, altså $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$, hvor $\alpha_1 \dots \alpha_n$ ligger i M. For vilkårligt $c \in \mathbb{R}$ dannes

$$g(x) = \prod_{1 \leqq i < j \leqq n} [x - (\alpha_i + \alpha_j + c\alpha_i\alpha_j)] \text{ , grad}\, g(x) = \binom{n}{2} = \frac{n(n-1)}{2}$$

$$g(x) = x^{\binom{n}{2}} + h_1(\alpha_1, \dots, \alpha_n)x^{\binom{n}{2}-1} + \cdots + h_{\binom{n}{2}}(\alpha_1, \dots, \alpha_n)$$

$h_1(\alpha_1 \dots \alpha_n), \dots,$ er symmetriske polynomier i $\alpha_1, \dots, \alpha_n$ med koefficienter i $\mathbb{R}$. Derfor kan (iflg. hovedsætningen om symmetriske polynomier) $h_1(\alpha_1, \dots, \alpha_n)$, etc . skrives som polynomier i de elementærsymmetriske $\alpha_1 + \cdots + \alpha_n$, $\sum_{i<j} \alpha_i\alpha_j$, etc. med reelle koefficienter, dvs.: $g(x) \in \mathbb{R}[X]$. Endvidere gælder:

$$\mathrm{grad}\, g(x) = \frac{n(n-1)}{2} = \frac{2^r u \cdot (2^r u - 1)}{2},$$

der er $2^{r-1}\cdot$(ulige tal), da $r > 0$.

Ifølge induktionsantagelsen har $g(x)$ en rod inden for $\mathbb{C}$. Dvs. for ethvert $c \in \mathbb{R}$ findes (i,j) så $\alpha_i + \alpha_j + c\alpha_i\alpha_j \in \mathbb{C}$. Da der er uendelig mange muligheder for c, findes to forskellige tal i $\mathbb{R}$, c_1 og c_2 hvortil svarer samme (i,j) dvs.: $\alpha_i + \alpha_j + c_1\alpha_i\alpha_j \in \mathbb{C}$ og $\alpha_i + \alpha_j + c_2\alpha_i\alpha_j \in \mathbb{C}$. Da $c_1 \neq c_2$ følger heraf at $\alpha_i + \alpha_j \in \mathbb{C}$ og $\alpha_i \cdot \alpha_j \in \mathbb{C}$, dvs.: α_i og $\alpha_j \in \mathbb{C}$ er rødder i et andengradspolynomium over $\mathbb{C}$ dvs.: $f(x)$ har (mindst én) rod i $\mathbb{C}$.

Beroligende Bemærkning. De udførte abstrakte legemsudvidelser angående rodadjunktioner kan i første omgang virke lidt fremmede. I langt de fleste tilfælde - bortset fra afsnittet om endelige legemer - kan man forestille sig, at det hele udspiller sig inden for de komplekse tals legeme. Da "algebraens fundamentalsætning" også er kendt fra analysen, bliver eksistenssætninger vedrørende rodadjunktioner og spaltningslegemer etc. trivielle, og når vi senere ofte behandler spaltningslegemer for polynomier over $\mathbb{Q}$ kan vi tænke på disse som dellegemer af de komplekse tals legeme.

STØRSTE FÆLLES DIVISOR FOR POLYNOMIER.

Lad K være et legeme, $f(x)$, $g(x) \in K[X]$. Da $K[X]$ er PID, har $f(x)$ og $g(x)$ en største fælles divisor, som vi – for at fremhæve at $f(x)$ og $g(x)$ betragtes som polynomier i $K[X]$ – betegner $(f(x), g(x))_K$. Her normeres $(f(x), g(x))_K$ så øverste koefficient er 1.

For en udvidelse $K \subseteq L$ af grundlegemet gælder

Sætning 16. *Hvis K er et dellegeme af legemet L, gælder, at $(f(x), g(x))_K = (f(x), g(x))_L$ for alle polynomier $f(x)$, $g(x)$ i $K[X]$.*

Bevis. Lad $d_K = (f(x), g(x))_K$, $d_L = (f(x), g(x))_L$ (ifølge *definition* begge normerede, så øverste koefficient $= 1$). $d_K|f(x)$ og $d_K|g(x)$ indenfor $K[X]$, specielt indenfor $L[X]$. Dvs.: $d_K|d_L$ (indenfor $L[X]$). Da d_K er frembringer for idealet i $K[X]$ frembragt af $f(x)$ og $g(x)$, må vi have: $d_K = f(x)a(x) + g(x)b(x)$ for visse $a(x), b(x)$ i $K[X]$. Indenfor $L[X]$ vil $d_L|f(x)$ og $d_L|g(x)$; følgelig har vi på grund af ovenstående ligning, at $d_L|d_K$ (indenfor $L[X]$). Altså er d_K og d_L normerede polynomier, for hvilke $d_K|d_L$ og $d_L|d_K$. Dette medfører $d_K = d_L$. $\square$

Korollar. *Lad K være et dellegeme af legemet L og lad $f(x)$ og $g(x)$ være polynomier i $K[X]$. Hvis $f(x)$ går op i $g(x)$ inden for $L[X]$, vil $f(x)$ også gå op i $g(x)$ indenfor $K[X]$.*

Sætning 16 udsiger - løst sagt - at største fælles divisor for polynomier ikke ændres ved grundlegemeudvidelse.

KARAKTERISTIK AF ET LEGEME.

Vi minder kort om begrebet karakteristik (kendt fra 2AL) for et legeme K.

For et helt tal $n \in \mathbb{Z}$ og et element $k \in K$ defineres (jfr. definition p.1.1.):

$$nk = \begin{cases} k + \cdots + k \quad (n \text{ led}) & \text{for} \quad n > 0 \\ 0 & \text{for} \quad n = 0 \\ (-n)(-k) & \text{for} \quad n < 0\,. \end{cases}$$

Da gælder regnereglerne:

$$(n_1 + n_2)k = n_1k + n_2k \text{ for alle } n_1, n_2 \in \mathbb{Z},\ k \in K$$

$$n(k_1 + k_2) = nk_1 + nk_2 \text{ for alle } n \in \mathbb{Z}, k_1, k_2 \in K$$

$$(n_1k_1)(n_2k_2) = (n_1n_2)(k_1k_2) \text{ for alle } n_1, n_2 \in \mathbb{Z}, k_1, k_2 \in K$$

Lad nu e betegne etelementet i legemet K. Da vil den ved $\phi(n) = ne$ bestemte afbildning ϕ fra $\mathbb{Z}$ ind i K (som en følge af ovenstående regneregler) være en ringhomomorfi.

Da billedet $\phi\mathbb{Z}$ er en delring af legemet K, vil nulreglen gælde i ϕZ, der således må være et integritetsområde. På grund af isomorfisætningen for ringe (se RNG 3.7 i 2AL) er $\mathbb{Z}/Ker(\phi) \simeq \phi\mathbb{Z}$, hvorfor $Ker(\phi)$ er et primideal i $\mathbb{Z}$.

Der er nu to muligheder:

1) $Ker(\phi) = 0$.

2) $Ker(\phi)$ er hovedidealet $\mathbb{Z}p$ frembragt af et primtal p.

ad 1). I dette tilfælde er ϕ injektiv, og der gælder:

$$nk = (ne)k = 0 \Leftrightarrow n = 0 \text{ eller } k = 0.$$

Vi siger her, at K har karakteristik 0.

Nu er $\phi\mathbb{Z} \simeq \mathbb{Z}$, og K må indeholde brøklegemet for $\phi\mathbb{Z}$. Dette brøklegeme er isomorft med de rationale tals legeme $\mathbb{Q}$.

ad 2). I dette tilfælde er ϕ ikke injektiv, og der gælder:

$nk = (ne)k = 0 \Leftrightarrow n \in \mathbb{Z}p$ eller $k = 0 \Leftrightarrow p \mid n$ eller $k = 0$.

Vi siger her, at K har karakteristik p.

Her er $\phi\mathbb{Z} \simeq \mathbb{Z}/\mathbb{Z}p$ og K indeholder således et dellegeme, kaldet *primlegemet*, med netop p elementer.

En vigtig regneregel gældende for legemer af karakteristik p er følgende:

Sætning 17. ("Freshman's dream"). *For vilkårlige element x og y i et legeme af karakteristik p er*

$$(x + y)^p = x^p + y^p$$

Bevis.

$$(x + y)^p = x^p + \binom{p}{1} x^{p-1}y + \cdots + \binom{p}{p-1} xy^{p-1} + y^p.$$

Da p går op i $\binom{p}{i}$ for $1 \leqq i \leqq p - 1$, fås derfor $(x + y)^p = x^p + y^p$. □

For et legeme K af karakteristik p bliver den ved $\sigma(x) = x^p$ definerede afbildning af K ind i sig selv en homomorfi, både m.h.t $+$ og $\cdot$, altså en ringhomomorfi af K ind i sig selv.

Bemærkning. Da $Ker(\sigma)$ åbenbart er 0, bliver σ en injektiv ringhomomorfi af K ind i sig selv. Hvis K specielt er et endeligt legeme bliver σ også surjektiv, dvs. en isomorfi (automorfi) af K på sig selv. σ kaldes *Frobeniusautomorfien* for det endelige legeme. Hvis K ikke er et endeligt legeme, behøver σ ikke at være surjektiv.

MULTIPLE RØDDER, FORMEL DIFFERENTIATION OG SEPARABILITET.

Vi minder kort om begreberne multiple rødder og multiplicitet. Hvis α er et element i legemet K og er rod i polynomiet $f(x) \in K[X]$, findes et entydigt bestemt naturligt tal t, så

$$f(x) = (x-\alpha)^t \cdot g(x)$$

hvor $g(x)$ er et polynomium i $K[X]$, der ikke har α som rod. Tallet t kaldes *multipliciteten* af α som rod i $f(x)$. Hvis $t = 1$ kaldes α en *simpel rod* til $f(x)$; hvis $t > 1$ kaldes α en *multipel rod* til $f(x)$.

For nærmere undersøgelser angående forekomsten af multiple rødder er det hensigtsmæssigt at indføre begrebet *formel differentiation.*

Lad K være et vilkårligt legeme. For $f(x) \in K[X]$

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

defineres den *formelt afledede* $f'(x)$ ved

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$$

Da gælder følgende umiddelbart verificerbare regneregler, der er analoge til de fra den klassiske analyse velkendte:

$$\begin{aligned} (f+g)' &= f' + g' \,, \quad (kf)' = kf' \quad \text{for alle } k \in K \\ (f \cdot g)' &= f \cdot g' + f' \cdot g \,. \end{aligned}$$

Mange af de fra den klassiske analyse kendte sætninger vedrørende differentiation gælder også for formelt afledede; men i visse tilfælde, specielt for legemer af primtalskarakteristik skal man være mere forsigtig.

Sætning 18. *Lad K være et legeme og*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

et polynomium i $K[X]$.

1) Hvis K har karakteristik 0, er $f'(x) = 0 \Leftrightarrow a_i = 0$ for alle $i > 0$.

2) Hvis K har karakteristik p, er $f'(x) = 0 \Leftrightarrow a_i = 0$ for alle i, der ikke er delelige med p.

Bevis.

ad 1)

$$f'(x) = \sum_{i>0} i a_i x^{i-1} = 0 \Leftrightarrow \; a_i = 0 \text{ for alle } i > 0,$$

hvor vi har udnyttet de i karakteristik 0 gældende regneregler.

ad 2)

$$f'(x) = \sum_{i>0} i a_i x^{i-1} = 0 \Leftrightarrow \ a_i = 0 \text{ for alle } i \text{ der ikke er delelige med } p,$$

hvor vi har udnyttet de i karakteristik p gældende regneregler.

□

Den efterfølgende sætning gælder for legemer af vilkårlig karakteristik.

Sætning 19. *Lad K være et vilkårligt legeme . Hvis polynomiet $f(x) \in K[X]$ har en multipel rod α i et udvidelseslegeme M af K, da er α også rod i $f'(x)$.*

Bevis. Vi kan skrive

$$f(x) = (x-\alpha)^{\nu} g(x), \text{ hvor } \nu > 1$$

og får

$$f'(x) = (x-\alpha)^{\nu} g'(x) + \nu (x-\alpha)^{\nu-1} g(x) = (x-\alpha)^{\nu-1}\{(x-\alpha)g'(x) + \nu g(x)\}$$

hvilket viser, at α er rod i $f'(x)$.

□

Sætning 20. *Et irreducibelt polynomium $f(x)$ over et legeme K af karakteristik 0, har ingen multiple rødder i noget udvidelseslegeme af K, specielt ikke i spaltningslegemet for $f(x)$ over K.*

Bevis. Lad α være en multipel rod til $f(x)$ i et udvidelseslegeme M af K. Som udregningen i beviset for den foregående sætning viser, vil $(x-\alpha)$ være en divisor i $f'(x)$ inden for $M[X]$. Den største fælles divisor $d_M = (f(x), f'(x))_M$ har derfor grad mindst 1. Nu ændres største fælles divisor ikke ved grundlegemeudvidelse, hvorfor $d_M = d_K = (f(x), f'(x))_K$. Da d_K således har grad ≥ 1 og $f(x)$ er irreducibelt i $K[X]$, må d_K (pånær en eventuel konstant i $K \setminus \{0\}$) være lig $f(x)$. Specielt må $f(x)$ gå op i $f'(x)$. Men dette er umuligt, da K har karakteristik 0 og $f'(x)$ derfor er et egentligt polynomium, hvis grad er mindre end graden af $f(x)$.

□

Sætning 21. *Lad K legeme være et legeme af karakteristik p. Et irreducibelt polynomium $f(x)$ i $K[X]$ har multiple rødder i spaltningslegemet over $K \Leftrightarrow f'(x) = 0$.*

Bevis. "$\Rightarrow$"

Hvis $f'(x)$ var et egentligt polynomium, kunne vi ganske som i beviset for sætning 20 slutte, at $f(x)$ ikke kan have multiple rødder i noget udvidelseslegeme af K.

"$\Leftarrow$" Hvis $f'(x) = 0$, må $f(x)$ ifølge sætning 18 have formen:

$$f(x) = a_0 + a_p x^p + a_2 x^{2p} + \cdots + a_{kp} x^{kp} .$$

Det er nok at vise, at $f(x)$ har multiple rødder i et passende "stort" legeme, hvori $f(x)$ spaltes til bunds i 1.gradsfaktorer.

Vi adjungerer nu til K elementer $b_0, b_1, \ldots, b_k$ så $b_0^p = a_0$, $b_1^p = a_p, \ldots, b_k^p = a_{kp}$. I $K(b_0, b_1, \ldots, b_k)$ gælder

$$f(x) = b_0^p + b_1^p x^p + \cdots + b_k^p x^{kp} = (b_0 + b_1 x + \cdots + b_k x^k)^p .$$

Lad L være spaltningslegemet for $g(x) = b_0 + b_1 x + \cdots + b_k x^k$ over $K(b_0, b_1, \ldots, b_k)$, så vi inden for L har $g(x) = b_k(x - \beta_1) \cdots (x - \beta_k)$ og dermed $f(x) = a_{kp}(x - \beta_1)^p \cdots (x - \beta_k)^p$ (indenfor $L[X]$).

Ovennævnte fremstilling for $f(x)$ må også gælde inden for spaltningslegemet for $f(x)$ over K. Vi ser at endda samtlige rødder til $f(x)$ er multiple.

$\square$

Definition. Et irreducibelt polynomium $f(x)$ i $K[X]$ kaldes *separabelt*, hvis $f(x)$ ikke har nogen multipel rod i spaltningslegemet over K (og dermed ikke nogen multipel rod i noget udvidelseslegeme af K). Et vilkårligt polynomium $f(x)$ i $K[X]$ kaldes separabelt, hvis hver af dets irreducible faktorer er separable i henhold til ovenstående.

Bemærkning. Lad $f(x)$ være irreducibel. Da gælder (iflg. Sætning 20 og 21): $f(x)$ separabel $\Leftrightarrow$ $f'(x) \neq 0$. Specielt er altså ethvert polynomium i $K[X]$ separabelt, såfremt legemet K har karakteristik 0.

Definition. Et legeme K kaldes *fuldkomment*, hvis alle polynomier i $K[X]$ er separable.

Specielt er ethvert legeme af karakteristik 0 fuldkomment.

Sætning 22. *Lad K være legeme af primtalskarakteristik p. Da gælder: K fuldkommen $\Leftrightarrow$ afbildningen $\sigma : \alpha \to \alpha^p$, der sender ethvert element i K over i sin p-te potens, er surjektiv.*

Bevis. $\Rightarrow$ Lad $\beta \in K$ og $f(x) = x^p - \beta$.

Lad γ være en rod til $f(x)$ i spaltningslegemet for $f(x)$ over K. Da gælder $x^p - \beta = (x - \gamma)^p$.

Nu er $\mathrm{Irr}(\gamma, K)$ ifølge forudsætningen irreducibelt og derfor uden multiple rødder i ovenstående spaltningslegeme. Da endvidere $\mathrm{Irr}(\gamma, K)$ er divisor i $x^p - \beta$, slutter vi, at $\mathrm{Irr}(\gamma, K)$ må være $x - \gamma$, hvorfor γ må ligge i K, dvs. $\beta = \gamma^p$.

$\Leftarrow$ Det er nok at vise, at ethvert polynomium $f(x) \in K[X]$, $\operatorname{grad} f(x) > 0$ er reducibelt, såfremt $f'(x) = 0$. Som tidligere bemærket medfører $f'(x) = 0$, at $f(x)$ har formen

$$f(x) = a_0 + a_1 x^p + \cdots + a_k x^{kp} .$$

Da afbildningen $\sigma : \alpha \to \alpha^p$ er surjektiv findes $b_0, \ldots, b_k \in K$ så $a_0 = b_0^p$, $a_1 = b_1^p, \ldots, a_k = b_k^p$, og derfor er

$$f(x) = (b_0 + b_1 + \cdots + b_k x^k)^p\,,$$

hvilket viser at $f(x)$ er reducibelt. $\square$

Bemærkning. Da afbildningen $\sigma : \alpha \to \alpha^p$ er injektiv for ethvert legeme af karakteristik p (jfr. tidligere bemærkning), får vi af ovenstående sætning, at ethvert endeligt legeme er fuldkomment.

Eksempel på et ikke-fuldkomment legeme. Lad $K = \mathbb{Z}_p(t)$ (dvs.: legemet af alle brudne rationale funktioner i én variabel over legemet $\mathbb{Z}_p$). Elementet t er ikke en p-te potens af et element i K, idet en p-te potens må have formen

$$\frac{a_0 + a_1 t^p + a_2 t^{2p} + \ldots}{b_0 + b_1 t^p + b_2 t^{2p} + \ldots}$$

$(a_i, b_i \in \mathbb{Z}_p)$.

Definition. Lad $L \supseteqq K$ være legemer. Et element $\alpha \in L$ kaldes *separabelt* over K, hvis α er algebraisk over K og $\mathrm{Irr}(\alpha, K)$ er et separabelt polynomium i $K[X]$. $L \supseteq K$ kaldes en *separabel* udvidelse, hvis alle elementer i L er separable over K.

ABEL-STEINITZ'S SÆTNING.

De fleste af de legemsudvidelser, som vi vil betragte, er "simple". Den præcise definition er følgende:

Definition. En algebraisk udvidelse L/K kaldes *simpel*, hvis der findes $\alpha \in L$ så $L = K(\alpha)$. Et sådant α kaldes et *primitivt element* for L/K.

Sætning 23 (Abel, Steinitz). *Lad L/K være en endelig (og dermed specielt algebraisk) udvidelse, der er separabel. Da er L/K simpel, dvs. der findes et primitivt element for udvidelsen L/K.*

Bevis. Hvis K er endelig, er L også endelig. Som vist i gruppeteorien (se fx. POL 3.13 i MAT 2AL noterne) er $L \setminus \{0\}$ en cyklisk gruppe. Hvis α er en frembringer for $L \setminus \{0\}$, er specielt $L = K(\alpha)$.

Vi kan derfor antage, at K er uendelig. I dette tilfælde fås Abel-Steinitz's sætning ved successiv anvendelse af: *Hvis $K \subset M$, $\alpha, \beta \in M$ α algebraisk over K, β separabelt over K, da findes et $\gamma \in M$ så $K(\alpha, \beta) = K(\gamma)$.*

Bevis. Lad $f(x) = \mathrm{Irr}(\alpha, K)$, $g(x) = \mathrm{Irr}(\beta, K)$. Vi arbejder nu inden for et udvidelseslegeme N af M, hvori $f(x)$ og $g(x)$ spaltes til bunds i 1.gradsfaktorer. Vi kan fx. lade N være spaltningslegemet for $f(x)\cdot g(x)$ over M. Indenfor N kan vi derfor skrive

$$\begin{aligned} f(x) &= (x-\alpha_1)\dots(x-\alpha_n)\,, &&\text{hvor vi kan antage } \alpha=\alpha_1 \\ g(x) &= (x-\beta_1)\dots(x-\beta_m)\,, &&\text{hvor vi kan antage } \beta=\beta_1\,. \end{aligned}$$

Da β er separabel, er $\beta_1,\dots,\beta_m$ indbyrdes forskellige. Idet K har uendelig mange elementer findes et $c\in K$ så

$$\gamma=\alpha+c\beta\neq\alpha_i+c\beta_j \qquad \begin{matrix} 1\leqq i\leqq n \\ 2\leqq j\leqq m \end{matrix} \quad \begin{pmatrix} c & \text{vælges} \neq & \frac{\alpha-\alpha_i}{\beta_j-\beta} \\ 1\leq i\leq n\,, & & 2\leq j\leq m \end{pmatrix}$$

Vi påstår $K(\gamma)=K(\alpha,\beta)$.

Det er klart, at $K(\gamma)\subseteqq K(\alpha,\beta)$.

For at vise den modsatte inklusion bemærker vi, at $f(\gamma-cx)$ har β som rod. På grund af valget af c er intet β_j, $2\leq j\leq m$, rod i $f(\gamma-cx)$. Vi kan derfor skrive:

$$f(\gamma-cx)=(x-\beta)^t\cdot h(x)\,,\ \text{ hvor } t \text{ er helt tal} \geq 1$$

og $h(x)$ er et polynomium der ikke har noget β_j, $1\leq j\leq m$, som rod.

Indenfor N har vi derfor

$$(f(\gamma-cx),g(x))_N=(x-\beta)\,.$$

Nu er $g(x)\in K[X]\subseteq K(\gamma)[X]$ og $f(\gamma-cx)\in K(\gamma)[X]$. Ifølge sætning 16 er $(f(\gamma-cx),g(x))_{K(\gamma)}=(f(\gamma-cx),g(x))_N=x-\beta$. Dette indebærer at $\beta\in K(\gamma)$.

Da $\alpha=\gamma-c\beta\in K(\gamma)$ fås, at $K(\alpha,\beta)\subseteq K(\gamma)$, der sammenholdt med den modsatte (trivielle) inklusion giver $K(\gamma)=K(\alpha,\beta)$. $\square$

Bemærkning. Separabilitetsforudsætningen i Abel-Steinitz's sætning er væsentlig. Lad $L=\mathbb{Z}_2(x,y)$ (dvs. legemet af brudne rationale funktioner i to variable x og y over legemet $\mathbb{Z}_2$) og $K=\mathbb{Z}_2(x^2,y^2)$ (dvs.: dellegemet af rationale funktioner i x^2 og y^2). Her er $[L:K]=4$, idet 1, x, y, xy er en basis for L betragtet som vektorrum over K. Men L/K er ikke simpel, idet $\alpha^2\in K$ for ethvert $\alpha\in L$, dvs. $[K(\alpha):K]\leqq 2$.

– – – – – – – – – – – – – – – – –

ENDELIGE LEGEMER.

Vi viser først en sætning om elementantallet for et endeligt legeme.

Sætning 24. *Antallet af elementer i et endeligt legeme K er en primtalspotens.*

Bevis. Da K er endelig, må karakteristikken af K være et primtal p. Legemet K må derfor indeholde legemet $\mathbb{Z}_p$ som dellegeme. Betragtet som vektorrum over $\mathbb{Z}_p$ må K have endelig dimension n, hvor n er et naturligt tal. Lad $\omega_1, \dots, \omega_n$ være en basis for K over $\mathbb{Z}_p$. Ethvert element i K kan da på entydig måde skrives på formen $a_1\omega_1 + \cdots + a_n\omega_n$, hvor $a_1, \dots, a_n$ gennemløber $\mathbb{Z}_p$. Legemet K må derfor have netop p^n elementer.

□

Vi viser nu en art omvending:

Sætning 25. *Til enhver primtalspotens p^n findes ét og pånær isomorfi kun ét legeme med p^n elementer.*

Bevis. 1) *Eksistens.* Lad M være spaltningslegemet for polynomiet $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$. Da $f'(x) = -1$, har $f(x)$ (ifl. Sætning 19) præcist p^n forskellige rødder indenfor M.

Ved direkte udregning ses, at $f(\alpha) = 0$ og $f(\beta) = 0 \Rightarrow f(\alpha \pm \beta) = 0$, $f(\alpha \cdot \beta) = 0$ og $f\left(\frac{\alpha}{\beta}\right) = 0$ $(\beta \neq 0)$, dvs. de p^n rødder til $f(x)$ udgør et dellegeme K af M. K er således et legeme med p^n elementer. I øvrigt ser man, at $K = M$; thi $f(x)$ spaltes til bunds i 1.gradsfaktorer indenfor K og da $f(x)$ har p^n forskellige rødder og $|K| = p^n$ kan $f(x)$ ikke spaltes i 1.gradsfaktorer indenfor et ægte dellegeme af K.

2) *Entydighed.* Lad K være et legeme med p^n elementer. K må have karakteristik p og primlegeme $\mathbb{Z}_p$. Elementerne i $K^* = K \setminus \{0\}$ udgør en multiplikativ gruppe af orden $p^n - 1$. Ifølge Lagranges sætning er derfor $\alpha^{p^n-1} = 1$ for alle $\alpha \in K$, $\alpha \neq 0$, og derfor er samtlige elementer i K rødder i polynomiet $x^{p^n} - x$. Dette har højst (endda eksakt) p^n rødder. Derfor er K netop mængden af rødder til $x^{p^n} - x$, og K således spaltningslegemet for $x^{p^n} - x$ over $\mathbb{Z}_p$. På grund af spaltningslegemets entydighed (Sætning 15) er K entydig bestemt pånær isomorfi. □

Definition. For en primtalspotens p^n kaldes det i henhold til ovennævnte Sætning pånær isomorfi entydigt bestemte legeme med p^n elementer "Galoisfeltet" og betegnes $\mathrm{GF}(p^n)$ eller $\mathbb{F}_{p^n}$. (For $n = 1$ findes således tre benævnelser for legemet med p elementer: $\mathbb{Z}_p$, $\mathrm{GF}(p)$ og $\mathbb{F}_p$!)

Sætning 26. *For et givet primtal p gælder $\mathrm{GF}(p^m) \subseteqq \mathrm{GF}(p^n) \Leftrightarrow m|n$. ("$\subseteqq$" skal læses: "isomorf med et dellegeme af").*

Bevis. "$\Rightarrow$" Da de multiplikative grupper af de fra 0 forskellige elementer i $\mathrm{GF}(p^m)$ (resp. $\mathrm{GF}(p^n)$) har orden $p^m - 1$ (resp. $p^n - 1$) ses, at $\mathrm{GF}(p^m) \subseteqq \mathrm{GF}(p^n) \Rightarrow p^m - 1 | p^n - 1$.

Skriv $n = mq + r, \quad 0 \leqq r < m$. Da er $p^n = (p^m)^q \cdot p^r \equiv p^r \pmod{p^m - 1}$ og dermed $p^n - 1 \equiv= p^r - 1 \mod (p^m - 1)$. Men $p^m - 1 | p^n - 1$, så $p^r - 1 \equiv 0 \mod (p^m - 1)$ dvs.: $(p^m - 1) | p^r - 1)$ hvilket kun er muligt, dersom $r = 0$ dvs.: $m|n$.

"$\Leftarrow$" $m|n \Rightarrow p^m - 1|p^n - 1 \Rightarrow (x^{p^m-1} - 1) \mid (x^{p^n-1} - 1) \Rightarrow (x^{p^m} - x) \mid (x^{p^n} - x) \Rightarrow$ spaltningslegemet (over $\mathbb{Z}_p$) for $(x^{p^n} - x) \supseteqq$ spaltningslegemet (over $\mathbb{Z}_p$) for $(x^{p^m} - x)$. Dvs.: $\mathrm{GF}(p^n) \supseteqq \mathrm{GF}(p^m)$. $\square$

— — — — — — — — — — — — — — — — —

Vi giver nu en helt konkret talteoretisk anvendelse af ovenstående, idet vi udleder en explicit formel for antallet $\pi(n)$ af normerede irreducible n'te gradspolynomier over $\mathbb{Z}_p$.

Lad $x^{p^n} - x = \Pi\, p(x)$, hvor $p(x)$ gennemløber de (over $\mathbb{Z}_p$) normerede irreducible faktorer i $x^{p^n} - x$. $\mathrm{GF}(p^n)$ = spaltningslegemet for $x^{p^n} - x$. Hvis $\alpha \in \mathrm{GF}(p^n)$, $p(\alpha) = 0$ er $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p]$ = graden d af $p(x)$, dvs.: $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = d$ dvs.: $|\mathbb{Z}_p(\alpha)| = p^d \Rightarrow d|n$.

Omvendt vil ethvert irreducibelt polynomium $q(x) \in \mathbb{Z}_p[X]$ af grad d, hvor $d|n$ være en divisor i $x^{p^n} - x$. Lad $L = \mathbb{Z}_p(\alpha)$, hvor α rod i $q(x)$, (eller $q(x) = \mathrm{Irr}(\alpha, \mathbb{Z}_p)$). Da er $[L; \mathbb{Z}_p] = d \Rightarrow |L| = p^d$. Men da er α rod i $x^{p^d} - x$ og dermed vil $q(x) = \mathrm{Irr}(\alpha, \mathbb{Z}_p)|x^{p^d} - x|x^{p^n} - x$.

Da $x^{p^n} - x$ ikke har multiple faktorer, bliver de irreducible faktorer $p(x)$ i fremstillingen $x^{p^n} - x = \Pi p(x)$ netop mængden af (normerede) irreducible polynomier, hvis grad er en divisor i n. Herved fås formlen $p^n = \sum_{d|n} d \cdot \pi(d)$.

For herved at finde $\pi(d)$ får vi brug for den (fra talteorien kendte) *Möbius-funktion* $\mu(n)$, defineret på $\mathbb{N}$ ved

$$\mu(n) = \begin{cases} 1 & \text{for} \quad n = 1, \\ 0 & \text{hvis } n \text{ er delelig med et kvadrat} > 1, \\ (-1)^r & \text{hvis } n = p_1 \cdots p_r, \text{ hvor } p_1, \dots, p_r \text{ er indbyrdes forskellige primtal.} \end{cases}$$

Sætning 27.

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \textit{for } n = 1 \\ 0 & \textit{for } n > 1. \end{cases}$$

Bevis. For $n = 1$ er sætningen klar. For $n > 1$, lad $n = p_1^{a_1} \dots p_r^{a_r}$ $p_i \neq p_j$ for $i \neq j$; da bliver

$$\sum_{d|n} \mu(d) = \sum_{\nu=0}^{r} (-1)^\nu \binom{r}{\nu} = (1-1)^r = 0\,.$$

$\square$

Ved Sætning 27 fås:

$$\sum_{d|n} p^{\frac{n}{d}} \mu(d) = \sum_{d|n} \mu(d) \cdot \left\{ \sum_{\delta | \frac{n}{d}} \delta \pi(\delta) \right\} =$$

$$\sum_{\substack{d,\delta \\ d\cdot\delta|n}} \delta\pi(\delta)\mu(d) = \sum_{\delta|n} \delta\pi(\delta) \cdot \left\{ \sum_{d|\frac{n}{\delta}} \mu(d) \right\} =$$

$$n \cdot \pi(n)\,.$$

Dvs. vi finder følgende explicitte udtryk for $\pi(n)$:

$$\pi(n) = \frac{1}{n} \cdot \sum_{d|n} p^{\frac{n}{d}} \mu(d)\,.$$

DISKRIMIMANT FOR ET POLYNOMIUM.

Vi indfører nu en klassisk invariant, der har stor betydning ikke mindst for eksplicitte (numeriske) spørgsmål angående rødderne i et polynomium.

Hertil betragter vi først følgende polynomium i n variable $x_1, \cdots, x_n$:

$$\Delta(x_1, x_2, \ldots, x_n) = \prod_{n \geq i > j \geq 1} (x_i - x_j) = \begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \cdots & & & & \\ 1 & x_n & x_n^2 & & x_n^{n-1} \end{vmatrix}$$

der spiller en vigtig rolle ved indførelse af diskriminant. Den eksplicitte udregning af ovenstående determinant (kaldet *Vandermondes determinant*) er gennemført i Appendiks bagest i disse noter.

Åbenbart gælder for en permutation $\sigma \in S_n$ at

$$\Delta(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = \begin{cases} \Delta(x_1, x_2, \ldots, x_n) & \text{når } \sigma \text{ er lige} \\ -\Delta(x_1, x_2, \ldots, x_n) & \text{når } \sigma \text{ er ulige} \end{cases}$$

Specielt er $d(x_1, x_2, \ldots, x_n) = [\Delta(x_1, x_2, \ldots, x_n)]^2$ et symmetrisk polynomium.

Lad nu K være et vilkårligt legeme og $f(T) = T^n + b_1 T^{n-1} + \cdots + b_n$ et *normeret* polynomium i $K[T]$. Hvis $\beta_1, \beta_2, \ldots, \beta_n$ er rødderne til $f(T)$ i spaltningslegemet for $f(T)$ over K defineres *diskriminanten* $\operatorname{disk}(f)$ for f som

$$d(\beta_1, \beta_2, \ldots, \beta_n) = \prod_{n \geq i > j \geq 1} (\beta_i - \beta_j)^2\,.$$

Da $d(x_1, x_2, \ldots, x_n)$ er symmetrisk, kan $d(x_1, x_2, \ldots, x_n)$ iflg. hovedsætningen om symmetriske polynomier skrives som et polynomium (med koefficienter i K) i de elementærsymmetriske polynomier af $x_1, x_2, \ldots, x_n$. Ved indsætning af β_1 for x_1, β_2 for x_2, osv. ses, at $d(\beta_1, \beta_2, \ldots, \beta_n)$ bliver et polynomium (med koefficienter fra K) i $b_1, b_2, \ldots, b_n$, idet de elementærsymmetriske polynomier af $x_1, x_2, \ldots, x_n$ ved indsætning af β_1 for x_1, β_2 for x_2, osv. på nær fortegnene netop giver b_1, b_2 osv.

Specielt ses, at diskriminanten $\operatorname{disk}(f)$ for et polynomium f med koefficienter i legemet K er et element i K. Af definitionen ses umiddelbart, at f har lutter simple rødder hvis og kun hvis $\operatorname{disk}(f) \neq 0$.

Vi giver her en simpel sætning, der ofte kan være til nytte.

Sætning 28. *Lad K være et legeme og M spaltningslegemet over K for et normeret n-te gradspolynomium $f(x) \in K[X]$. Da vil $\sqrt{\operatorname{disk}(f)}$ være et element i M.*

Bevis. Lad $\beta_1, \ldots, \beta_n$ være rødderne til $f(x)$. Da vil $\Delta(\beta_1, \ldots, \beta_n)$ åbenbart være et element i M. Da $\operatorname{disk}(f) = [\Delta(\beta_1, \ldots, \beta_n)]^2$, vil $\sqrt{\operatorname{disk}(f)}$ tilhøre M. □

Lad os udregne diskriminanten for polynomier af anden og tredie grad.

Det ses let, at $\operatorname{disk}(T^2 + a_1 T + a_2) = a_1^2 - 4a_2$.

For trediegradspolynomier betragter vi polynomiet $T^3 + pT + q$. Hvis rødderne er β_1, β_2 og β_3, gælder

$$\begin{aligned} &\beta_1 + \beta_2 + \beta_3 = 0 \\ &\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 = p \\ &\beta_1\beta_2\beta_3 = -q\ . \end{aligned}$$

For potenssummerne

$$P_t = \beta_1^t + \beta_2^t + \beta_3^t$$

fås da

$$\begin{aligned} P_1 &= 0 \\ P_2 &= -2p \end{aligned}$$

og idet

$$\sum_{i=1}^{3} \left(\beta_i^3 + p\beta_i + q\right) = 0$$

og

$$\sum_{i=1}^{3} (\beta_i^4 + p\beta_i^2 + q\beta_i) = 0$$

udledes $P_3 = -3q$ og $P_4 = 2p^2$.

Nu er

$$\operatorname{disk}(T^3+pT+q) = [(\beta_2-\beta_1)(\beta_3-\beta_2)(\beta_3-\beta_1)]^2 =$$

$$\begin{vmatrix} 1 & \beta_1 & \beta_1^2 \\ 1 & \beta_2 & \beta_2^2 \\ 1 & \beta_3 & \beta_3^2 \end{vmatrix}^2 = \begin{vmatrix} 3 & P_1 & P_2 \\ P_1 & P_2 & P_3 \\ P_2 & P_3 & P_4 \end{vmatrix} = \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{vmatrix}$$

$$= -27q^2 - 4p^3 \,.$$

For et trediegradspolynomium med reelle koefficienter kan antallet af reelle rødder aflæses af diskriminanten, idet

Sætning 29. *Lad $f(x)$ være et normeret trediegradspolynomium med reelle koefficienter. Da gælder*

$\operatorname{disk}(f) > 0 \Leftrightarrow f$ *har tre forskellige reelle rødder;*
$\operatorname{disk}(f) = 0 \Leftrightarrow f$ *har en multipel rod;*
$\operatorname{disk}(f) < 0 \Leftrightarrow f$ *har netop én reel rod.*

Bevis. Øvelse.

Mere alment gælder følgende

Sætning 30. *Lad $f(x)$ være et normeret n-te gradspolynomium med reelle koefficienter.*

i) disk$(f) = 0$ netop når $f(x)$ har multiple rødder.

Antag $f(x)$ har lutter simple rødder. Lad r_1 være antallet af reelle rødder og r_2 antallet af par af komplekst konjugerede rødder (dvs. $r_1 + 2r_2 = n$).

ii) disk(f) er positiv netop når r_2 er lige.

iii) disk(f) er negativ netop når r_2 er ulige.

Bevis. Udsagnet i) er klart.

Antag nu $f(x)$ har n simple rødder $\beta_1, \dots, \beta_n$. Da er diskriminanten $\operatorname{disk}(f) = [\Delta(\beta_1, \dots, \beta_n)]^2$.

Nu er

$$\Delta(\beta_1,\dots,\beta_n) = \begin{vmatrix} 1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{n-1} \\ 1 & \beta_2 & \beta_2^2 & \cdots & \beta_2^{n-1} \\ \cdots & & & & \\ 1 & \beta_n & \beta_n^2 & & \beta_n^{n-1} \end{vmatrix}$$

Ved anvendelse af kompleks konjugering på $\Delta(\beta_1, \dots, \beta_n)$ vil der i ovenstående determinant ske en ombytning af r_2 rækker.

Hvis r_2 er lige, vil $\Delta(\beta_1, \dots, \beta_n)$ derfor være invariant under kompleks konjugering og således være et reelt tal. Kvadratet $\operatorname{disk}(f) = [\Delta(\beta_1, \dots, \beta_n)]^2$ må da være et positivt tal.

Hvis r_2 er ulige, vil $\Delta(\beta_1, \dots, \beta_n)$ skifte fortegn ved kompleks konjugering og således være af formen $\sqrt{-1}\cdot$(et reelt tal). Kvadratet $\operatorname{disk}(f) = [\Delta(\beta_1, \dots, \beta_n)]^2$ må da være et negativt tal. $\square$

Til eksplicit beregning af diskriminanter er følgende ofte nyttig

Sætning 31. *Lad $f(T) = T^n + b_1 T^{n-1} + \cdots + b_n$ være et polynomium med rødderne $\beta_1, \ldots, \beta_n$. Da er* $\operatorname{disk}(f) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\beta_i)$.

Bevis. Ud fra regnereglerne for formel differentiation fås for $f(T) = \prod_{i=1}^{n} (T - \beta_i)$, at

$$
\begin{aligned}
&f'(T) = (T-\beta_2)\cdots(T-\beta_n) + (T-\beta_1)(T-\beta_3)\cdots(T-\beta_n) \\
&+ \cdots + (T-\beta_1)(T-\beta_2)\cdots(T-\beta_{n-1}) \; .
\end{aligned}
$$

Heraf fås, at $\prod_{i=1}^{n} f'(\beta_i)$ bliver produktet

$$
\begin{gathered}
(\beta_1-\beta_2)\cdot(\beta_1-\beta_3)\cdots(\beta_1-\beta_n) \\
(\beta_2-\beta_1)\cdot(\beta_2-\beta_3)\cdots(\beta_2-\beta_n) \\
\cdots \\
(\beta_n-\beta_1)\cdot(\beta_n-\beta_2)\cdots(\beta_n-\beta_{n-1})
\end{gathered}
$$

$$
= (-1)^{\frac{n(n-1)}{2}} d(\beta_1, \ldots, \beta_n) = (-1)^{\frac{n(n-1)}{2}} \operatorname{disk}(f) \; .
$$

□

Sætning 32. *Diskriminanten for polynomiet $f(T) = T^n - 1$ er $n^n(-1)^{\frac{(n-1)(n-2)}{2}}$.*

Bevis. Åbenbart er $f'(T) = nT^{n-1}$. For rødderne $\beta_1, \ldots, \beta_n$ gælder, at $\beta_1 \cdots \beta_n = (-1)^{n-1}$, hvorfor vi ved anvendelse af sætning 31 får

$$
\begin{aligned}
&\operatorname{disk}(f) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\beta_i) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (n\beta_i^{n-1}) \\
&= (-1)^{\frac{n(n-1)}{2}} n^n \left(\prod_{i=1}^{n} \beta_i \right)^{n-1} = n^n (-1)^{\frac{n(n-1)}{2}} (-1)^{(n-1)^2} \\
&= n^n (-1)^{\frac{(n-1)(n-2)}{2}} .
\end{aligned}
$$

□

Øvelse. Vis, at diskriminanten for polynomiet $T^4 + aT^2 + b$ er $16(a^2 - 4b)^2 b$.

Kapitel III. Galoisteori

The essence of Galois Theory: The systematically developed connection between two seemingly unrelated subjects, the theory of fields and the theory of groups.

More specifically, but in the same line, is the idea of studying a mathematical object by its group of automorphisms, an idea emphasized in Klein's Erlanger Program, which has been accepted as a powerful tool in a great variety of mathematical disciplines.

The Galois Theory of field extensions combines the esthetic appeal of a theory of nearly perfect beauty with the technical development and difficulty that reveal the depth of the theory and that make possible its great usefulness primarily in algebraic number theory and related parts of algebraic geometry.

(Fra Roger Lyndon i:
Encyclopedia of Mathematics and Its Applications)

Indledende begreber og sætninger.

En *automorfi* for et legeme L er en bijektiv afbildning af L på sig selv, der også er en isomorfi, dvs. en bijektiv afbildning σ, der fører sum over i sum og produkt over i produkt: $\sigma(x+y) = \sigma(x) + \sigma(y)$ og $\sigma(xy) = \sigma(x)\sigma(y)$ for alle $x, y \in L$. Mængden $\mathrm{Aut}(L)$ af alle automorfier for L udgør en gruppe med sammensætning som komposition. Denne gruppes neutrale element er identitetsafbildningen, der sender ethvert element i L over i sig selv. Denne afbildning betegnes 1_L eller e.

Hvis $\mathcal{S}$ er en vilkårlig delmængde af $\mathrm{Aut}(L)$ defineres fixpunktsmængden $\mathcal{F}(\mathcal{S})$ som $\mathcal{F}(\mathcal{S}) = \{x \in L \mid \sigma x = x \ \forall \sigma \in \mathcal{S}\}$.

$\mathcal{F}(\mathcal{S})$ ses let at være et dellegeme af L og kaldes fixpunktslegemet for $\mathcal{S}$.

Eksempel. Lad $L = \mathbb{C}$ og $\sigma =$ overgang til kompleks-konjugeret, da er $\mathcal{F}(\{\sigma\}) = \mathbb{R}$.

Lad K være et dellegeme af L. Vi definerer

$$\mathrm{Gr}(L/K) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma_{\mathrm{Res},K} = 1_K\} = \{\sigma \in \mathrm{Aut}(L) \mid \sigma k = k \ \forall k \in K\}.$$

$\mathrm{Gr}(L/K)$ ses let at være en undergruppe i $\mathrm{Aut}(L)$. Den kaldes for den *relative automorfigruppe* for L over K.

Af definitionen følger umiddelbart:

1) $\mathcal{F}(\mathrm{Gr}(L/K)) \supseteqq K$
2) $\mathrm{Gr}(L/\mathcal{F}(\mathcal{S})) \supseteqq \mathcal{S}$

I almindelighed gælder ikke $=$ i 1) og 2).

Bemærkning. Hvis der gælder $=$ i 2) da må $\mathcal{S}$ være undergruppe i $\mathrm{Aut}(L)$.

Til bestemmelse af den relative automorfigruppe er følgende ofte meget nyttig:

Praktisk Lemma. *Lad L/K være en vilkårlig legemsudvidelse og $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ et (ikke nødvendigvis irreducibelt) polynomium i $K[X]$. Hvis α er et element i L og er rod i $f(x)$, da er også $\sigma(\alpha)$ rod i $f(x)$ for enhver automorfi $\sigma \in \mathrm{Gr}(L/K)$.*

Bevis. Da α er rod i $f(x)$, er

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$$

Ved at anvende automorfien σ på hver side i ovenstående ligning fås

$$(\sigma(\alpha))^n + a_1(\sigma(\alpha))^{n-1} + \cdots + a_n = 0 \quad (\star)$$

hvor vi har udnyttet, at $a_1, \cdots a_n$ er fixe under automorfien σ. Men ligningen $(\star)$ betyder netop, at $\sigma(\alpha)$ er rod i $f(x)$. $\square$

Eksempel. $L = \mathbb{C}$, $K = \mathbb{R}$, $\mathrm{Gr}(L/K) = \{1_L, \text{ kompleks-konjugering}\}$. Her er $\mathcal{F}(\mathrm{Gr}(L/K)) = K$.(Benyt Praktisk Lemma.)

Eksempel. $L = \mathbb{Q}(\sqrt{2})$, $K = \mathbb{Q}$, $\mathrm{Gr}(L/K) = \{1_L, \ \sigma\}$ hvor $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$; $a, b \in \mathbb{Q}$. Her er $\mathcal{F}(\mathrm{Gr}(L/K)) = K$.(Benyt Praktisk Lemma.)

Eksempel. $L = \mathbb{Q}(\sqrt[3]{2})$, $K = \mathbb{Q}$, $\mathrm{Gr}(L/K) = 1_L$. Her er $\mathcal{F}(\mathrm{Gr}(L/K)) = L \supsetneqq K$.(Benyt Praktisk Lemma.)

Eksempel. $L = \mathbb{R}$, $K = \mathbb{Q}$. Her er $\mathrm{Gr}(L/K) = 1_L$ dvs.: $\mathcal{F}(\mathrm{Gr}(L/K)) = L$. (Beviset er ikke trivielt.)

Eksempel. $L = \mathbb{C}$, $K = \mathbb{Q}$, $\mathrm{Gr}(L/K) = \mathrm{Aut}(\mathbb{C})$ har kardinalitet $2^{2^{\aleph_0}}$ og $\mathcal{F}(\mathrm{Gr}(L/K)) = K$ (Beviset er ikke trivielt.)

Ovenstående eksempler refererer sig til 1).

Eksempel. Vi viser det kan hænde at 2) har $\supsetneqq$ (og $\mathcal{S}$ en gruppe). $L = \mathbb{C}(X)$, $K = \mathbb{C}$, $\mathcal{S}$ = alle "translationer"

$$\mathcal{S} = \{\sigma \in \mathrm{Aut}\,\mathbb{C}(X) \mid \sigma\left(\frac{f(x)}{g(x)}\right) = \frac{f(x+a)}{g(x+a)}\},$$

hvor a gennemløber $\mathbb{C}$. Her er $\mathcal{F}(\mathcal{S}) = \mathbb{C}$ og $\mathrm{Gr}(L/\mathcal{F}(\mathcal{S})) \supsetneqq \mathcal{S}$, idet $x \to \frac{1}{x}$ inducerer automorfi i $\mathrm{Gr}(\mathbb{C}(X)/C)$ der ikke tilhører $\mathcal{S}$.

Definition. $L \supseteqq K$ kaldes en *normal udvidelse*, hvis $K = \mathcal{F}(\mathrm{Gr}(L/K))$. Hvis ydermere $[L : K] < \infty$ kaldes L en *endelig normal udvidelse* af K.

Sætning 1. *Hvis M er spaltningslegemet over legemet K for et separabelt polynomium $f(x) \in K[X]$, da er M en endelig normal udvidelse af K.*

Bevis. $[M : K] < \infty$ er klart. Hvis alle rødderne til $f(x)$ ligger i K, er $M = K$, og der er intet at bevise. Så lad os antage at $M \supsetneqq K$. Vi kan da vælge rødder $\alpha_1, ..., \alpha_t$ til $f(x)$, så $M = K(\alpha_1, \dots, \alpha_t)$ og $K \subsetneqq K(\alpha_1) \subsetneqq K(\alpha_1, \alpha_2) \subsetneqq \cdots \subsetneqq K(\alpha_1, ..., \alpha_t) = M$. Vi skal vise, at $\forall \beta \in M \setminus K \; \exists \sigma \in \mathrm{Gr}(M/K)$ så $\sigma(\beta) \neq \beta$.

Antag $\beta \in K(\alpha_1, \dots, \alpha_i) \setminus K(\alpha_1, \dots, \alpha_{i-1})$. For at lette notationen sættes $L = K(\alpha_1, \dots, \alpha_{i-1})$, $\gamma = \alpha_i$. Altså $\beta \in L(\gamma)$, $\beta \notin L$. Nu må gælde:

$$\mathrm{Irr}(\gamma, L) \big| \mathrm{Irr}(\gamma, K) \big| f(x)\,.$$

Da $f(x)$ er separabel, har $\mathrm{Irr}(\gamma, K)$ og dermed specielt $\mathrm{Irr}(\gamma, L)$ lutter simple rødder.

Hvis $[L(\gamma) : L] = \mathrm{Grad}(\mathrm{Irr}(\gamma, L)) = n$, har $\mathrm{Irr}(\gamma, L)$ altså præcist n indbyrdes forskellige rødder $\gamma_1, \gamma_2, \dots, \gamma_n$, hvor f.eks. $\gamma = \gamma_1$.

β kan skrives på formen

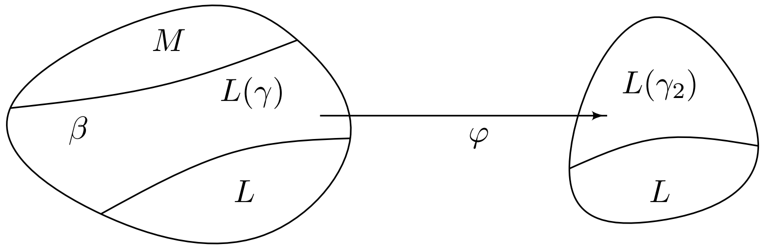
$$\beta = a_0 + a_1\gamma + \cdots + a_{n-1}\gamma^{n-1}\,,\; a_0, \dots, a_{n-1} \in L$$

og $\beta \notin L \Rightarrow a_i \neq 0$ for mindst et $i \geqq 1$.

Ikke alle elementerne $a_0 + a_1\gamma_j + \cdots + a_{n-1}\gamma_j^{n-1}$, $j = 1, 2, \dots, n$ kan være $= \beta$. Thi ellers ville det egentlige polynomium $\beta - a_0 - a_1 x - \cdots - a_{n-1}x^{n-1}$ af grad $< n$ have n rødder $\gamma_1, \dots, \gamma_n$.

Antag f.eks. $a_0 + a_1\gamma_2 + \cdots + a_{n-1}\gamma_2^{n-1} \neq \beta$.

Ifølge entydighedssætningen vedrørende adjunktion af en rod til et irreducibelt polynomium findes en isomorfi $\varphi : L(\gamma) \to L(\gamma_2)$ så $\varphi_{\mathrm{Res},L} = 1_L$ og $\varphi(\gamma) = \gamma_2$.



Her er $\varphi(\beta) = \varphi(a_0 + a_1\gamma + \cdots + a_{n-1}\gamma^{n-1}) = a_0 + a_1\gamma_2 + \cdots + a_{n-1}\gamma_2^{n-1}$, der ifølge ovenstående er $\neq \beta$. Nu er M spaltningslegeme for $f(x)$ over $L(\gamma)$ og M er spaltningslegeme for $f(x)$ over $L(\gamma_2)$.

Da $f(x) \in K[X] \subseteqq L[X]$ vil $f(x)$ ved den af φ inducerede afbildning af polynomiumsringene $L(\gamma)[X] \to L(\gamma_2)[X]$ føres over i sig selv. Ifølge sætningen om entydighed af spaltningslegemet kan φ fortsættes til en automorfi $\widetilde{\varphi} : M \to M$. $\widetilde{\varphi}$ har egenskaberne $\widetilde{\varphi}(\beta) \neq \beta$ og $\widetilde{\varphi}_{\mathrm{Res},K} = 1_K$ dvs.: $\widetilde{\varphi}$ er automorfi i $\mathrm{Gr}(M/K)$ med den ønskede egenskab. $\square$

— — — — — — — — — — — — — — — —

Eksempel. $M = K(T)$, $f(x) = (x - T)(x - \frac{1}{T}) = x^2 - (T + \frac{1}{T})x + 1$. M er spaltningslegeme for $f(x)$ over $L = K(T + \frac{1}{T})$. $f(x)$ er øjensynlig separabel. $\mathrm{Gr}(M/L) = \{1_L \quad \text{og} \quad \sigma\}$, hvor $\sigma(g(T)) = g(\frac{1}{T})$ for $g(T) \in K(T)$. Heraf fås $g(T) = g(\frac{1}{T}) \Leftrightarrow g =$ brudden rational funktion af $T + \frac{1}{T}$.

Eksempel. $M = K(x_1, \dots, x_n)$, $L = K(s_1, \dots, s_n)$, hvor $s_1, \dots, s_n$ er de elementar-symmetriske polynomier $s_1 = x_1 + \cdots + x_n$, $s_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n, \dots, s_n = x_1 \dots x_n$, $f(Y) = (Y - x_1)\dots(Y - x_n) = Y^n - s_1Y^{n-1} + \cdots + (-1)^n s_n \in L[Y]$. M er spaltningslegeme for $f(y)$ over L og $f(y)$ separabelt. Ifølge ovenstående sætning er $L = \mathcal{F}(\mathrm{Gr}(M/L))$; automorfierne i $\mathrm{Gr}(M/L)$ er netop dem, der induceres af de $n!$ permutationer af de n variable $x_1, \dots, x_n$. Hvilken "klassisk" sætning fås herved?

Sætning 2. *Idet* $\mathrm{GF}(p^n)$ *som sædvanlig betegner legemet med* p^n *elementer, gælder:* $\mathrm{Gr}(\mathrm{GF}(p^n)/\mathbb{Z}_p)$ *er cyklisk af orden* n *og frembringes af den automorfi ("Frobenius-automorfien"), der sender ethvert element over i dets* p*-te potens.*

Bevis. Vælg $\alpha \in \mathrm{GF}(p^n)$ så $\mathrm{GF}(p^n) = \mathbb{Z}_p(\alpha)$. Lad $f(x) = \mathrm{Irr}(\alpha, \mathbb{Z}_p)$. En automorfi $\sigma \in \mathrm{Gr}(GF(p^n)/\mathbb{Z}_p)$ er entydigt bestemt ved værdien på α; derfor er der højst n muligheder for σ. På den anden side er (som tidligere vist): $\sigma : a \to a^p$ (potensering med p) en automorfi. Her er $\sigma^n =$ identiteten, og $\sigma^i \neq$ identiteten for $0 < i < n$. Thi ellers var alle elementer i $\mathrm{GF}(p^n)$ rødder i polynomiet $X^{p^i} - X$, hvilket er umuligt, da $\mathrm{GF}(p^n)$ har p^n elementer. Altså består $\mathrm{Gr}(\mathrm{GF}(p^n)/\mathbb{Z}_p)$ netop af potenserne $\sigma, \sigma^2, \dots, \sigma^n = e$. $\square$

Sætning 3. *Enhver mængde af indbyrdes forskellige automorfier* $\sigma_1, \dots, \sigma_n$ *i et legeme* L *er uafhængig, dvs. hvis* $a_1, \dots, a_n \in L$ *og* $a_1\sigma_1(x) + \cdots + a_n\sigma_n(x) = 0$ *for alle* $x \in L$*, da er* $a_1 = \cdots = a_n = 0$.

Bevis. Induktion efter n.

Tilfældet $n = 1$ er klart. Thi for $x = 1$ er $a_1\sigma_1(1) = a_1 = 0$.

Angående $n - 1 \to n$:

Antag, at

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \cdots + a_n\sigma_n(x) = 0 \;\forall x \in L\,. \tag{$*$}$$

For ethvert $b \in L$ er $a_1\sigma_1(bx) + a_2\sigma_2(bx) + \cdots + a_n\sigma_n(bx) = 0 \;\forall x \in L$ eller

$$a_1\sigma_1(b)\sigma_1(x) + a_2\sigma_2(b)\sigma_2(x) + \cdots + a_n\sigma_n(b)\sigma_n(x) = 0 \;\forall x \in L\,.$$

Ved multiplikation af $(*)$ med $\sigma_1(b)$ fås

$$a_1\sigma_1(b)\sigma_1(x) + a_2\sigma_1(b)\sigma_2(x) + \cdots + a_n\sigma_1(b)\sigma_n(c) = 0 \;\forall x \in L$$

og hermed

$$a_2(\sigma_2(b) - \sigma_1(b))\sigma_2(x) + \cdots + a_n(\sigma_n(b) - \sigma_1(b))\sigma_n(x) = 0 \;\forall x \in L\,.$$

Vælges $b \in L$ så $\sigma_n(b) \neq \sigma_1(b)$ giver induktionsantagelsen at $a_n = 0$. Indsat i $(*)$ fås (igen ved induktionsantagelsen), at $a_1 = \cdots = a_{n-1} = 0$. $\square$

Sætning 4. *Lad $\sigma_1, \dots, \sigma_n$ være indbyrdes forskellige automorfier i L, og lad K være et legeme,der er indeholdt i $\mathcal{F}(\{\sigma_1, \dots, \sigma_n\})$. Da er $[L : K] \geqq n$.*

Bevis. Indirekte. Antag $[L : K] = r < n$. Lad $\omega_1, \dots, \omega_r$ være en basis for L som vektorrum over K. Det homogene ligningssystem

$$\begin{gathered} x_1\sigma_1(\omega_1) + \cdots + x_n\sigma_n(\omega_1) = 0 \\ \cdots \\ x_1\sigma_1(\omega_r) + \cdots + x_n\sigma_n(\omega_r) = 0 \end{gathered} \tag{$**$}$$

har egentlig løsning i L, da $r < n$ (sætning fra Mat 1[1]). Et vilkårligt element $\beta \in L$ kan skrives $\beta = a_1\omega_1 + \cdots + a_r\omega_r$, hvor $a_1, \dots, a_r \in K$. På grund af $(**)$ gælder:

$$x_1\sigma_1(\beta) + \cdots + x_n\sigma_n(\beta) = 0$$

dvs. modstrid med foregående sætning. □

Sætning 5. *Lad G være en gruppe af automorfier i L. Da gælder $[L : \mathcal{F}(G)] = |G|$ (forstået således, at hvis den ene side er endelig, er den anden også, og da = den første).*

Bevis. På grund af den foregående sætning er det nok at betragte tilfældet, hvor G er endelig. Antag G har orden n $(< \infty)$. Igen på grund af den foregående sætning er det nok at vise $[L : \mathcal{F}(G)] \leqq n$. Vi skal hertil vise, at hvilke som helst $(n + 1)$ elementer i L er lineært afhængige over $\mathcal{F}(G)$.

Hertil to lemmaer:

Lemma 1. *For ethvert $x \in L$ er "sporet" $S(x) = \sum_{\sigma\in G} \sigma(x)$ et element i $\mathcal{F}(G)$.*

Bevis. For ethvert $\sigma' \in G$ er $\sigma'(S(x)) = \sum_{\sigma\in G} \sigma'\sigma(x) = \sum_{\sigma\in G} \sigma(x) = S(x)$. □

Lemma 2. *$\exists x \in L$ så $S(x) \neq 0$.*

Bevis. Anvend sætning 3 om uafhængighed af forskellige automorfier. □

Nu tilbage til beviset for sætning 5. Lad $G = \{\sigma_1, \dots, \sigma_n\}$.

Det homogene lineære ligningssystem, hvor $\omega_1, \dots, \omega_{n+1}$ er vilkårlige elementer i L,

$$\begin{gathered} x_1\sigma_1^{-1}(\omega_1) + \cdots + x_{n+1}\sigma_1^{-1}(\omega_{n+1}) = 0 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ x_1\sigma_n^{-1}(\omega_1) + \cdots + x_{n+1}\sigma_n^{-1}(\omega_{n+1}) = 0 \end{gathered}$$

[1] Et homogent lineært ligningssystem har en egentlig løsning, når antallet af ubekendte er større end antallet af ligninger.

har egentlig løsning $(x_1, \ldots, x_{n+1})$ i L. Vi kan antage $x_1 \neq 0$ og ved multiplikation med passende element i L kan vi (p.gr. af Lemma 2) opnå $S(x_1) \neq 0$.

Ved anvendelse af automorfierne $\sigma_1, \ldots, \sigma_n$ på ovenstående ligningssystem fås

$$S(x_1)\omega_1 + \cdots + S(x_{n+1})\omega_{n+1} = 0$$

dvs.: $\omega_1, \ldots, \omega_{n+1}$ er lineært afhængige over $\mathcal{F}(G)$. $\square$

(*Bemærkning.* Ovenstående sætning gælder ikke for uendelige kardinaltal.)

Korollar 1. *For en endelig gruppe G af automorfier i L gælder: $Gr(L/\mathcal{F}(G)) = G$.*

Bevis. Det er klart at $\mathrm{Gr}(L/\mathcal{F}(G)) \supseteqq G$. Lad os nu vise den modsatte inklusion. Antag G har orden n. Da er $[L : \mathcal{F}(G)] = n$. På grund af Sætning 5 kan $\mathrm{Gr}(L/\mathcal{F}(G))$ ikke indeholde flere automorfier end de i G forekommende. $\square$

Korollar 2. *Forskellige endelige automorfigrupper i L har forskellige fixpunktslegemer.*

Vi minder om begrebet normal udvidelse. L/K er endelig normal, hvis $[L : K] < \infty$ og $K = \mathcal{F}(\mathrm{Gr}(L/K))$. $\mathrm{Gr}(L/K)$ kaldes *Galoisgruppen for L/K.*

På grund af ovenstående vil ordenen af Galoisgruppen $\mathrm{Gr}(L/K)$ *være lig dimensionen* $[L : K]$.

Endvidere gælder åbenbart for en endelig udvidelse L/K, at L/K normal $\Leftrightarrow K =$ fixpunktslegeme for en gruppe af automorfier i L.

Eksempel. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ er normal, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ er ikke normal.

Eksempel. $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ er normal og $\mathrm{Gr}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \simeq$ Kleins Viergruppe (hvorfor ?)

Vi giver nu en meget vigtig karakterisering af de endelige normal udvidelser.

Sætning 6. *L/K endelig normal $\Leftrightarrow L =$ spaltningslegemet for et separabelt polynomium $f(x)$ over K.*

Bevis. "$\Leftarrow$" er tidligere vist (Sætning 1).

"$\Rightarrow$" fås som konsekvens af

Sætning 7. *Lad L/K være en endelig normal udvidelse. Hvis et i $K[X]$ irreducibelt polynomium $p(x)$ har blot én rod $\alpha \in L$, da ligger samtlige rødder til $p(x)$ i L og disse er alle simple, og de er de forskellige blandt $\{\sigma(\alpha) \mid \sigma \in \mathrm{Gr}(L/K)\}$.Specielt er $p(x)$ separabelt.*

Bevis. Idet $p(x)$ antages normeret, er $p(x) = \mathrm{Irr}(\alpha, K)$. Lad $\sigma_1(\alpha), \ldots, \sigma_j(\alpha)$ være de indbyrdes forskellige elementer i mængden $\{\sigma(\alpha) \mid \sigma \in \mathrm{Gr}(L/K)\}$. For enhver automorfi $\tau \in \mathrm{Gr}(L/K)$ bliver da $\{\tau\sigma_1(\alpha), \ldots, \tau\sigma_j(\alpha)\} = \{\sigma_1(\alpha), \ldots, \sigma_j(\alpha)\}$.

Lad $\hat{\tau}$ være den af τ inducerede automorfi af $L[X]$ på sig selv. ($\hat{\tau}$ (polynomium i $L[X]$) = det polynomium der fås ved koefficientvis anvendelse af τ). Lad $f(x) = [x - \sigma_1(\alpha)] \cdots [x - \sigma_j(\alpha)]$. Da er

$$\hat{\tau} f(x) = [x - \tau\sigma_1(\alpha)] \cdots [x - \tau\sigma_j(\alpha)] = f(x)\,.$$

Dette gælder for alle $\tau \in \mathrm{Gr}(L/K)$, dvs.: $f(x)$ har koefficienter i $\mathcal{F}(\mathrm{Gr}(L/K)) = K$. $f(x)$ er altså et polynomium i $K[X]$ og $f(\alpha) = 0$, derfor vil $p(x) = \mathrm{Irr}(\alpha, K) | f(x)$.

På den anden side gælder (ifl. Praktisk Lemma), at $p(\alpha) = 0 \Rightarrow p(\sigma(\alpha)) = 0\ \forall \sigma \in \mathrm{Gr}(L/K)$. Følgelig er hvert af elementerne $\sigma_1(\alpha), \ldots, \sigma_j(\alpha)$ rødder i $p(x)$ og dermed vil $f(x) = [x - \sigma_1(\alpha)] \cdots [x - \sigma_j(\alpha)] \mid p(x)$. Men så er $f(x)$ og $p(x)$ altså normerede polynomier, for hvilke $f(x) \mid p(x)$ og $p(x) \mid f(x)$. Dette medfører $f(x) = p(x)$. $\square$

Nu tilbage til beviset for "$\Rightarrow$" i Sætning 6.

Den lige viste sætning indebærer specielt, at enhver endelig normal udvidelse er separabel. Ifølge Abel-Steinitz's sætning er L/K simpel dvs.: $L = K(\alpha)$ for passende $\alpha \in L$. $p(x) = \mathrm{Irr}(\alpha, K)$ spaltes på grund af den lige viste sætning til bunds i 1-gradsfaktorer inden for L, og intet ægte dellegeme af L indholdende K har denne egenskab; altså er L spaltningslegeme for $\mathrm{Irr}(\alpha, K)$ og $\mathrm{Irr}(\alpha, K)$ er separabelt. $\square$

Vi giver endnu en karakterisering af endelige normale udvidelser.

Sætning 8. *For en endelig udvidelse L/K gælder: L/K normal $\Leftrightarrow$ L/K separabel og ethvert irreducibelt polynomium i $K[X]$ med blot én rod i L har samtlige rødder i L.*

Bevis. "$\Rightarrow$" er allerede vist.

"$\Leftarrow$" På grund af Abel-Steinitz's sætning er $L = K(\alpha)$ for et passende $\alpha \in L$. L er derfor spaltningslegeme for det separable polynomium $p(x) = \mathrm{Irr}(\alpha, K)$. $\square$

Bemærkning. Hos nogle forfattere kaldes en endelig udvidelse L/K normal, hvis ethvert i $K[x]$ irreducibelt polynomium med blot én rod i L har samtlige rødder i L, mens en udvidelse, der er normal i disse noters terminologi, kaldes Galois'sk. For fuldkomne legemer, specielt legemer af karakteristik 0, stemmer de to definitioner overens.

Sætning 9. *Antag $M \supseteq L \supseteq K$, M/K endelig, normal. Da er M/L endelig, normal.*

Bevis. M/K endelig normal $\Rightarrow$ M = spaltningslegeme for separabelt polynomium $f(x)$ over K $\Rightarrow$ M = spaltningslegemet for $f(x)$ over L $\Rightarrow$ M/L endelig normal. $\square$

Eksempel. $M \supsetneqq L \supsetneqq K$, M/K endelig normal $\not\Rightarrow$ L/K normal. Et modeksempel fås ved at tage $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$, M = spaltningslegemet for $x^3 - 2$ over $\mathbb{Q}$. Ifølge sætning 1 er $M/\mathbb{Q}$ normal, mens $L/\mathbb{Q}$ som tidligere omtalt ikke er normal.

Sætning 10. *Lad L/K være endelig. Da findes et legeme M indeholdende L, så M/K er en endelig, normal udvidelse $\Leftrightarrow$ L/K separabel.*

Bevis. "$\Rightarrow$" klar.

"$\Leftarrow$" Ifølge Abel-Steinitz's sætning er $L = K(\alpha)$ for passende $\alpha \in L$. Hvis vi lader $M =$ være spaltningslegemet over K for $p(x) = \mathrm{Irr}(\alpha, K)$. Da er M en normal udvidelse af K indeholdende L. $\square$

Sætning 11. *Lad L/K være en vilkårlig udvidelse og α og β elementer i L. Da gælder α og β separable over $K \Rightarrow \alpha + \beta$, $\alpha \cdot \beta$, $\frac{\alpha}{\beta} (\beta \neq 0)$ separable over K.*

Bevis. Lad $f(x) = \mathrm{Irr}(\alpha, K)$, $g(x) = \mathrm{Irr}(\beta, K)$. Polynomiet $f(x) \cdot g(x)$ er separabelt, hvorfor spaltningslegemet M for $f(x) \cdot g(x)$ over K er en normal udvidelse af K. Vi kan antage at $M \supseteqq K(\alpha, \beta)$. Ifølge det ovenfor viste er M/K separabel, og $\alpha \pm \beta$, $\alpha \cdot \beta$, $\frac{\alpha}{\beta} (\beta \neq 0)$ tilhører M. $\square$

Ved hjælp af de foregående sætninger er vi nu i stand til at bevise

Galoisteoriens hovedsætning. *M/K antages at være en endelig normal udvidelse med Galoisgruppe $G = \mathrm{Gr}(M/K)$. (Her er $[M : K] = |G|$ (jvf. Sætning 5)). Da findes en $(1-1)$ forbindelse mellem undergrupperne i G og "mellemlegemerne" i M/K (dvs.: dellegemer af M indeholdende K). Denne $(1-1)$ forbindelse fås på følgende måde:*

Til ethvert mellemlegeme L tilordnes $TL = \mathrm{Gr}(M/L)$ (som er en undergruppe i G); til enhver undergruppe H i G tilordnes fixpunktslegemet $\mathcal{F}(H)$ $(K \subseteq \mathcal{F}(H) \subseteq M)$. Da gælder

1) *$\mathcal{F}(TL) = L$, $T(\mathcal{F}(H)) = H$ (dette giver den omtalte $(1-1)$ forbindelse).*
2) *$|TL| = [M : L]$; $[L : K] = [G : TL]$.*
3) *$L_1 \subseteqq L_2 \Leftrightarrow TL_1 \supseteqq TL_2$; $H_1 \subseteqq H_1 \Leftrightarrow \mathcal{F}(H_1) \supseteqq \mathcal{F}(H_2)$.*
4) *For et mellemlegeme L gælder: L/K normal $\Leftrightarrow TL \lhd G$.*
5) *Hvis L/K er normal (hvorfor ifølge 4) $TL \lhd G$) er $\mathrm{Gr}(L/K) \cong G/TL$ og enhver automorfi i $\mathrm{Gr}(L/K)$ kan fortsættes til en automorfi i $\mathrm{Gr}(M/K)$.*

Bevis.

ad 1) $\mathcal{F}(TL) = L$ følger af Sætning 9, $T\mathcal{F}(H) = H$ følger af Korollar 1 til Sætning 5.

ad 2) Jvf. Sætning 5.

ad 3) De to pile $\Rightarrow$ fra venstre mod højre er trivielle. Lad os nu betragte de modsatte implikationer. Antag $TL_1 \supseteqq TL_2$. Anvendes den (trivielle)$\Rightarrow$ herpå, fås $\mathcal{F}(TL_1) \subseteqq \mathcal{F}(TL_2)$, hvilket ifl. 1) netop betyder $L_1 \subseteqq L_2$. Den anden pil $\Leftarrow$ fås ved et analogt argument.

ad 4) Hertil et

Lemma. *For et mellemlegeme L gælder: L/K normal $\Leftrightarrow \sigma L = L\ \forall \sigma \in G$.*

Bevis. "$\Rightarrow$" Det er nok at godtgøre $\sigma L \subsetneqq L$ for $\forall \sigma \in G$ (hvorfor ?).

Lad $\alpha \in L$, $p(x) = \mathrm{Irr}(\alpha, K)$, da er $\sigma(\alpha)$ (ifl. Praktisk Lemma) også rod i $p(x)$ for $\forall \sigma \in G$. Ifølge Sætning 7 er $\sigma(\alpha)$ et element i L dvs.: $\sigma(\alpha) \in L$, for $\forall \alpha \in L$, $\forall \sigma \in G$.

"$\Leftarrow$" Da M/K er normal, er M/K separabel, specielt er L/K separabel. Ifølge Abel-Steinitz sætning er $L = K(\alpha)$ for et passende $\alpha \in L$. Rødderne til $p(x) = \mathrm{Irr}(\alpha, K)$ er (Sætning 7) elementerne $\sigma(\alpha)$, $\sigma \in G$.

Da $\sigma L = L$ ligger alle disse rødder i L, der herved ses at blive spaltningslegeme for det separable polynomium $p(x)$ over K, dvs.: L/K er normal ifl.Sætning 1. $\square$

Vi anvender nu dette lemma til beviset for 4). Ifølge definitionen er $TL = \{\sigma \in G \mid \sigma(\ell) = \ell\ \forall \ell \in L\}$. For en automorfi $\tau \in G$ er $T(\tau L) = \{\sigma \in G \mid \sigma\tau\ell = \tau\ell\ \forall \ell \in L\} = \{\sigma \in G \mid \tau^{-1}\sigma\tau\ell = \ell\ \forall \ell \in L\} = \{\sigma \in G \mid \tau^{-1}\sigma\tau \in TL\} = \tau(TL)\tau^{-1}$. Altså får vi

$$\begin{aligned} L/K \text{ normal } &\Leftrightarrow \tau L = L\ \forall \tau \in G \Leftrightarrow T(\tau L) = TL\ \forall \tau \in G \\ &\Leftrightarrow \tau TL\tau^{-1} = TL\ \forall \tau \in G \Leftrightarrow TL \lhd G\,. \end{aligned}$$

ad 5) Antag L/K normal og dermed $TL \lhd G$.

Vi definerer en afbildning $\varphi : G = \mathrm{Gr}(M/K) \to \mathrm{Gr}(L/K)$ ved $\varphi(\sigma) = \sigma_{\mathrm{Res},L}$. Ifølge ovenstående lemma er $\sigma_{\mathrm{Res},L}$ virkelig en automorfi for L (der er identiteten på K) dvs.: $\sigma_{\mathrm{Res},L} \in \mathrm{Gr}(L/K)$. Derfor er φ en veldefineret homomorfi fra G ind i $\mathrm{Gr}(L/K)$.

For kernen af denne homomorfi gælder $\mathrm{Ker}\,\varphi = \{\sigma \in G \mid \sigma_{\mathrm{Res},L} = 1_L\} = \mathrm{Gr}(M/L) = TL$. Derfor fås en isomorfi $G/TL \simeq \varphi G \subsetneqq \mathrm{Gr}(L/K)$. Nu er ifl. 2) $|G/TL| = [L:K]$. Endvidere er ifl. Sætning 5 $|Gr(L/K)| = [L:K]$, hvorfor φG er en undergruppe af $\mathrm{Gr}(L/K)$ af samme orden som $\mathrm{Gr}(L/K)$. Følgelig er $\varphi G = \mathrm{Gr}(L/K)$. $\square$

Opgave. Lad M/L og L/K være endelige normal udvidelser. Vis ved et eksempel, at M/K ikke nødvendigvis er en normal udvidelse.

Lad M/L og L/K være endelige normale udvidelser og antag yderligere, at enhver automorfi i $\mathrm{Gr}(L/K)$ kan fortsættes til en automorfi for M. Vis, at dette medfører, at M/K er en normal udvidelse. (Sammenhold dette med punkt 5 i Galoisteoriens Hovedsætning.)

— — — — — — — — — — — — — — — —

Supplement til Galoisteoriens hovedsætning. For to legemer L_1, L_2 indeholdt i M findes et mindste legeme ("*kompositet*") der indeholder L_1 og L_2. Det betegnes $\{L_1, L_2\}$ eller blot L_1L_2. Tilsvarende for undergrupper H_1, H_2 i given gruppe. Kompositet benævnes $\{H_1, H_2\}$. Med de i Galoisteoriens hovedsætning indførte benævnelser gælder da:

$$
\begin{aligned}
&T\{L_1, L_2\} = TL_1 \cap TL_2,\\
&T(L_1 \cap L_2) = \{TL_1, TL_2\},\\
&\mathcal{F}(H_1 \cap H_2) = \{\mathcal{F}H_1, \mathcal{F}H_2\},\\
&\mathcal{F}\{H_1, H_2\} = \mathcal{F}H_1 \cap \mathcal{F}H_2.
\end{aligned}
$$

Bevis. Vi nøjes med at eftervise den første:

$$
\left.\begin{array}{l}
\{L_1, L_2\} \supseteqq L_1 \Rightarrow TL_1 \supseteqq T\{L_1, L_2\}\\[2ex]
\{L_1, L_2\} \supseteqq L_2 \Rightarrow TL_2 \supseteqq T\{L_1, L_2\}
\end{array}\right\} \Rightarrow T\{L_1, L_2\} \subseteqq TL_1 \cap TL_2
$$

Endvidere

$$
\left.\begin{array}{l}
\mathcal{F}(TL_1 \cap TL_2) \supseteqq \mathcal{F}TL_1 = L_1\\[2ex]
\mathcal{F}(TL_1 \cap TL_2) \supseteqq \mathcal{F}TL_2 = L_2
\end{array}\right\} \Rightarrow \mathcal{F}(TL_1 \cap TL_2) \supseteqq \{L_1, L_2\}
$$

$\Rightarrow TL_1 \cap TL_2 \subseteqq T\{L_1, L_2\}$. □

Korollar. *Med de foregående betegnelser gælder: L_1/K normal og L_2/K normal $\Rightarrow L_1 \cap L_2/K$ normal og $\{L_1, L_2\}/K$ normal.*

Vi skal nu vise en sætning, der kan være nyttig til den praktiske bestemmelse af Galoisgruppen for en normal udvidelse.

Sætning 12. *Lad M være spaltningslegemet over et legeme K for et n-tegradspolynomium $p(x)$ uden multiple rødder. Da findes en isomorfi φ af Galoisgruppen* $\mathrm{Gr}(M/K)$ *på en undergruppe i den symmetriske gruppe S_n. Derfor gælder følgende: $[M : K] \leqq n!$ og endda $[M : K] \mid n!$. Hvis $p(x)$ er irreducibelt i $K[X]$, er $\varphi\,\mathrm{Gr}(M/K)$ en transitiv undergruppe i S_n og man har: $n \leqq [M : K] \leqq n!$ og endda $n \mid [M : K] \mid n!$*

Bevis. $M = K(\alpha_1, \dots, \alpha_n)$ hvor $\alpha_1, \dots, \alpha_n$ er de (indbyrdes forskellige) rødder i $p(x)$. En automorfi $\sigma \in Gr(M/K)$ er entydig bestemt ved værdierne på $\alpha_1, \dots, \alpha_n$. Ifølge Praktisk Lemma er elementerne $\sigma(\alpha_i)$, $1 \leqq i \leqq n$, rødder i $p(x)$. Heraf følger, at $\begin{pmatrix} \alpha_1, \dots, \alpha_n \\ \sigma(\alpha_1), \dots, \sigma(\alpha_n) \end{pmatrix}$ er en permutation af rødderne $\alpha_1, \dots, \alpha_n$. Endvidere bliver afbildningen $Gr(M/K) \xrightarrow[\varphi]{} S_n$, $\varphi\sigma = \begin{pmatrix} \alpha_1, \dots, \alpha_n \\ \sigma(\alpha_1), \dots, \sigma(\alpha_n) \end{pmatrix}$ en homomorfi af $Gr(M/K)$ ind i S_n; da σ er entydig bestemt ved værdierne på $\alpha_1, \dots, \alpha_n$ bliver φ injektiv. Hvis $p(x)$ antages at være irreducibelt i $K[X]$ medfører Sætning 7, at $\varphi(Gr(M/K))$ er en transitiv undergruppe i S_n. Transitivitetssætningen (Sætn.9 i Kap.II) medfører $n \mid [M : K]$, idet M indeholder f.eks. $K(\alpha_1)$, der har dimension n over K. □

Sætning 12A. *Lad M være spaltningslegemet over et legeme K for et n-tegradspolynomium $p(x)$ uden multiple rødder og antag at karakteristikken for K er $\neq 2$. Da vil for den i Sætning 12 indførte isomorfi φ gælde, at $\varphi\,\mathrm{Gr}(M/K)$ er en undergruppe i den alternerende gruppe A_n hvis og kun hvis diskriminanten $disk(p)$ er kvadratet af et element i K.*

Bevis. $M = K(\alpha_1, \dots, \alpha_n)$, hvor $\alpha_1, \dots, \alpha_n$ er de indbyrdes forskellige rødder i $p(x)$. Vi betragter den i forrige sætning indførte afbildning $\varphi : \mathrm{Gr}(M/K) \to S_n$.

Antag $\varphi(\mathrm{Gr}(M/K) \subseteq A_n$. Da er $\Delta(\alpha_1, \dots, \alpha_n) = \prod_{i>j}(\alpha_i - \alpha_j)$ invariant overfor alle automorfier i $\mathrm{Gr}(M/K)$, hvorfor $\Delta(\alpha_1, \dots, \alpha_n) \in K$. Derfor er $disk(p) = (\Delta(\alpha_1, \dots, \alpha_n))^2$ kvadratet af et element i K.

Antag dernæst, at $\varphi\,\mathrm{Gr}(M/K) \nsubseteq A_n$. Da findes $\sigma \in \mathrm{Gr}(M/K)$, så $\sigma\Delta(\alpha_1, \dots, \alpha_n) = -\Delta(\alpha_1, \dots, \alpha_n)$. Da K's karakteristik ikke er 2 , er $\Delta(\alpha_1, \dots, \alpha_n)$ ikke et element i K og $disk(p)$ dermed ikke kvadratet af et element i K. □

Eksempel. Lad M være spaltningslegemet for $x^3 - 2$ over $\mathbb{Q}$. $x^3 - 2$ er irreducibelt (Eisenstein) og separabelt. Ifølge foregående sætning er $\mathrm{Gr}(M/\mathbb{Q}) \simeq$ transitiv undergruppe i S_3. Da $M = \mathbb{Q}(\sqrt[3]{2}, \rho)$, hvor ρ er en fra 1 forskellig 3^{de} enhedsrod $\frac{-1+i\sqrt{3}}{2}$, er $[M : \mathbb{Q}] = 6$ og $\mathrm{Gr}(M/\mathbb{Q}) \simeq S_3$.

Opgave. Vis, at enhver udvidelse M af $\mathbb{Q}$ så $M/\mathbb{Q}$ er normal og $\mathrm{Gr}(M/\mathbb{Q}) \cong S_3$ fås som spaltningslegeme for et irreducibelt 3^{de} gradspolynomium over $\mathbb{Q}$.

Eksempel. Lad M være spaltningslegeme for $x^4 - 2$ over $\mathbb{Q}$. $M = \mathbb{Q}(\sqrt[4]{2}, i)$, hvoraf $[M : \mathbb{Q}] = 8$ (hvorfor ?)

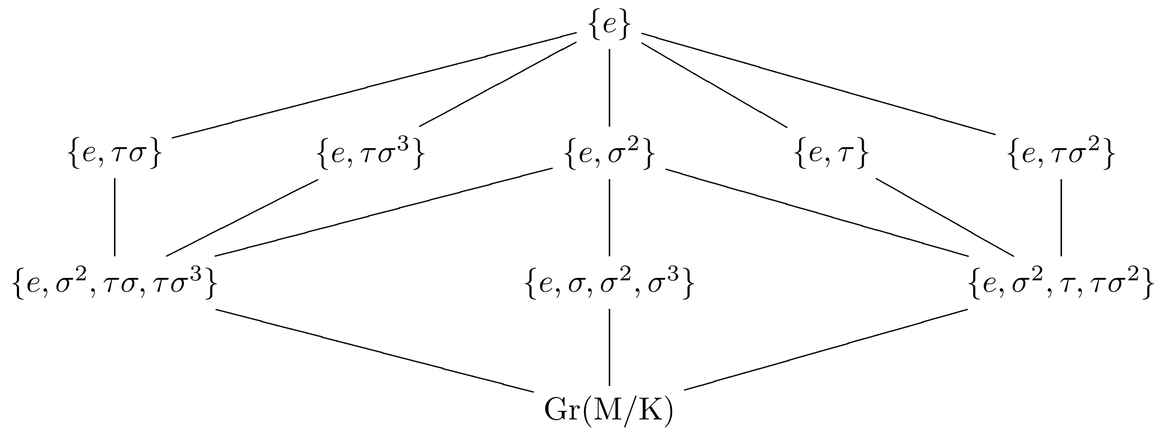
Ifølge den ovenfor viste sætning er $\mathrm{Gr}(M/\mathbb{Q}) \simeq$ transitiv undergruppe i S_4 og følgelig $\simeq$ diedergruppen D_4 af orden 8 (hvorfor ?)

En automorfi i $\mathrm{Gr}(M/\mathbb{Q})$ er entydigt bestemt ved værdierne på $\sqrt[4]{2}$ og i. For værdierne på $\sqrt[4]{2}$ er der (ifl. Praktisk Lemma) følgende muligheder: $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$. For værdierne på i er der mulighederne $+i$ og $-i$. Da $\mathrm{Gr}(M/\mathbb{Q})$ har orden 8, kan enhver af de ovenstående 8 kombinationer realiseres eksakt én gang. Altså består $\mathrm{Gr}(M/\mathbb{Q})$ af følgende automorfier:

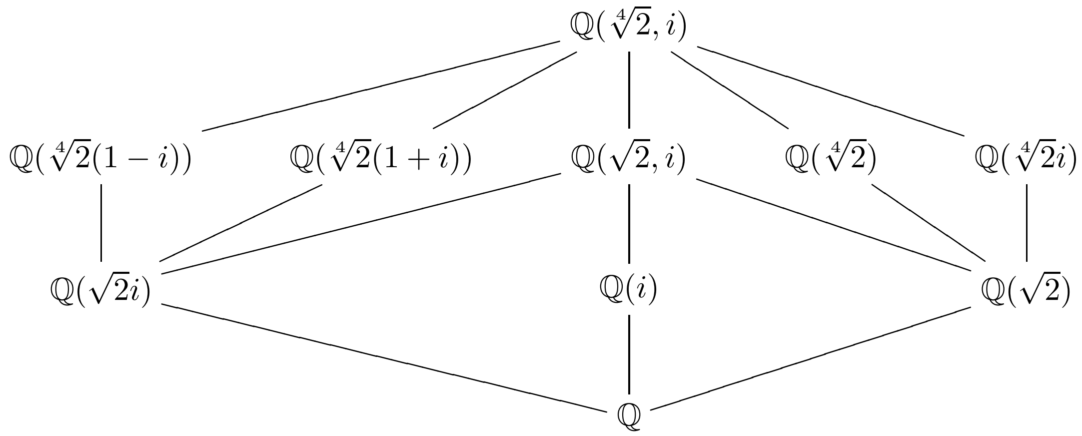
$$\begin{aligned}
&\sigma\,,\ \sigma^2\,,\ \sigma^3\,,\ \sigma^4 = e\,,\ \tau\,,\ \tau\sigma\,,\ \tau\sigma^2\,,\ \tau\sigma^3\,,\ \text{ hvor}\\
&\sigma(\sqrt[4]{2}) = \sqrt[4]{2}i\,,\ \sigma^2(\sqrt[4]{2}) = -\sqrt[4]{2}\,;\ \sigma^3(\sqrt[4]{2}) = -i\sqrt[4]{2}\,;\ \sigma^4(\sqrt[4]{2}) = \sqrt[4]{2}\\
&\sigma(i) = i\,;\ \sigma^2(i) = i\,;\ \sigma^3(i) = i\,;\ \sigma^4(i) = i\\
&\tau(\sqrt[4]{2}) = \sqrt[4]{2}\ \ \tau\sigma(\sqrt[4]{2}) = -i\sqrt[4]{2}\ \ \tau\sigma^2(\sqrt[4]{2}) = -\sqrt[4]{2}\ \ \tau\sigma^3(\sqrt[4]{2}) = i\sqrt[4]{2}\\
&\tau(i) = -i\ \ \tau\sigma(i) = -i\ \ \tau\sigma^2(i) = -i\ \ \tau\sigma^3(i) = -i\,.
\end{aligned}$$

Her er $\tau^2 = e$, $\sigma\tau = \tau\sigma^{-1}$.

Ved direkte udregning findes samtlige undergrupper i $\mathrm{Gr}(M/\mathbb{Q})$:



Fra Galoisteoriens hovedsætning ved vi at den indbyrdes placering af dellegemerne i M er som i diagrammet ovenfor. De tilsvarende legemer bliver:



Hvilke af disse legemer er normale over $\mathbb{Q}$?

*Opgave**. Vis, at $M = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ er normal over $\mathbb{Q}$, $[M : \mathbb{Q}] = 8$ og vis, at $\mathrm{Gr}(M/\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

*Opgave**. Lad $f(x)$ være et irreducibelt polynomium i $\mathbb{Q}[X]$ af grad n. Lad antallet r af reelle rødder til $f(x)$ opfylde $0 < r < n$. Lad M være spaltningslegemet for $f(x)$ over $\mathbb{Q}$ (opfattet som dellegeme af de komplekse tals legeme $\mathbb{C}$). Vis, at $L = M \cap \mathbb{R}$ er en ikke-normal udvidelse af $\mathbb{Q}$ og $[L : \mathbb{Q}] \geqq n$.

1) Vis, at $[M : \mathbb{Q}] \geq 2n$.
2) Vis, at $f(x) = x^4 - 2x^3 - 2x + 1$ er irreducibel over $\mathbb{Q}$ (betragt $f(x+1)$).
3) Vis, at antallet af reelle rødder til $f(x)$ er 2.
4) Lad M være spaltningslegemet for $f(x)$ over $\mathbb{Q}$. Bestem $[M : \mathbb{Q}]$ og $\mathrm{Gr}(M/\mathbb{Q})$.

Opgave. Vis, at for spaltningslegemet M for $x^4+x^3+x^2+x+1$ over $\mathbb{Q}$ gælder, at $M/\mathbb{Q}$ er normal og $\mathrm{Gr}(M/\mathbb{Q})$ er cyklisk af orden 4.

*Opgave***. Vis, at $M=\mathbb{Q}(\sqrt{(2-\sqrt{2})(3-\sqrt{3})})$ er normal over $\mathbb{Q}$, og at $\mathrm{Gr}(M/\mathbb{Q})$ er $\cong$ quaterniongruppen af orden 8.

– – – – – – – – – – – – – – – –

Translationssætningen. *Lad M og L være udvidelseslegemer af et legeme K, begge indeholdt i et fælles udvidelseslegeme af K. Antag M/K er endelig normal, medens L kan være en vilkårlig udvidelse af K. Da er kompositet ML normalt over L og $\mathrm{Gr}(ML/L)\simeq\mathrm{Gr}(M/M\cap L)$. Specielt er $[ML:L]=[M:M\cap L]$.*

Endvidere giver tilordningerne $N\to NL$, $(M\cap L\subseteqq N\subseteqq M)$ og $\Lambda\to\Lambda\cap M$, $(L\subseteqq\Lambda\subseteqq ML)$ en $(1-1)$ forbindelse mellem legemerne N mellem $M\cap L$ og M og legemerne Λ mellem L og ML, idet

$$NL\cap M=N \ \ \textit{og} \ \ (\Lambda\cap M)L=\Lambda\,.$$

Bevis. Da M/K er endelig normal, er $M=K(\alpha)$ for passende $\alpha\in M$, og $p(x)=\mathrm{Irr}(\alpha,K)$ er separabelt. $ML=L(\alpha)$ bliver da spaltningslegeme for $p(x)$ over L, hvorfor ML/L er normal.

Legemernes indbyrdes placering illustreres ved:

$$\begin{tikzcd}
M \arrow[r, dash] \arrow[d, dash] & ML \arrow[d, dash] \\
M\cap L \arrow[r, dash] \arrow[d, dash] & L \\
K \arrow[ur, dash] &
\end{tikzcd}$$

Hvis σ er en automorfi i $\mathrm{Gr}(ML/L)$ vil $\sigma_{\mathrm{Res},M}$ være automorfi i $\mathrm{Gr}(M/K)$ (hvorfor?) og afbildningen $\varphi:\mathrm{Gr}(ML/L)\to\mathrm{Gr}(M/K)$ defineret ved $\varphi\sigma=\sigma_{\mathrm{Res},M}$ er en homomorfi. Da σ er entydigt bestemt ved værdien på α, er φ injektiv. $\varphi\,\mathrm{Gr}(ML/L)$ er en undergruppe i $\mathrm{Gr}(M/K)$ og derfor ifølge Galoisteoriens hovedsætning bestemt ved $\mathcal{F}(\varphi\,\mathrm{Gr}(ML/L))$. Ifølge definitionen bliver

$$\begin{aligned}
&\mathcal{F}(\varphi\,\mathrm{Gr}(ML/L)=\{m\in M|\sigma(m)=m\ \forall\sigma\in\mathrm{Gr}(ML/L)\}=\\
&\{m\in M|m\in\mathcal{F}(\mathrm{Gr}(ML/L)=L\}=M\cap L\,.
\end{aligned}$$

Altså bliver $\varphi\,\mathrm{Gr}(ML/L)=\mathrm{Gr}(M/M\cap L)$. Da φ er injektiv fås herved den i translationssætningen nævnte isomorfi. Specielt er $[ML:L]=[M:M\cap L]$.

For at vise sætningens sidste halvdel, skal godtgøres

$$1) \qquad NL \cap M = N \qquad\qquad 2) \qquad (\Lambda \cap M)L = \Lambda\,.$$

ad 1)

$$\begin{tikzcd}
M \arrow[r, dash] \arrow[d, dash] & ML \arrow[d, dash] \\
N \arrow[r, dash] \arrow[d, dash] & NL \arrow[d, dash] \\
M \cap L \arrow[r, dash] \arrow[d, dash] & L \\
K \arrow[ur, dash] &
\end{tikzcd}$$

Det er klart, at $NL \cap M \supseteqq N$. Nu er M/N normal, og idet $ML = M(NL)$ er ifølge sætningens første del: $[ML : NL] = [M : NL \cap M]$. Da $[M : M \cap L] = [ML : L]$ fås herved: $[NL \cap M : M \cap L] = [NL : L]$.

Lad $N = (M \cap L)(\beta)$ for et passende β i N; da er $[N : M \cap L] = \mathrm{Grad}(\mathrm{Irr}(\beta, M \cap L)) \geqq \mathrm{Grad}(\mathrm{Irr}(\beta, L)) = [L(\beta) : L] = [NL : L]$. Heraf: $[N : M \cap L] \geqq [NL \cap M : M \cap L]$. Dette sammenholdt med $NL \cap M \supseteqq N$ giver $[N : M \cap L] = [NL \cap M : M \cap L]$ og dermed $NL \cap M = N$.

ad 2)

$$\begin{tikzcd}
M \arrow[r, dash] \arrow[d, dash] & ML \arrow[d, dash] \\
M \cap \Lambda \arrow[r, dash] \arrow[dd, dash] \arrow[dr, dash] & \Lambda \arrow[d, dash] \\
 & (M \cap \Lambda)L \arrow[d, dash] \\
M \cap L \arrow[r, dash] \arrow[d, dash] & L \\
K \arrow[ur, dash] &
\end{tikzcd}$$

Det er klart, at $\Lambda \supseteqq (M \cap \Lambda)L$. Af beviset for punkt 1) fremgår (med $N = M \cap \Lambda$) at $[(M \cap \Lambda)L : L] = [M \cap \Lambda : M \cap L]$. Ifølge translationssætningens første del er

$$[M : M \cap \Lambda] = [ML : \Lambda] \;\text{ og }\; [M : M \cap L] = [ML : L],$$

og ifølge sætning 9 i kap. II (transitivitetssætningen) fås da

$$[M \cap \Lambda : M \cap L] = [\Lambda : L]$$

Følgelig er $[(M \cap \Lambda)L : L] = [\Lambda : L]$. Sammenholdt med $\Lambda \supseteqq (M \cap \Lambda)L$ fås herved $\Lambda = (M \cap \Lambda)L$.

$\square$

Sætning om kompositet af normale udvidelser. *Lad L og M være endelige normale udvidelser af et legeme K og antag L og M er indeholdt i et fælles legeme. Da er kompositet LM en endelig normal udvidelse af K og Galoisgruppen* $\mathrm{Gr}(LM/K)$ *er isomorf med en undergruppe i det direkte produkt* $\mathrm{Gr}(L/K) \times G(M/K)$. *Der består en isomorfi* $\mathrm{Gr}(LM/K) \simeq \mathrm{Gr}(L/K) \times \mathrm{Gr}(M/K)$ *såfremt* $L \cap M = K$.

Bevis. Ifølge Sætning 6 findes separable polynomier $f(x)$ og $g(x) \in K[X]$ så L (resp. M) er spaltningslegemet over K for $f(x)$ (resp. $g(x)$). Lad $\alpha_1, \ldots, \alpha_s$ (resp. $\beta_1, \ldots, \beta_t$) være rødderne i $f(x)$ (resp. $g(x)$). Da er $LM = K(\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t)$ spaltningslegemet over K for $f(x)g(x)$ og derfor en endelig normal udvidelse af K, (jvf. Sætning 6). Endvidere findes en veldefineret homomorf afbildning $\mathrm{Gr}(LM/K) \mapsto \mathrm{Gr}(L/K) \times \mathrm{Gr}(M/K)$ bestemt ved

$$\sigma \in \mathrm{Gr}(LM/K) \mapsto (\sigma_{\mathrm{res},L}, \sigma_{\mathrm{res},M}) \; .$$

Da σ er entydigt bestemt ved værdierne på $\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t$ vil ovenstående afbildning være injektiv.

Såfremt $L \cap M = K$ giver Translationssætningen, at

$$|\,\mathrm{Gr}(LM/K)| = [LM : K] = [L : K][M : K] = |\,\mathrm{Gr}(L/K) \times \mathrm{Gr}(M/K)|$$

hvorfor den injektive afbildning

$$\mathrm{Gr}(LM/K) \mapsto \mathrm{Gr}(L/K) \times \mathrm{Gr}(M/K)$$

bliver surjektiv og dermed en isomorfi. $\square$

Opgave. Konstruer en endelig normal udvidelse $M/\mathbb{Q}$, hvis Galoisgruppe er $\mathbb{Z}_4 \times \mathbb{Z}_2$

Kapitel IV. Cirkeldelingslegemer og anvendelser heraf

ENHEDSRØDDER OG CIRKELDELINGSPOLYNOMIER.

Vi skal i dette kapitel undersøge en vigtig klasse af normale udvidelser af de rationale tals legeme $\mathbb{Q}$. Historisk var disse de første algebraiske udvidelser af $\mathbb{Q}$, der blev undersøgt mere indgående.

Først et par bemærkninger om enhedsrødder.

De komplekse løsninger til ligningen $x^n = 1$, dvs. $e^{\frac{2\pi i}{n}k}$, $0 \leqq k < n$, kaldes de *n'te enhedsrødder*. Disse udgør en multiplikativ cyklisk gruppe af orden n. En n'te enhedsrod ε kaldes en *primitiv n'te enhedsrod*, hvis den frembringer gruppen af n'te enhedsrødder. Da gælder: En n'te enhedsrod ε er en primitiv n'te enhedsrod $\Leftrightarrow \varepsilon^k \neq 1\,,\ 0 < k < n$. Helt elementært vises

Lemma 1. *Lad ε være en primitiv n'te enhedsrod. Da er følgende betingelser ækvivalente*

1) *ε^k er en primitiv n'te enhedsrod.*
2) *$(k,n) = 1$ (dvs.: k og n indbyrdes primiske).*

Bevis. Simpel øvelse i gruppeteori. □

Specielt er $e^{\frac{2\pi i}{n}k}$, $1 \leq k < n$, $(k,n) = 1$, samtlige primitive n'te enhedsrødder.

Definition. Polynomiet $F_n(x) = \prod_{\substack{1\leq k\leq n \\ (k,n)=1}} \left(x - e^{\frac{2\pi i}{n}k}\right)$ kaldes det *n'te cirkeldelingspolynomium.*

$F_n(x)$ har netop de primitive n'te enhedsrødder som rødder. Graden af $F_n(x)$ er $\varphi(n)$, hvor $\varphi(n)$ er den såkaldte "Eulers φ-funktion", der er defineret som antallet af primiske restklasser modulo n.

Sætning 1. *$F_n(x)$ er et polynomium i $\mathbb{Z}[X]$.*

Vi godtgør først følgende lemma:

Lemma 2. $x^n - 1 = \prod_{d|n} F_d(x)$.

Bevis. Enhver n'te enhedsrod er en primitiv d'te enhedsrod for (netop) én divisor d i n. De to polynomier i lemmaet har derfor de samme rødder og de er alle simple. □

Bevis for sætning 1. Induktion efter n:

For $n = 1$ er udsagnet klart.

Antag $F_m(x) \in \mathbb{Z}[X]$ for alle $m < n$. Ifølge ovenstående lemma er $(x^n - 1) = F_n(x) \cdot \{\prod_{\substack{d|n \\ d<n}} F_d(x)\}$, hvor $\prod_{\substack{d|n \\ d<n}} F_d(x)$ er et normeret heltalspolynomium. Divisionsalgoritmen viser nu, at $F_n(x) \in \mathbb{Z}[X]$. □

Vi giver nu en explicit formel for $F_n(x)$.

Sætning 2. *$F_n(x) = \prod_{d|n}(x^{\frac{n}{d}} - 1)^{\mu(d)}$, hvor μ betegner Möbius funktionen.*

Bevis. Under anvendelse af lemmaet og Sætning 27 i Kap. II fås:

$$\prod_{d|n}(x^{\frac{n}{d}} - 1)^{\mu(d)} = \prod_{d|n}(\prod_{\delta|\frac{n}{d}} F_\delta(x))^{\mu(d)} =$$

$$\prod_{d,\delta,d\cdot\delta|n} F_\delta(x)^{\mu(d)} = \prod_{\delta|n} F_\delta(x)^{\sum_{d|\frac{n}{\delta}} \mu(d)} = F_n(x)\,.$$

□

Da $F_n(x)$ har grad $\varphi(n)$, hvor $\varphi(n)$ er Eulers φ-funktion, fås ved gradsammenligning

Korollar. *$\varphi(n) = \sum_{d|n} \frac{n}{d}\mu(d) = n \cdot \prod_{p|n}(1 - \frac{1}{p})$, hvor p gennemløber de forskellige primdivisorer i n.*

Nogle bemærkninger angående cirkeldelingspolynomiets udseende.

For $n > 2$ har $F_n(x)$ lige grad og konstantleddet er 1.

Koefficenten til næsthøjeste led (dvs. koefficienten til $x^{\varphi(n)-1}$) er lig $-\mu(n)$, idet summen af de primitive n'te enhedsrødder er $\mu(n)$ (jfr. opgave 85 i opgavesamlingen).

Hvis n højest er delelig med to forskellige ulige primtal, er alle koefficienterne i $F_n(x)$ lig 0, 1 eller -1. (Beviset er elementært, men ikke trivielt.)

For $n > 1$ er $F_n(x)$ "reciprokt", dvs. hvis a_i er koefficienten til x^i, da er $a_i = a_{\varphi(n)-i}$ for $0 \le i \le \varphi(n)$.

Hvis p er et primtal, er $F_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + \cdots + x + 1$.

Eksempler. $F_1(x) = x - 1,\ F_2(x) = x + 1,\ F_3(x) = x^2 + x + 1,\ F_4(x) = x^2 + 1,\ F_5(x) = x^4 + x^3 + x^2 + x + 1,\ F_6(x) = x^2 - x + 1,\ F_8(x) = x^4 + 1,\ F_9(x) = x^6 + x^3 + 1,\ F_{10}(x) = x^4 - x^3 + x^2 - x + 1,\ F_{12}(x) = x^4 - x^2 + 1,\ F_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$.

Ved beviset for den efterfølgende sætning får vi brug for følgende

Lemma 3. *Hvis $f(x)$ og $g(x)$ er normerede polynomier i $\mathbb{Q}[X]$ for hvilke $f(x)\cdot g(x) \in \mathbb{Z}[X]$, da vil $f(x) \in \mathbb{Z}[X]$ og $g(x) \in \mathbb{Z}[X]$.*

Bevis. Der findes naturlige tal a og b så $af(x)$ og $bg(x)$ er primitive polynomier i $\mathbb{Z}[X]$. Ifl. Gauss's lemma er produktet $af(x)bg(x) = abf(x)g(x)$ også et primitivt polynomium i $\mathbb{Z}[X]$. Men da må ab være lig $+1$, hvorfor a og b også må være 1. Dette indebærer, at $f(x)$ og $g(x)$ må være polynomier i $\mathbb{Z}[X]$. □

Sætning 3. *$F_n(x)$ er irreducibelt i $\mathbb{Q}[X]$.*

Bevis. Lad $f(x)$ være et normeret irreducibelt polynomium i $\mathbb{Q}[X]$. Vi viser:

1° For en vilkårlig primitiv n'te enhedsrod ε og et vilkårligt primtal p, der ikke går op i n gælder:

$$f(\varepsilon) = 0 \Rightarrow f(\varepsilon^p) = 0.$$

Bevis for 1°: Da $f(x) = \mathrm{Irr}(\varepsilon, \mathbb{Q})$ må $f(x)$ gå op i $x^n - 1$ indenfor $\mathbb{Q}[X]$. På grund af det foregående lemma må $f(x)$ være et polynomium i $\mathbb{Z}[X]$.

Vi betragter nu $g(x) = \mathrm{Irr}(\varepsilon^p, \mathbb{Q})$. Som før ses, at $g(x) \in \mathbb{Z}[X]$. Polynomiet $g(x^p)$ har ε som rod, hvorfor $f(x)|g(x^p)$ indenfor $\mathbb{Q}[X]$ og dermed som før indenfor $\mathbb{Z}[X]$. Vi har altså

$$g(x^p) = f(x) \cdot k(x)\,, \tag{$*$}$$

hvor $k(x) \in \mathbb{Z}[X]$. Antag nu $f(\varepsilon^p) \neq 0$. Da ville $f(x)$ og $g(x)$ være to ikke associerede irreducible polynomier i $\mathbb{Q}[X]$. Begge går op i $x^n - 1$ hvorfor (idet $\mathbb{Q}[X]$ er UFD) $f(x) \cdot g(x)|x^n - 1$ indenfor $\mathbb{Q}[X]$, og dermed som før indenfor $\mathbb{Z}[X]$, dvs.

$$x^n - 1 = f(x) \cdot g(x) \cdot h(x)\,, \tag{$**$}$$

hvor $h(x) \in \mathbb{Z}[X]$.

For de polynomier $\overline{f}(x)$, $\overline{g}(x)$, $\overline{h}(x)$ og $\overline{k}(x)$ i $\mathbb{Z}_p[X]$, der fås ved anvendelse af homomorfien $\mathbb{Z}[X] \to \mathbb{Z}_p[X]$, gælder p.gr. af $(*)$ og $(**)$

$$\overline{g}(x)^p = \overline{f}(x)\,\overline{k}(x)\,, \tag{$***$}$$

$$x^n - ① = \overline{f}(x)\,\overline{g}(x)\,\overline{h}(x)\,, \tag{$****$}$$

idet alment $\overline{g}(x^p) = (\overline{g}(x))^p$ for polynomier i $\mathbb{Z}_p[X]$.

Af $(***)$ ses, at enhver irreducibel faktor $\pi(x)$ i $\overline{f}(x)$ også må forekomme i $\overline{g}(x)$, hvorfor ligningen $(****)$ medfører at $x^n - ①$ (indenfor $\mathbb{Z}_p[X]$) må være delelig med kvadratet på polynomiumet $\pi(x)$, der har grad > 0

$$x^n - ① = \pi(x)^2 \cdot q(x)\,, \;\; \pi(x), q(x) \in \mathbb{Z}_p[X]\,.$$

Ved formel differentiation fås

$$n\, x^{n-1} = \pi(x)[2\pi'(x)q(x) + \pi(x)q'(x)]\,.$$

Da $p\nmid n$ er $ⓝ \neq 0$ i $\mathbb{Z}_p$ dvs.: ⓝ har et inverst $ⓝ^{-1}$ i $\mathbb{Z}_p$ og af ovenstående fås

$$① = \pi(x)\left\{[2\pi'(x)q(x) + \pi(x)q'(x)]\,x \cdot ⓝ^{-1} - \pi(x)q(x)\right\} \in \mathbb{Z}_p[X]\,,$$

hvilket er en modstrid, da $\pi(x)$ har grad > 0.

<u>$2°$</u> Hvis et normeret irreducibelt polynomium $f(x) \in \mathbb{Q}[X]$ har blot én primitiv n'te enhedsrod ε som rod, da vil samtlige primitive n'te enhedsrødder være rødder i $f(x)$.

Bevis for $2°$*:* Enhver primitiv n'te enhedrod har formen ε^k, hvor $(k,n) = 1$. Eksponenten k skrives som produkt af (ens eller forskellige) primfaktorer. Ingen af disse primfaktorer går op i n. Udsagnet $2°$ fås nu ved successiv anvendelse af $1°$.

<u>$3°$</u> $F_n(x)$ er irreducibelt i $\mathbb{Q}[X]$.

Bevis for $3°$*:* Lad ε være en primitiv n'te enhedsrod og lad $f(x) = \mathrm{Irr}(\varepsilon, \mathbb{Q})$. Da vil $f(x)$ være en divisor i $F_n(x)$. Ifølge $2°$ vil samtlige primitive n'te enhedsrødder være rødder i $f(x)$. Dette medfører, at $\mathrm{grad}(f(x)) \geqq \varphi(n) = \mathrm{grad}\, F_n(x)$, hvorfor $F_n(x) = f(x)$, da begge disse polynomier er normerede. Men $f(x)$ er pr. definition irreducibelt og derfor er $F_n(x)$ også irreducibelt. $\square$

— — — — — — — — — — — — — — — —

DIRICHLETS SÆTNING OM PRIMTAL I ARITMETISKE PROGRESSIONER.

Vi gør her en lille digression, hvor vi anvender at $F_n(x) \in \mathbb{Z}[X]$.

Dirichlets berømte sætning om primtal i aritmetiske progressioner udsiger, at for ethvert par (a, n) af indbyrdes primiske naturlige tal findes uendeligt mange primtal, der er $\equiv a \pmod{n}$. Vi viser denne sætning i et vigtigt specialtilfælde:

Dirichlets Sætning for $a = 1$. *For ethvert naturligt tal n findes uendeligt mange primtal, der er $\equiv 1 \pmod{n}$.*

Bevis. Udsagnet "For ethvert naturligt tal n findes et primtal, der er $\equiv 1 \pmod{n}$" medfører udsagnet: "For ethvert naturligt tal n findes uendeligt mange primtal, der er $\equiv 1 \pmod{n}$". (Hvorfor?)

Det er derfor nok at vise, at der til ethvert naturligt tal n findes et primtal der er $\equiv 1 \pmod{n}$.

Vi kan naturligvis antage $n > 2$.

Det ønskede udsagn er en konsekvens af følgende to påstande:

Påstand 1. *For ethvert naturligt tal $n > 2$ er $|F_n(n)| > 1$ og $F_n(n)$ dermed deleligt med mindst et primtal.*

Påstand 2. *Enhver primdivisor p i $F_n(n)$ er $\equiv 1 \pmod{n}$.*

Bevis for påstand 1. Da $F_n(n) = \prod\limits_{\substack{1 \le k < n \\ (k,n)=1}} (n - e^{\frac{2\pi i}{n} k})$ og hver faktor for $n > 2$ har numerisk værdi > 1, fås den ønskede ulighed.

Bevis for påstand 2. Lad p være en primdivisor i $F_n(n)$, hvor $n > 2$. Da $F_n(x)$ har konstantled 1, er $F_n(n) \equiv 1 \pmod n$ og p kan derfor ikke gå op i n.

Som tidligere vist, er $x^n - 1 = \prod_{d|n} F_d(x)$, og ved at sætte $x = n$ ses, at $n^n - 1$ må være delelig med p.

Den gruppeteoretiske orden t af restklassen n modulo p er derfor en divisor i n. Vi hævder, at $t = n$. Antag nemlig $t < n$. Da ville vi have en fremstilling

$$\frac{x^n - 1}{x^t - 1} = F_n(x) \prod_{\delta} F_\delta(x)$$

hvor δ gennemløber de divisorer δ i n for hvilke $\delta < n$ og δ ikke går op i t. Ved at sætte $x = n$ ses, at $F_n(n)$ går op i $\frac{n^n-1}{n^t-1}$. På den anden side viser

$$\frac{n^n - 1}{n^t - 1} = \frac{(n^t)^{\frac{n}{t}} - 1}{n^t - 1} = (n^t)^{\frac{n}{t}-1} + (n^t)^{\frac{n}{t}-2} + \ldots + n^t + 1$$

at

$$\frac{n^n - 1}{n^t - 1} \equiv \underbrace{1 + \cdots + 1}_{\frac{n}{t} \text{ led}} = \frac{n}{t} \pmod p$$

Ved kombination af ovenstående ville man derfor få, at p skulle gå op i $\frac{n}{t}$ og dermed i n, stridende mod vores første observation.

Altså er $t = n$, og eftersom den gruppeteoretiske orden af ethvert element i gruppen $(\mathbb{Z}_p \setminus \{0\}, .)$ er en divisor i $p - 1$ ses, at $p \equiv 1 \pmod n$. $\square$

CIRKELDELINGSLEGEMER.

Vi undersøger nu legemet $\mathbb{Q}_n = \mathbb{Q}\left(e^{\frac{2\pi i}{n}}\right)$, der kaldes det n'*te cirkeldelingslegeme*. $\mathbb{Q}_n$ er spaltningslegemet for $x^n - 1$ over $\mathbb{Q}$, hvorfor $\mathbb{Q}_n/\mathbb{Q}$ er normal. Her er $[\mathbb{Q}_n : \mathbb{Q}] = \operatorname{Grad}\left(\operatorname{Irr}\left(e^{\frac{2\pi i}{n}}, \mathbb{Q}\right)\right) = \operatorname{Grad} F_n(x) = \varphi(n)$. Sæt $\varepsilon = e^{\frac{2\pi i}{n}}$. For en automorfi $\sigma \in \operatorname{Gr}(\mathbb{Q}_n/\mathbb{Q})$ må (ifølge Praktisk Lemma) gælde $\sigma(\varepsilon) = \varepsilon^a$, hvor ε^a er rod i $F_n(x)$, dvs. ε^a er en primitiv n'te enhedsrod, hvorfor $(a, n) = 1$, hvor a er bestemt modulo n. Følgelig fås en veldefineret afbildning:

$$\operatorname{Gr}(\mathbb{Q}_n/\mathbb{Q}) \xrightarrow{\psi} \mathbb{Z}_n^*\,, \quad \text{(hvor } \mathbb{Z}_n^* \text{ er de primiske restklasser modulo } n\text{)}$$

ved

$$\psi(\sigma) = a \text{ (modulo } n\text{), hvis } \sigma(\varepsilon) = \varepsilon^a\,.$$

Da σ er entydigt bestemt ved værdien på ε, er ψ injektiv. Eftersom $|\operatorname{Gr}(\mathbb{Q}_n/\mathbb{Q})| = [\mathbb{Q}_n : \mathbb{Q}] = \varphi(n) = \operatorname{Ord}(\mathbb{Z}_n^*)$, er ψ surjektiv. De primiske restklasser $\mathbb{Z}_n^*$ modulo n udgør en gruppe med multiplikation som komposition. ($\mathbb{Z}_n^*$ er de invertible elementer i $\mathbb{Z}_n$). Endvidere er ψ en homomorfi:

$$\begin{aligned}
&\psi(\sigma_1\sigma_2) \text{ bestemt ved } \sigma_1\sigma_2(\varepsilon) = \varepsilon^{\psi(\sigma_1\sigma_2)} \\
&\sigma_2(\varepsilon) = \varepsilon^{\psi(\sigma_2)}\,;\ \sigma_1(\sigma_2(\varepsilon)) = \sigma_1\left(\varepsilon^{\psi(\sigma_2)}\right) = (\sigma_1(\varepsilon))^{\psi(\sigma_2)} = \\
&\left(\varepsilon^{\psi(\sigma_1)}\right)^{\psi(\sigma_2)} = \varepsilon^{\psi(\sigma_1)\psi(\sigma_2)} \text{ dvs.: } \psi(\sigma_1\sigma_2) = \psi(\sigma_1)\psi(\sigma_2)\,.
\end{aligned}$$

Vi har således vist

Sætning 4. $\operatorname{Gr}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}_n^*$ *(= den multiplikative gruppe af primiske restklasser modulo n).*

Specielt er $\operatorname{Gr}(\mathbb{Q}_n/\mathbb{Q})$ *abelsk.*

Det er klart (iflg. Galoisteoriens hovedsætning) at ethvert dellegeme $K \subseteq \mathbb{Q}_n$ er normalt over $\mathbb{Q}$ med abelsk Galoisgruppe $\operatorname{Gr}(K/\mathbb{Q})$ ($\simeq \operatorname{Gr}(\mathbb{Q}_n/\mathbb{Q})/\operatorname{Gr}(\mathbb{Q}_n/K)$).

En klassisk, (dybtliggende) sætning giver en karakterisering af normale udvidelser af $\mathbb{Q}$ med abelsk Galoisgruppe.

Kronecker–Webers Sætning. *Lad $K/\mathbb{Q}$ være en endelig udvidelse. Da gælder: $K/\mathbb{Q}$ er normal med abelsk Galoisgruppe $\Leftrightarrow K \subseteq \mathbb{Q}_n$ for passende n.*

Vi vil vise denne sætning i det (meget) specielle tilfælde, hvor $\operatorname{Gr}(K/\mathbb{Q})$ er cyklisk af orden 2.

Først et ganske elementært lemma.

Lemma 4. *Lad K være et legeme af karakteristik 0 og L en kvadratisk udvidelse af K, dvs. $[L : K] = 2$.*

i) Da findes et element a i K, så $L = K(\sqrt{a})$.

ii) Hvis $K = \mathbb{Q}$, kan a vælges som et helt rationalt kvadratfrit tal (dvs. $a \in \mathbb{Z}$ og a er ikke deleligt med kvadratet af noget primtal).

Bevis. ad i) For et vilkårligt $\alpha \in L \setminus K$ vil $L = K(\alpha)$. Polynomiet $\operatorname{Irr}(\alpha, K)$ kan skrives $x^2 + k_1x + k_2$, hvor k_1 og k_2 tilhører K. Et brugbart a vil da være diskriminanten $k_1^2 - 4k_2$.

ad ii) Påstanden følger af, at til ethvert rationalt tal $q \neq 0$ findes et rationalt q_1, så qq_1^2 er et helt kvadratfrit tal.

$\square$

Bevis for Kronecker-Webers sætning for kvadratiske udvidelser af $\mathbb{Q}$.

På grund af ovenstående er det nok at vise, at $\mathbb{Q}(\sqrt{a}) \subsetneqq \mathbb{Q}_{4|a|}$ for ethvert kvadratfrit helt tal a. Dette sker i 4 skridt:

1. Vi bemærker først, at $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}_4$ og $\mathbb{Q}(\sqrt{-1}, \sqrt{2}) = \mathbb{Q}(\sqrt{-1}, \sqrt{-2}) = \mathbb{Q}_8$.

2. For et naturligt tal n er $\mathbb{Q}_n$ spaltningslegemet over $\mathbb{Q}$ for polynomiet $x^n - 1$. Ifølge sætning 28 i Kap.II ligger da $\sqrt{disk(x^n - 1)}$ i $\mathbb{Q}_n$. I sætning 32 i Kap. II har vi udregnet denne diskriminant til $n^n(-1)^{\frac{(n-1)(n-2)}{2}}$. Når n er ulige, bliver diskriminanten $(n^{\frac{n-1}{2}})^2 \cdot (-1)^{\frac{n-1}{2}} \cdot n$. Følgelig er $\mathbb{Q}(\sqrt{disk(x^n - 1)}) = \mathbb{Q}(\sqrt{n(-1)^{\frac{n-1}{2}}})$, der bliver

$\mathbb{Q}(\sqrt{n})$, hvis $n \equiv 1 \pmod 4$ og
$\mathbb{Q}(\sqrt{-n})$, hvis $n \equiv 3 \pmod 4$.

3. Når n og m er naturlige tal og n går op i m, da er åbenbart $\mathbb{Q}_n \subsetneqq \mathbb{Q}_m$.

4. For ethvert kvadratfrit tal a gælder $\mathbb{Q}(\sqrt{a}) \subsetneqq \mathbb{Q}_{4|a|}$.
Der er to muligheder: i) a ulige og ii) a lige.
ad i) Vi skelner mellem tilfældet i1), hvor a er positiv og tilfældet i2), hvor a er negativ.
I tilfælde i1) gælder ifl. punkt 2 og punkt 3 for $a \equiv 1$ mod 4, at $\mathbb{Q}(\sqrt{a}) \subsetneqq \mathbb{Q}_a \subsetneqq \mathbb{Q}_{4|a|}$. I tilfælde i1) gælder ifl. punkt 1, punkt 2 og punkt 3 for $a \equiv 3$ mod 4, at $\mathbb{Q}(\sqrt{a}) \subsetneqq \mathbb{Q}(\sqrt{-1}, \sqrt{-a}) \subsetneqq \mathbb{Q}_{4|a|}$.
I tilfælde i2) gælder, at $\mathbb{Q}(\sqrt{a}) \subsetneqq \mathbb{Q}(\sqrt{-1}, \sqrt{|\, a\,|})$. Ifl. punkt 1, punkt 3 og det ovenstående tilfælde i1) gælder da, at $\mathbb{Q}(\sqrt{a}) \subsetneqq \mathbb{Q}_{4|a|}$.

ad ii) Her er $a = 2u$, hvor u er ulige, idet a er kvadratfri. Åbenbart er $\mathbb{Q}(\sqrt{a}) \subsetneqq \mathbb{Q}(\sqrt{2}, \sqrt{u})$, der [ifl. punkt 1, punkt 3 og det ovenstående tilfælde i)], er indeholdt i $\mathbb{Q}_8\mathbb{Q}_{4|u|} \subsetneqq \mathbb{Q}_{4|a|}$.

$\square$

Eksempel Hvis p er et ulige primtal, er Galoisgruppen $\mathrm{Gr}(\mathbb{Q}_p/\mathbb{Q})$ cyklisk af orden $p-1$, da den multiplikative gruppe af de fra 0 forskellige elementer i et endeligt legeme er cyklisk. $\mathrm{Gr}(\mathbb{Q}_p/\mathbb{Q})$ indeholder derfor netop én undergruppe af indeks 2. På grund af Galoisteoriens hovedsætning indeholder $\mathbb{Q}_p$ da netop ét kvadratisk dellegeme. Som det fremgår af ovenstående bevis, bliver dette kvadratiske dellegeme $\mathbb{Q}(\sqrt{p})$ når $p \equiv 1 \pmod 4$ og $\mathbb{Q}(\sqrt{-p})$, når $p \equiv 3 \pmod 4$.

KONSTRUKTION AF REGULÆRE POLYGONER MED PASSER OG LINEAL.

I dette afsnit benytter vi cirkeldelingslegemer til at besvare klassiske problemer, der går helt tilbage til Euklid.

Vi antager, at der er givet en udgangsfigur i den reelle plan, bestående af punkterne $(0,0)$ og $(1,0)$. Et punkt kaldes *konstruerbart*, hvis det kan fås ud fra udgangsfiguren ved successiv anvendelse af følgende operationer:

1) Tegne den rette linie gennem to givne eller allerede konstruerede punkter.
2) Tegne cirklen med et givet eller allerede konstrueret punkt som centrum og afstanden mellem to givne eller allerede konstruerede punkter som radius.
3) Opsøge fællespunkter mellem to konstruerede rette linier, mellem en konstrueret ret linie og en konstrueret cirkel, samt mellem to konstruerede cirkler.

Ved direkte udregning fås let (jvf. B. Jessen: Elementær algebra)

Sætning 5. *Antag en konstruktion successivt giver følgende punkter $P_0(=(0,0))$, $P_1(=(1,0))$, P_2, $P_3, \dots, P_n$, $P_{n+1}, \dots$. Hvis koordinaterne til $P_0, P_1, \dots, P_n$ tilhører et reelt tallegeme K vil P_{n+1}'s koordinater enten tilhøre K eller et tallegeme af formen $K(\sqrt{d})$, hvor d er et positivt reelt tal der ikke er kvadrat af et tal i K.*

Definition. Et komplekst tal $a+ib$ kaldes *konstruerbart*, hvis punktet (a,b) er konstruerbart i henhold til ovenstående definition.

Den ovenstående sætning giver nu:

Sætning 6. *Hvis et komplekst tal z er konstruerbart, findes en følge af kvadratiske udvidelser $K = \mathbb{Q}$, $K_1 = \mathbb{Q}(i)$, $(i = \sqrt{-1})$, $K_2 = K_1(\sqrt{d_1})$, $(d_1 \in K_1)$, $K_3 = K_2(\sqrt{d}_2), (d_2 \in K_2), \dots, K_t = K_{t-1}(\sqrt{d}_{t-1})$, $d_{t-1} \in K_{t-1}$, så $z \in K_t$.*

Idet vi kan antage, at $K_1 \subsetneqq K_2 \subsetneqq K_3$ etc., vil $[K_t : \mathbb{Q}] = 2^t$, hvorfor vi kan slutte:

$$z \text{ konstruerbart tal } \Rightarrow [\mathbb{Q}(z) : \mathbb{Q}] = \text{ potens af } 2\,.$$

Endvidere gælder

Sætning 7. *Mængden af alle konstruerbare tal udgør et tallegeme med kvadratrod. (dvs. afsluttet overfor dannelse af kvadratrødder).*

Bevis. Følger af de sædvanlige kendte konstruktioner ("Fjerdeproportionalkonstruktion" og "Mellemproportionalkonstruktion"). □

Definition. Den regulære n-kant kaldes *konstruerbar*, hvis $e^{\frac{2\pi i}{n}}$ er et konstruerbart tal.

Gauss' sætning. (Disquisitiones Arithmeticae 1801). *Den regulære n-kant er konstruerbar $\Leftrightarrow$ n har formen $n = 2^a \cdot p_1 \cdots p_r$, hvor a er et helt ikke-negativt tal og $p_1, \dots, p_r$ er indbyrdes forskellige ulige primtal, der alle er af formen: (en potens af 2) $+1$.*

Forbemærkning. Hvis 2^k+1 er primtal, må k nødvendigvis være potens af 2. Thi i modsat fald var $k = u \cdot s$, $u =$ ulige tal $u > 1$, og: $2^k+1 = (2^s)^u+1 = (2^s)^u-(-1)^u = (2^s-(-1)).\ ((2^s)^{u-1} + (2^s)^{u-2}(-1) + \cdots + (-1)^{u-1})$. Dvs. 2^s+1 Er en divisor i

$2^k + 1$. Da $u > 1$ er $s < k$, og dermed er $2^s + 1$ *ægte* divisor i $2^k + 1$, som derfor ikke kan være primtal.

Bevis for Gauss' sætning.

Da den regulære n-kant er konstruerbar hvis og kun hvis den regulære $2n$-kant er konstruerbar ("halvering af vinkler") er det nok at vise Gauss' sætning for et ulige tal $n > 1$.

"$\Rightarrow$" Ethvert ulige tal $n > 1$ kan skrives: $n = {p_1}^{a_1} \dots {p_r}^{a_r}$, hvor $p_1, \dots, p_r$ er indbyrdes forskellige ulige primtal og eksponenterne $a_1, \dots, a_r$ er naturlige tal. Nu er ifølge sætning 4 $[\mathbb{Q}(e^{\frac{2\pi i}{n}}) : \mathbb{Q}] = \varphi(n)$, hvor $\varphi(n)$ betegner Eulers φ-funktion. På grund af sætning 6 må $\varphi(n)$ derfor være en potens af 2. Ifølge korollaret til sætning 2 er $\varphi(n) = n \cdot \prod_{p|n}(1 - \frac{1}{p}) = p_1^{a_1 - 1}(p_1 - 1) \cdots p_r^{a_r - 1}(p_r - 1)$.

Hvis dette tal er en potens af 2, må hver af eksponenterne $a_1, \dots, a_r$ være 1, og tallene $p_1 - 1, \dots, p_r - 1$ må være potenser af 2. Men dette betyder netop, at n må have den i Gauss' sætning angivne form.

"$\Leftarrow$" Hvis n har den i sætningen nævnte form, fremgår det af udregningen i den foregående del af beviset, at $[\mathbb{Q}_n : \mathbb{Q}]$ er en potens af 2. Galoisgruppen $G = \mathrm{Gr}(\mathbb{Q}_n/\mathbb{Q})$ er da en abelsk 2-gruppe. Denne er specielt opløselig, så faktorerne i en kompositionsrække $G \supset G_1 \supset G_2 \supset \cdots \supset G_k = \{e\}$ være må være cykliske af orden 2,(jfr. sætning 32 i Kap. 1), dvs. $[G : G_1] = [G_1 : G_2] = \cdots = [G_{k-1} : G_k] = 2$.

Vi har nu følgende situation:

$$
\begin{tikzcd}
G_k = \{e\} \arrow[d, dash, "2"'] & \mathcal{F}(G_k) = \mathbb{Q}_n \arrow[d, dash, "2"] \\
G_{k-1} \arrow[d, dash, "2"'] & \mathcal{F}(G_{k-1}) \arrow[d, dash, "2"] \\
\vdots \arrow[d, dash, "2"'] & \vdots \arrow[d, dash, "2"] \\
G_2 \arrow[d, dash, "2"'] & \mathcal{F}(G_2) \arrow[d, dash, "2"] \\
G_1 \arrow[d, dash, "2"'] & \mathcal{F}(G_1) \arrow[d, dash, "2"] \\
G & \mathcal{F}(G) = \mathbb{Q}
\end{tikzcd}
$$

$\mathcal{F}(G_1)$ er en kvadratisk udvidelse af $\mathcal{F}(G)$ og fås derfor ifl. Lemma 4 ved adjunktion af kvadratroden af et tal i $\mathcal{F}(G)$. Endvidere er $\mathcal{F}(G_2)$ en kvadratisk udvidelse af $\mathcal{F}(G_1)$ og fås derfor ved adjunktion af kvadratroden af et tal tal i $\mathcal{F}(G_1)$ etc.

Da legemet af konstruerbare tal er afsluttet overfor dannelse af kvadratrod (Sætning 7) og de rationale tal er konstruerbare, ses ud fra ovenstående, at $\mathbb{Q}_n$ er indeholdt i legemet af konstruerbare tal. Specielt ligger $e^{\frac{2\pi i}{n}}$ i legemet af konstruerbare tal. $\square$

Bemærkning angående de i Gauss' sætning forekommende primtal. Disse primtal kaldes de *Fermat'ske primtal.* $2^1+1=3$, $2^2+1=5$, $2^4+1=17$, $2^8+1=257$, $2^{16}+1=65537$ er Fermat'ske primtal. Flere Fermat'ske primtal end disse kendes ikke. (Et kriterium for at $2^{2^n}+1$ er et primtal vil komme i Kap. VI.)

Bemærkning angående "vinklens tredeling". Af Gauss' sætning følger specielt, at den regulære 9-kant ikke kan konstrueres ved passer og lineal. Dette giver en negativ løsning på den klassiske opgave, hvorvidt enhver vinkel kan tredeles ved passer og lineal.

EN ANVENDELSE PÅ "GALOISTEORIENS OMVENDINGSPROBLEM".

Vi afslutter dette kapitel med endnu en anvendelse af cirkeldelingslegemer. Det er et berømt problem (gående tilbage til Hilbert (1892)), hvorvidt enhver endelig gruppe kan realiseres som Galoisgruppe for en endelig normal udvidelse af de rationale tals legeme $\mathbb{Q}$. Dette problem, Galoisteoriens omvendingsproblem, er stadig uløst og indtager en central placering i den aktuelle forskning indenfor Galoisteori.

Vi skal her vise, at enhver endelig *abelsk* gruppe kan realiseres som Galoisgruppe over $\mathbb{Q}$.

Hertil får vi brug for følgende

Sætning 8. *Lad m og n være naturlige tal der er indbyrdes primiske. Da gælder for cirkeldelingslegemerne $\mathbb{Q}_m$ og $\mathbb{Q}_n$, at fællesmængden $\mathbb{Q}_m \cap \mathbb{Q}_n = \mathbb{Q}$ og kompositet $\mathbb{Q}_m\,\mathbb{Q}_n = \mathbb{Q}_{nm}$.*

Bevis. Vi viser først, at $\mathbb{Q}_m\mathbb{Q}_n = \mathbb{Q}_{mn}$.

Det er klart, at $\mathbb{Q}_m\mathbb{Q}_n \subseteqq \mathbb{Q}_{mn}$.

For at godtgøre den modsatte inklusion bemærker vi, at for de indbyrdes primiske hele tal m og n findes hele tal a og b så $am+bn=1$, og dermed $\frac{a}{n}+\frac{b}{n}=\frac{1}{mn}$. Derfor er

$$\mathbb{Q}_{mn} = \mathbb{Q}(e^{\frac{2\pi i}{mn}}) = \mathbb{Q}(e^{\frac{2\pi i\, a}{n}} e^{\frac{2\pi i\, b}{m}}) \subseteq \mathbb{Q}_m\mathbb{Q}_n\ .$$

Da m og n er indbyrdes primiske, fremgår det af formlen for Eulers φ-funktion, at $\varphi(mn)=\varphi(m)\varphi(n)$, dvs. $[\mathbb{Q}_m\mathbb{Q}_n:\mathbb{Q}] = [\mathbb{Q}_m:\mathbb{Q}][\mathbb{Q}_n:\mathbb{Q}]$. Af transitivitetssætningen for endelige udvidelser fås derfor $[\mathbb{Q}_m\mathbb{Q}_n:\mathbb{Q}_n] = [\mathbb{Q}_m:\mathbb{Q}]$.

Translationssætningen anvendt på

$$\begin{tikzcd}
\mathbb{Q}_m \arrow[r, dash] \arrow[d, dash] & \mathbb{Q}_{mn} \arrow[d, dash] \\
\mathbb{Q}_m \cap \mathbb{Q}_n \arrow[r, dash] \arrow[d, dash] & \mathbb{Q}_n \\
\mathbb{Q} &
\end{tikzcd}$$

viser nu, at $\mathbb{Q}_m \cap \mathbb{Q}_n = \mathbb{Q}$. $\square$

Sætning 9. *Lad $\mathbb{Z}_n$ være den cykliske gruppe af orden n og lad p være et primtal så $p \equiv 1 \pmod{n}$. Da findes et dellegeme af $\mathbb{Q}_p$ der er normalt over $\mathbb{Q}$ med $\mathbb{Z}_n$ som Galoisgruppe.*

Bevis. Da $\mathrm{Gr}(\mathbb{Q}_p/\mathbb{Q}) \simeq \mathbb{Z}_p^* \simeq (Z_{p-1}, +)$, findes (netop) én undergruppe H i $\mathrm{Gr}(\mathbb{Q}_p/\mathbb{Q})$ af orden $\frac{p-1}{n}$. Fixpunktslegemet $\mathcal{F}(H)$ bliver ifølge Galoisteoriens hovedsætning en normal udvidelse af $\mathbb{Q}$ med $\mathrm{Gr}(\mathbb{Q}_p/\mathbb{Q})/H \simeq \mathbb{Z}_n$ som Galoisgruppe. $\square$

Vi er nu i stand til at vise

Sætning 10. *Enhver endelig abelsk gruppe kan realiseres som Galoisgruppe for en endelig normal udvidelse af $\mathbb{Q}$.*

Bevis. Lad A være en endelig abelsk gruppe. Ifølge en kendt sætning fra Mat 2AL er A et direkte produkt af cykliske grupper

$$A \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_t}$$

Ifølge det tidligere beviste specialtilfælde af Dirichlets sætning om primtal i aritmetiske progressioner, findes indbyrdes forskellige primtal $p_1, \ldots, p_t$, så

$$p_1 \equiv 1 \pmod{n_1}\ ,\ p_2 \equiv 1 \pmod{n_2}, \ldots, p_t \equiv 1 \pmod{n_t}\ .$$

På grund af Sætning 9 findes dellegemer $K_1 \subseteq \mathbb{Q}_{p_1}$, $K_2 \subseteq \mathbb{Q}_{p_2}, \ldots, K_t \subseteq \mathbb{Q}_{p_t}$, der er normale over $\mathbb{Q}$ og

$$\mathrm{Gr}(K_1/\mathbb{Q}) \simeq \mathbb{Z}_{n_1}, \mathrm{Gr}(K_2/\mathbb{Q}) \simeq \mathbb{Z}_{n_2}, \ldots, \mathrm{Gr}(K_t/\mathbb{Q}) \simeq \mathbb{Z}_{n_t}\ .$$

Ved anvendelse af Sætning 8 og sætningen om kompositet af normale udvidelser får vi, at $K_1 K_2 \ldots K_t$ er normal over $\mathbb{Q}$ og

$$\mathrm{Gr}(K_1 K_2 \ldots K_t/\mathbb{Q}) \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_t} \simeq A.$$

$\square$

Kapitel V. Opløselighed ved Rodtegn

En af de ældste opgaver i algebraen var at finde rødder i en ligning. Allerede i oldtiden kendte man løsningerne til en andengradsligning. I renæssancen kendte man - modulo mangel på eksakt kendskab til komplekse tal - løsninger til trediegrads- og fjerdegradsligninger udtrykt ved successiv anvendelse af de fire klassiske regningsarter og roduddragning. (Se nærmere herom senere i dette kapitel.)

I flere århundreder var det et åbent problem at "løse" en ligning af femte eller højere grad. Det første egentlige gennembrud kom fra den italienske læge og matematiker Paulo Ruffini (1765-1822). I 1799 publicerede han værket "Teoria generale delle equazioni" med påstanden om at en femtegradsligning i almindelighed ikke kan løses ved hjælp af rodtegn og de fire klassiske regningsarter. Hans "bevis" indeholdt mange fejl, men de tilgrundliggende ideer var de rigtige. Det var også en bedrift, at han overhovedet - som den første - kom på den tanke, at sådanne ligninger i almindelighed slet ikke kunne løses ved rodtegn. Hans arbejde fik ikke megen response i samtiden. Det første anerkendte bevis for at den "almindelige femtegradsligning" ikke kan løses ved rodtegn skyldes den norske matematiker Niels Henrik Abel (1802-29), der behandlede dette emne i et arbejde ("Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré") fra 1824. (Der har dog været nogen diskussion om hvorvidt hans bevis var helt i orden.)

Først med Galois's arbejder (specielt "Mémoire sur les conditions de résolubilité des équations par radicaux") fik problemet en systematisk og fuldt ud tilfredsstillende behandling. I dette kapitel giver vi en fremstilling heraf, hvor vi dog benytter nyere terminologi og begrebsdannelser.

Vi begynder med nogle abstrakte sætninger, der ved første blik ikke synes at have relation til femtegradsligninger etc.

KRYDSEDE PRODUKTER OG ANVENDELSER HERAF.

Lad G være en gruppe af automorfier for et legeme K.

Definition. En afbildning f af G ind i K^* (den multiplikative gruppe af de fra 0 forskellige elementer i K) kaldes en *krydset homomorfi*, hvis den opfylder betingelsen

$$f(\sigma\tau) = \sigma(f(\tau)) \cdot f(\sigma) \; \forall \sigma, \tau \in G\,.$$

Bemærkning. For enhver krydset homomorfi f gælder $f(e) = 1$. De krydsede homomorfier udgør med multiplikation som kompositionsregel en kommutativ gruppe H.

Hvis a er et element i K^*, er afbildningen fra G til K^* defineret ved $f(\sigma) = \frac{a}{\sigma(a)}$ en krydset homomorfi (eftervises direkte). En krydset homomorfi af ovenstående form kaldes "principal". De principale krydsede homomorfier udgør en undergruppe P i H.

Definition. Faktorgruppen H/P kaldes *den 1'ste kohomologigruppe* for G med koefficienter i K og betegnes $H^1(G, K^*)$.

Sætning 1. *Hvis G er en endelig automorfigruppe, er $H^1(G, K^*) = 1$ dvs.: enhver krydset homomorfi er principal.*

Bevis. Da forskellige automorfier er uafhængige (Sætning 3 i Kap.III) over K findes et $x \in K$ så
$\sum_{\tau \in G} f(\tau)\tau(x) \neq 0$, hvor f er en vilkårlig givet krydset homomorfi. Hvis vi sætter $a = \sum_{\tau \in G} f(\tau)\tau(x)$, er

$$\sigma(a) = \sum_{\tau} \sigma f(\tau)\sigma\tau(x) = \sum_{\tau} \frac{f(\sigma\tau)}{f(\sigma)} \cdot \sigma\tau(x) =$$
$$\frac{1}{f(\sigma)} \sum_{\tau} f(\tau)\tau(x) = \frac{a}{f(\sigma)}\,, \text{ hvoraf } f(\sigma) = \frac{a}{\sigma(a)}$$

dvs.: f er principal. $\square$

Eksempel. Hvis G ikke er endelig, er $H^1(G, K^*)$ ikke nødvendigvis triviel. Et modeksempel er følgende: Lad $K = \mathbb{C}(X)$ og G være gruppen af automorfier i K defineret ved $\sigma\left(\frac{f(x)}{g(x)}\right) = \frac{f(x+1)}{g(x+1)}$, $G = \{\sigma^n | n \in \mathbb{Z}\}$. Vi definerer en krydset homomorfi f fra G ind i K^* ved

$$\begin{aligned} f(\sigma) &= x \\ f(\sigma^n) &= x \cdot \sigma(x) \ldots \sigma^{n-1}(x) \qquad && n > 0 \\ f(\sigma^{-n}) &= \sigma^{-1}\left(\frac{1}{x}\right) \ldots \sigma^{-n}\left(\frac{1}{x}\right) \qquad && n > 0. \end{aligned}$$

Da vil f ikke være principal (hvorfor ?)

Korollar til Sætning 1. ("Hilbert Satz 90") *Lad L/K være endelig normal udvidelse med cyklisk Galoisgruppe* $\mathrm{Gr}(L/K) = \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$. *Hvis $\beta \in L$ og $\prod_{i=0}^{n-1} \sigma^i(\beta) = 1$, da findes $\alpha \in L \setminus \{0\}$ så $\beta = \frac{\alpha}{\sigma(\alpha)}$.*

Bevis. Vi definerer en afbildning f fra $\mathrm{Gr}(L/K)$ ind i L^* ved

$$\begin{aligned} f(e) &= 1 \\ f(\sigma) &= \beta \\ f(\sigma^2) &= \beta\sigma(\beta) \\ f(\sigma^{n-1}) &= \beta\sigma(\beta) \ldots \sigma^{n-2}(\beta)\,. \end{aligned}$$

For afbildningen f gælder: $f(\sigma^j) = \beta \cdot \sigma(\beta) \cdots \sigma^{j-1}(\beta)$ for *alle* $j > 0$ (hvorfor ?). f er en krydset homomorfi; thi

$$f(\sigma^i \sigma^j) = \beta\, \sigma(\beta) \ldots \sigma^{i+j-1}(\beta)$$
$$\sigma^i f(\sigma^j) f(\sigma^i) = [\sigma^i \beta \cdot \sigma^{i+1}(\beta) \ldots \sigma^{i+j+1}(\beta)] \cdot [\beta \cdot \sigma(\beta) \ldots \sigma^{i-1}(\beta)]\,.$$

Ifølge sætning 1 er f principal dvs.: $\exists\, \alpha \in L \setminus \{0\}$ så

$$f(\sigma^i) = \frac{\alpha}{\sigma^i(\alpha)} \forall i, \quad \text{specielt er}$$
$$\beta = f(\sigma) = \frac{\alpha}{\sigma(\alpha)}\,.$$

□

Inden vi bringer den for os vigtigste anvendelse af ovenstående, giver vi nogle almene sætninger angående Galoisgrupper for binomier (dvs. polynomier af formen $x^n - a$).

Lad K være et legeme af karakteristik 0 og lad n være et naturligt tal. Antag K indeholder de n'te enhedsrødder, (dvs.: $\mathbb{Q}_n \subseteq K$).

Sætning 2. *Under ovenstående forudsætninger gælder: Hvis M er spaltningslegemet for $x^n - a$, ($a \in K$), over K, da er M/K normal og Galoisgruppen* $\mathrm{Gr}(M/K)$ *er cyklisk af en orden, der er divisor i n.*

Bevis. Tilfældet $a = 0$ er trivielt, så vi kan antage, at a er $\neq 0$. Hvis ε betegner en primitiv n'te enhedsrod og β er en rod til $x^n - a$, da er samtlige rødder til $x^n - a$ netop $\beta, \beta\varepsilon, \beta\varepsilon^2, \ldots, \beta\varepsilon^{n-1}$ dvs.: $x^n - a =$ $(x-\beta)(x-\beta\varepsilon)\cdots(x-\beta\varepsilon^{n-1})$ (indbyrdes forskellige rødder). Følgelig er $M = K(\beta)$.

Lad $\sigma \in \mathrm{Gr}(M/K)$, $\sigma(\beta) = \beta \cdot \varepsilon^i$, $0 \leqq i < n$. Vi definerer afbildningen φ fra $\mathrm{Gr}(M/K)$ over i den cykliske gruppe af n'te enhedsrødder ved: $\varphi(\sigma) = \frac{\beta}{\sigma(\beta)}$.

Da σ er entydigt bestemt ved værdien på β, er φ injektiv. φ er en homomorfi:

$$\varphi(\sigma\tau) = \frac{\beta}{\sigma\tau(\beta)} = \frac{\beta}{\sigma(\beta)} \cdot \frac{\sigma(\beta)}{\sigma\tau(\beta)}\,.$$

Da $\frac{\beta}{\tau(\beta)} = n$'te enhedsrod $\in K$ er $\sigma\left(\frac{\beta}{\tau(\beta)}\right) = \frac{\beta}{\tau(\beta)}$:

$$\varphi(\sigma\tau) = \frac{\beta}{\sigma(\beta)} \frac{\beta}{\tau(\beta)} = \varphi(\sigma)\varphi(\tau)\,.$$

Altså er $\mathrm{Gr}(M/K)$ isomorf med en undergruppe i gruppen af n'te enhedsrødder. Dvs.: $\mathrm{Gr}(M/K)$ er cyklisk og $|\,\mathrm{Gr}(M/K)|$ er divisor i n. □

Sætning 3. *Lad p være et primtal og K et legeme af karakteristik 0 indeholdende de p'te enhedsrødder. For et vilkårligt $a \in K$ gælder: $x^p - a$ er enten irreducibelt i $K[X]$ eller produkt af førstegradsfaktorer inden for $K[X]$.*

Bevis. Vi kan antage $a \neq 0$. Spaltningslegemet M for $x^p - a$ over K fås ved at adjungere en rod β til $x^p - a$. Altså er $M = K(\beta)$. Da er ifølge foregående sætning $[M : K]$ en divisor i p, dvs.: $[M : K] = 1$ eller $[M : K] = p$. Hvis $[M : K] = 1$ ligger β og dermed samtlige rødder til $x^p - a$ i K. I tilfældet $[M : K] = p$ bemærker vi, at $\mathrm{Irr}(\beta, K) | x^p - a$. Da $\mathrm{Grad}(\mathrm{Irr}(\beta, K)) = \mathrm{Grad}(x^p - a)$, vil $x^p - a = \mathrm{Irr}(\beta, K)$, dvs.: $x^p - a$ er irreducibelt. $\square$

Den efterfølgende sætning kan betragtes som en art omvending af sætning 2.

Sætning 4. *Lad K være legeme af karakteristik 0 og n et naturligt tal. Antag K indeholder alle n'te enhedsrødder. Hvis M/K er en endelig normal udvidelse med cyklisk Galoisgruppe af orden n, da er $M = K(\beta)$ for passende $\beta \in M$, hvor $\beta^n =$ element i K.*

Bevis. Lad $\mathrm{Gr}(M/K) = \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ og lad ε være primitiv n'te enhedsrod. $\varepsilon \in K$ og $\prod_{i=0}^{n-1} \sigma^i(\varepsilon) = \varepsilon^n = 1$. Ifølge korollaret til Sætning 1 findes $\beta \in M$ så $\frac{\beta}{\sigma(\beta)} = \varepsilon$. Da gælder

$$\begin{aligned} \sigma(\beta) &= \beta\varepsilon^{-1} \\ \sigma^2(\beta) &= \beta\varepsilon^{-2} \\ &\cdots \\ &\cdots \\ \sigma^{n-1}(\beta) &= \beta\varepsilon^{-(n-1)} \end{aligned}$$

$$\begin{tikzcd} M \arrow[r, dash] \arrow[d, dash] & \{e\} \arrow[d, dash] \\ K(\beta) \arrow[r, dash] \arrow[d, dash] & TK(\beta) \arrow[d, dash] \\ K \arrow[r, dash] & Gr(M/K) \end{tikzcd}$$

$$\begin{aligned} TK(\beta) &= \{\tau \in \mathrm{Gr}(M/K) | \tau\beta = \beta\} = \{e\} \\ K(\beta) &= \mathcal{F}(T(K(\beta))) = \mathcal{F}(\{e\}) = M \end{aligned}$$

$\sigma(\beta^n) = \beta^n$ dvs.: $\beta^n =$ element i K. $\square$

Opgave. Lad $L = \mathbb{Q}(\sqrt[p]{2}, \varepsilon)$, hvor p er ulige primtal og ε er primitiv p'te enhedsrod.

1) Find $[L : \mathbb{Q}]$.

2) Vis, at $L/\mathbb{Q}$ er normal med ikke-abelsk Galoisgruppe.

3) Lad α være et tal i L, så $L = \mathbb{Q}(\alpha, \varepsilon)$, hvor $\alpha^p \in \mathbb{Q}(\varepsilon)$.

Vis, at $\alpha^p = \beta^p \cdot 2^t$, $1 \leq t \leq p-1$, $\beta \in \mathbb{Q}(\varepsilon)$. (*Vink:* skriv α som $\mathbb{Q}(\varepsilon)$-lineærkombination af $1, \sqrt[p]{2}, \ldots, (\sqrt[p]{2})^{p-1}$ og anvend automorfien $\sigma \in \mathrm{Gr}(L/\mathbb{Q}(\varepsilon))$ bestemt ved $\sigma(\sqrt[p]{2}) = \varepsilon \sqrt[p]{2}$.

4) For hvilke $a \in \mathbb{Q}$ er L spaltningslegemet (over $\mathbb{Q}$) for $x^p - a$?

RADIKALUDVIDELSER.

I resten af dette kapitel betragter vi kun legemer af karakteristik 0. En udvidelse M/K kaldes *abelsk* (resp. *cyklisk*), hvis M/K er normal med abelsk (resp. cyklisk) Galoisgruppe.

DEFINITION. En udvidelse kaldes en *radikaludvidelse*, hvis man kan indskyde mellemlegemer $K_0 = K$, $K_1, K_2, \ldots, K_t = M$ så

$$\begin{array}{llll} K_1 = K_0(\alpha_1) & {\alpha_1}^{n_1} \in K_0 & \text{for passende naturligt tal} & n_1\,, \\ K_2 = K_1(\alpha_2) & {\alpha_2}^{n_2} \in K_1 & \text{for passende naturligt tal} & n_2\,, \\ & \cdots\cdots & & \\ K_t = K_{t-1}(\alpha_t) & {\alpha_t}^{n_t} \in K_{t-1} & \text{for passende naturligt tal} & n_t\,. \end{array}$$

Motiveringen for ovenstående definition er følgende: Når vi vil udtrykke at rødderne i et polynomium f.eks. i $\mathbb{Q}[X]$ ikke kan fås ved anvendelse af de fire klassiske regneoperationer og roduddragning, er vi nødt til at formalisere sådanne procedurer. I ovenstående definition fås hvert legeme K_i ved at adjungere en rod $\sqrt[n_i]{a_i}$,$(a_i = {\alpha_i}^{n_i} \in K_{i-1})$. At et tal ligger i en radikaludvidelse, hvor f.eks. $K_0 = \mathbb{Q}$, betyder netop at det kan fås ved at starte med elementer(tal) i grundlegemet ($\mathbb{Q}$) og udføre en endelig følge af de rationale (klassiske) regneoperationer og løsninger af ligninger af formen $x^n = a$.

DEFINITION. En udvidelse M/K kaldes *meta-abelsk*, hvis man kan indskyde mellemlegemer $K_0 = K, K_1, K_2, \ldots, K_t$ så K_1/K_0, $K_2/K_1, \ldots, K_t/K_{t-1}$ er abelske.

Sætning 5. *Enhver radikaludvidelse kan indlejres i en meta-abelsk udvidelse.*

Bevis. Lad M/K være radikaludvidelse.

Da findes $K_1, K_2, \dots, K_t = M$ så $K_i = K_{i-1}(\alpha_i)$ $\;\alpha_i{}^{n_i} \in K_{i-1}$, $i = 1, 2, \dots, t$. $(K_0 = K)$.

Lad $n = n_1 n_2 \dots n_t$, og lad ε være en primitiv n'te enhedsrod.

Vi har da følgende diagram af legemer:

$$\begin{tikzcd}
M = K_t \arrow[r, dash] \arrow[d, dash] & K_t(\varepsilon) \arrow[d, dash] \\
K_{t-1} \arrow[r, dash] \arrow[d, dash, dotted] & K_{t-1}(\varepsilon) \arrow[d, dash, dotted] \\
K_1 \arrow[r, dash] \arrow[d, dash] & K_1(\varepsilon) \arrow[d, dash] \\
K = K_0 \arrow[r, dash] & K(\varepsilon)
\end{tikzcd}$$

Da gælder $K_i(\varepsilon) = K_{i-1}(\varepsilon)(\alpha_i)$, $\alpha_i{}^{n_i} \in K_{i-1}(\varepsilon)$. Da $K_{i-1}(\varepsilon)$ indeholder de n'te enhedsrødder, er $K_i(\varepsilon)$ spaltningslegemet for $x^{n_i} - \alpha_i{}^{n_i}$ over $K_{i-1}(\varepsilon)$, og derfor er ifølge Sætning 2 $K_i(\varepsilon)/K_{i-1}(\varepsilon)$ normal med cyklisk Galoisgruppe. $(i = 1, 2, \dots, t)$.

Da K har karakteristik 0, indeholder K de rationale tals legeme $\mathbb{Q}$. Vi har følgende diagram:

$$\begin{tikzcd}
\mathbb{Q}(\varepsilon) \arrow[r, dash] \arrow[d, dash] & K(\varepsilon) \arrow[d, dash] \\
K \cap \mathbb{Q}(\varepsilon) \arrow[r, dash] & K
\end{tikzcd}$$

Ifølge translationssætningen er $K(\varepsilon)/K$ normal med en Galoisgruppe, der er isomorf med $\mathrm{Gr}(\mathbb{Q}(\varepsilon)/K \cap \mathbb{Q}(\varepsilon))$ dvs.: $K(\varepsilon)/K$ er abelsk.

$K_t(\varepsilon)/K$ er derfor en meta-abelsk udvidelse indeholdende M. $\square$

Sætning 6. *Lad $L \supseteq K$ og $M \supseteq K$ være to meta-abelske udvidelser indeholdt i et fælles legeme. Da er kompositet LM en meta-abelsk udvidelse af K.*

Bevis. Lad $L = L_t \supset L_{t-1} \supset \cdots \supset L_0 = K$ og $M = M_s \supset M_{s-1} \supset \cdots \supset M_0 = K$ være mellemlegemer så L_i/L_{i-1} og M_j/M_{j-1} er abelske. Vi har nu følgende diagram:

$$\begin{tikzcd}
L \arrow[rrr, dash] \arrow[d, dash] & & & LM \arrow[d, dash] \\
L_{t-1} \arrow[rrr, dash] \arrow[d, dotted, dash] & & & L_{t-1}M \arrow[d, dotted, dash] \\
L_1 \arrow[rrr, dash] \arrow[dddd, dash] & & & L_1M \arrow[d, dash] \\
& & & M \arrow[dl, dash] \\
& & M_{s-1} \arrow[dl, dotted, dash] & \\
& M_1 \arrow[dl, dash] & & \\
K & & &
\end{tikzcd}$$

På grund af translationssætningen er $L_iM/L_{i-1}M$ abelske, hvorfor LM ifølge ovenstående diagram er en meta-abelsk udvidelse af K. $\square$

Sætning 7. *Enhver meta-abelsk udvidelse L/K kan indlejres i en normal meta-abelsk udvidelse.*

Bevis. Ifølge Abel-Steinitz' sætning kan L skrives $K(\alpha)$. (Da legemerne i dette afsnit har karakteristik 0, er L/K en separabel udvidelse.) Hvis M er spaltningslegemet over K for $f(x) = \mathrm{Irr}(\alpha, K)$, da er M en normal udvidelse af K indeholdende L. Lad $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ være rødderne i $f(x)$. Da vil $M = K(\alpha_1, \ldots, \alpha_n)$ være kompositet af legemerne $K(\alpha_1), \ldots, K(\alpha_n)$.

For hvert af legemerne $K(\alpha_i), 1 \leqq i \leqq n$, findes ifølge sætning 13 i Kap.II en isomorfi fra $L = K(\alpha_1)$ paa $K(\alpha_i)$, hvis restriktion til K er identiteten. Da L/K er metaabelsk, er også $K(\alpha_i)/K, 1 \leqq i \leqq n$, metaabelsk. Ifølge Sætning 6 er kompositet af disse legemer metaabelsk. Men dette kompositum er netop M, der således er en normal meta-abelsk udvidelse af K indeholdende L. $\square$

Korollar. *Enhver radikaludvidelse kan indlejres i en normal meta-abelsk udvidelse.*

Definition. $f(x)$ irreducibelt polynomium i $K[X]$. $f(x)$ siges at være *opløseligt ved rodtegn*, hvis der findes en radikaludvidelse af K, hvori $f(x)$ har en rod.

Hovedsætning angående opløselighed ved rodtegn. *Lad $f(x)$ være et irreducibelt polynomium i $K[X]$, og lad M være spaltningslegemet for $f(x)$ over K. Da gælder: $f(x)$ er opløseligt ved rodtegn* $\Leftrightarrow \mathrm{Gr}(M/K)$ *er opløselig.*

Bevis. "$\Rightarrow$" $f(x)$ har (mindst) en rod i en passende radikaludvidelse L af K. Ifølge Korollaret findes en normal meta-abelsk udvidelse $\widetilde{M}$ af K så $\widetilde{M} \supseteqq L$. Da $f(x)$ har en rod i $\widetilde{M}$ og $\widetilde{M}/K$ er normal, spaltes $f(x)$ til bunds i førstegradsfaktorer inden for $\widetilde{M}$ (jvf. Sætning 8 i Kapitel 3), dvs.: $\widetilde{M} \supseteqq M$.

Vi indskyder her

Lemma. *Lad M/K være en endelig normal udvidelse. Da gælder:*

$$M/K \quad \textit{meta-abelsk} \ \Leftrightarrow \mathrm{Gr}(M/K) \quad \textit{opløselig}\,.$$

Bevis for Lemma. "$\Rightarrow$"

Da M/K er metaabelsk, findes mellemlegemer $K_0 = K, K_1, ..., K_t$, så $K_1/K_0, ..., K_t/K_{t-1}$ er abelske:

$$\begin{tikzcd}
M = K_t \arrow[r, dash] \arrow[d, dash] & TK_t = \{e\} \arrow[d, dash] \\
K_{t-1} \arrow[r, dash] \arrow[d, dotted, dash] & TK_{t-1} \arrow[d, dotted, dash] \\
K_1 \arrow[r, dash] \arrow[d, dash] & TK_1 \arrow[d, dash] \\
K \arrow[r, dash] & TK = Gr(M/K)
\end{tikzcd}$$

Da K_i/K_{i-1} er abelsk, er TK_{i-1}/TK_i abelsk, hvorfor $Gr(M/K)$ har en normalrække med abelske faktorer og dermed er opløselig.

"$\Leftarrow$"

Da $Gr(M/K)$ er opløselig, findes en normalrække med $G \supset G_1 \supset \cdots \supset G_{t-1} \supset$

$G_t = \{e\}$ med abelske faktorer:

$$\begin{tikzcd}[arrows=dash]
M = \mathcal{F}(G_t) \arrow[r] \arrow[d] & G_t = \{e\} \arrow[d] \\
K_{t-1} = \mathcal{F}(G_{t-1}) \arrow[r] \arrow[d, dotted] & G_{t-1} \arrow[d, dotted] \\
K_1 = \mathcal{F}(G_1) \arrow[r] \arrow[d] & G_1 \arrow[d] \\
K \arrow[r] & G = Gr(M/K)
\end{tikzcd}$$

For den tilsvarende følge af fixpunktslegemer $K = \mathcal{F}(Gr(M/K)) \subset K_1 = \mathcal{F}(G_1) \subset \cdots \subset K_{t-1} = \mathcal{F}(G_{t-1}) \subset M = \mathcal{F}(\{e\})$, vil hvert legeme være en abelsk udvidelse af det foregående, hvorfor M/K er metaabelsk. $\square$

Nu tilbage til beviset for "$\Rightarrow$" fra Hovedsætningen. Ifølge ovenstående lemma er $\mathrm{Gr}(\widetilde{M}/K)$ opløselig; ifølge Galoisteoriens Hovedsætning er $\mathrm{Gr}(M/K)$ et homomorft billede af $\mathrm{Gr}(\widetilde{M}/K)$ og derfor (jvf. Sætning 29 i Kapitel 1) selv opløselig.

"$\Leftarrow$" Vi antager nu at $\mathrm{Gr}(M/K)$ er opløselig. Lad $n = [M : K]$ og lad ε være en primitiv n'te enhedsrod. Ifølge translationssætningen anvendt på

$$\begin{tikzcd}[arrows=dash]
M \arrow[r] \arrow[d] & M(\varepsilon) \arrow[d] \\
M \cap K(\varepsilon) \arrow[r] \arrow[d] & K(\varepsilon) \arrow[dl] \\
K &
\end{tikzcd}$$

er $\mathrm{Gr}(M(\varepsilon)/K(\varepsilon))$ isomorf med en undergruppe i $\mathrm{Gr}(M/K)$ og derfor (Sætning 29 i Kapitel I) opløselig. $\mathrm{Gr}(M(\varepsilon)/K(\varepsilon))$ indeholder da en normalrække med cykliske faktorer (betragt f.eks. en kompositionsrække, hvorved man endda kan opnå at faktorerne får primtalsorden, jfr. Sætning 32 i Kapitel I.) $G = \mathrm{Gr}(M(\varepsilon)/K(\varepsilon)) \supset G_1 \supset$

$G_2 \supset \cdots \supset G_{t-1} \supset (e) = G_t$

$$\begin{tikzcd}
M(\varepsilon) \arrow[r, dash] \arrow[d, dash] & G_t = \{e\} \arrow[d, dash] \\
\mathcal{F}(G_{t-1}) \arrow[r, dash] \arrow[d, dash, dotted] & G_{t-1} \arrow[d, dash, dotted] \\
\mathcal{F}(G_1) \arrow[r, dash] \arrow[d, dash] & G_1 \arrow[d, dash] \\
K(\varepsilon) \arrow[r, dash] & G = Gr(M(\varepsilon)/K(\varepsilon))
\end{tikzcd}$$

$\mathcal{F}(G_i)/\mathcal{F}(G_{i-1})$ er cyklisk af orden lig divisor i n. Da $\mathcal{F}(G_{i-1})$ indeholder alle n'te enhedsrødder findes (Sætning 4) et $\beta_i \in \mathcal{F}(G_i)$ så $\mathcal{F}(G_i) = \mathcal{F}(G_{i-1})\ (\beta_i)$, hvor ${\beta_i}^{n_i} \in \mathcal{F}(G_{i-1})$ og $n_i = [\mathcal{F}(G_i) : \mathcal{F}(G_{i-1})]$. $M(\varepsilon)/K(\varepsilon)$ er derfor en radikaludvidelse. Da $\varepsilon^n = 1$, bliver $M(\varepsilon)/K$ en radikaludvidelse, hvori $f(x)$ har en rod (endda samtlige rødder). $\square$

— — — — — — — — — — — — — — — —

EKSPLICITTE EKSEMPLER.

Vi betragter i det følgende polynomier med koefficienter i et legeme K af karakteristik 0, som vi antager er et dellegeme af de komplekse tals legeme $\mathbb{C}$. Lad $f(x)$ være et irreducibelt polynomium i $K[X]$ af grad n. Lad M være spaltningslegemet for $f(x)$ over K. Da er (Sætning 12 i Kapitel 3) $\mathrm{Gr}(M/K)$ isomorf med en undergruppe i S_n. Derfor er $f(x)$ opløseligt ved rodtegn for $n \leqq 4$.

For $n = 2$ er dette et klassisk resultat.

For $n = 3$ haves Cardanos formel, som vi nu skal beskrive.

Vi bemærker her først alment, at for løsningen af et n'te gradspolynomium kan man antage, at koefficienten til x^{n-1} forsvinder.

Betragt nemlig et n'te gradspolynomium

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n$$

Ved substitutionen $x \to x - a_1/n$ vil $f(x)$ gå over i et polynomium, hvor koefficienten til x^{n-1} bliver 0.

Ved løsning af en trediegradsligning $f(x) = 0$, kan $f(x)$ derfor antages at have formen $x^3 + px + q$. For rødderne heri haves Cardanos formel, der udtrykker disse som

$$\sqrt[3]{-\tfrac{q}{2}+\sqrt{\tfrac{q^2}{4}+\tfrac{p^3}{27}}}+\sqrt[3]{-\tfrac{q}{2}-\sqrt{\tfrac{q^2}{4}+\tfrac{p^3}{27}}}$$

forstået på følgende måde: Lad u og v være valgt, så $u^3 = -\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$ og $v^3 = -\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$ og $uv = -\frac{p}{3}$. Dette er altid muligt: Thi hvis u og v har de nævnte 3-de potenser, da vil $u \cdot v$ være et af tallene $-\frac{p}{3}$, $\varepsilon(-\frac{p}{3})$ eller $\varepsilon^2(-\frac{p}{3})$, hvor ε er en primitiv tredie enhedsrod. Ved i givet fald at erstatte u med $u\varepsilon^2$ eller $u\varepsilon$ kan man opnå, at produktet bliver $-\frac{p}{3}$.

Når u og v er valgt så ovenstående gælder, bliver rødderne til den givne trediegradsligning netop $u+v$, $u\varepsilon+v\varepsilon^2$, $u\varepsilon^2+v\varepsilon$, hvor ε er en primitiv tredie enhedsrod.

Rigtigheden heraf følger af, at $f(x)$ kan skrives:

$$f(x) = x^3+px+q = [x-(u+v)][x-(u\varepsilon+v\varepsilon^2)][x-(u\varepsilon^2+v\varepsilon)]$$

Eksempel 1. Trediegradsligningen $x^3+3x+2=0$ har én reel rod og to komplekst konjugerede rødder, da diskriminanten $-4\cdot 3^3-27\cdot 2^2=-216$ er negativ (jfr. Sætning 29 i Kap.II). Den reelle rod er $\sqrt[3]{-1+\sqrt{2}}+\sqrt[3]{-1-\sqrt{2}}$ og de to komplekse rødder er $\sqrt[3]{-1+\sqrt{2}}\cdot\varepsilon+\sqrt[3]{-1-\sqrt{2}}\cdot\varepsilon^2$ og $\sqrt[3]{-1+\sqrt{2}}\cdot\varepsilon^2+\sqrt[3]{-1-\sqrt{2}}\cdot\varepsilon$, hvor ε betegner en primitiv tredie enhedsrod, f.eks. $(-1+i\sqrt{3})/2$. (Galoisgruppen for det tilsvarende spaltningslegeme over $\mathbb{Q}$ er den symmetriske gruppe S_3.)

Eksempel 2. Diskriminanten for x^3-3x+1 er 81, så polynomiet har tre reelle rødder (jfr. Sætning 29 i kap.II). Disse er $2\cos\frac{2\pi}{9}$, $2\cos\frac{8\pi}{9}$ og $2\cos\frac{14\pi}{9}$. x Galoisgruppen for det tilsvarende spaltningslegeme over $\mathbb{Q}$ er den alternerende gruppe A_3 ($\simeq$ den cykliske gruppe af orden 3). Dette spaltningslegeme er iøvrigt $\mathbb{Q}_9\cap\mathbb{R}$, dvs. de i det niende cirkeldelingslegeme $\mathbb{Q}_9$ liggende reelle tal.(Hvorfor?)

For $n=4$ kan $f(x)$ antages at have formen x^4+px^2+qx+r. Vi kan antage $q\neq 0$, da $f(x)$ ellers er et andengradspolynomium i x^2. $f(x)$ omskrives

$$f(x) = (x^2+u)^2-[(2u-p)x^2-qx-(r-u^2)],$$

hvor u vælges så andengradspolynomiet i den kantede parentes bliver et fuldstændigt kvadrat, dvs. diskriminanten forsvinder:

$$q^2-4(2u-p)(u^2-r)=0.$$

Dette giver en trediegradsligning i u. Da $q\neq 0$ må en rod u i denne trediegradsligning være $\neq p/2$. For en sådan rod u gælder:

$$f(x) = (x^2+u)^2-(2u-p)(x-\frac{q}{2(2u-p)})^2$$

og hermed

$$f(x) = \{(x^2+u) + \sqrt{2u-p}\cdot(x - \frac{q}{2(2u-p)})\}\{(x^2+u) - \sqrt{2u-p}\cdot(x - \frac{q}{2(2u-p)})\}$$

Rødddderne til $f(x)$ fås nu som rødderne i to andengradspolynomier.

EKSEMPEL 3. Lad os anvende ovenstående på polynomiet $f(x) = x^4 + 4x - 6$. Man føres til at finde et u, så $u^3 + 6u - 2 = 0$. Ved Cardanos formel findes $\sqrt[3]{4} - \sqrt[3]{2}$ at være et brugbart u. Man når da frem til omskrivningen:

$$f(x) = [x^2 - \sqrt{2u}x + u + \frac{\sqrt{2u}}{u}][x^2 + \sqrt{2u}x + u - \frac{\sqrt{2u}}{u}]$$

der umiddelbart tillader bestemmelse af følgende eksplicitte udtryk for rødderne til $f(x)$:

$$\sqrt{\frac{u}{2}} \pm \sqrt{-\frac{u}{2} - \sqrt{\frac{2}{u}}} \quad \text{og} \quad -\sqrt{\frac{u}{2}} \pm \sqrt{-\frac{u}{2} + \sqrt{\frac{2}{u}}},$$

hvor $u = \sqrt[3]{4} - \sqrt[3]{2}$.

(Hvad bliver mon Galoisgruppen for spaltningslegemet for $f(x)$ over $\mathbb{Q}$?)

POLYNOMIER AF GRAD $\geqq 5$.

Vi får brug et gruppeteoretisk resultat.

Lemma. *Lad p være et primtal, og $\mathfrak{p}$ en transitiv undergruppe i den symmetriske gruppe S_p. Hvis $\mathfrak{p}$ indeholder en transposition, er $\mathfrak{p} = S_p$.*

Bevis. I mængden $\{1, 2, \dots, p\}$ indføres en ækvivalensrelation ved $a \sim b$ hvis $a = b$ eller transpositionen $\begin{pmatrix} a & b \\ b & a \end{pmatrix} \in \mathfrak{p}$. Hvis $a \sim b$, og $\tau \in \mathfrak{p}$ gælder $\tau a \sim \tau b$, idet $\begin{pmatrix} \tau a & \tau b \\ \tau b & \tau a \end{pmatrix} = \tau \begin{pmatrix} a & b \\ b & a \end{pmatrix} \tau^{-1}$. Lad nu $S = \{a_1, \dots, a_s\}$ og $T = \{b_1, \dots, b_t\}$ være to ækvivalensklasser. Da $\mathfrak{p}$ er transitiv, findes et $\sigma \in \mathfrak{p}$, så $\sigma(a_1) = b_1$. Derfor vil $b_1 = \sigma(a_1), \sigma(a_2), \dots, \sigma(a_s)$ alle ligge i ækvivalensklassen T. Specielt er $s \leqq t$. Ganske analogt fås $t \leqq s$. Altsaa er $s = t$. Alle ækvivalensklasser har derfor lige mange elementer. Dette indebærer, at $p =$ (antal ækvivalensklasser) $\cdot$ (det fælles elementantal i ækvivalensklasserne).

Da $\mathfrak{p}$ indeholder en transposition, må den sidste faktor i ovenstående være $\geqq 2$. Eftersom p er et primtal, må denne sidste faktor være lig p. Altså findes netop én ækvivalensklasse, og $\mathfrak{p}$ indeholder således samtlige transpositioner, hvorfor $\mathfrak{p} = S_p$.$\square$

Sætning 8. *Lad $f(x)$ være et irreducibelt polynomium i $\mathbb{Q}[X]$ af grad p, hvor p er et primtal. Hvis $f(x)$ har eksakt $(p-2)$ reelle rødder, gælder for spaltningslegemet M, at* $\mathrm{Gr}(M/\mathbb{Q})$ *er isomorf med den symmetriske gruppe S_p, og $f(x)$ er derfor ikke opløseligt ved rodtegn for $p \geqq 5$.*

Bevis. Ifølge Sætning 12 i Kapitel 3 er $\mathrm{Gr}(M/\mathbb{Q})$ isomorf med en transitiv undergruppe i S_p. Hvis τ betegner overgangen til kompleks-konjugeret er τ en automorfi i $\mathrm{Gr}(M/\mathbb{Q})$, der svarer til en transposition i S_p. Ifølge Lemmaet ovenfor er derfor $\mathrm{Gr}(M/\mathbb{Q}) \simeq S_p$. □

Eksempel. $f(x) = x^5 - 4x + 2$ er irreducibelt over $\mathbb{Q}$ (hvorfor ?). Da $f(-\infty) < 0$, $f(0) > 0$, $f(1) < 0$, $f(+\infty) > 0$, må $f(x)$ have mindst 3 reelle rødder. Da $f(x)$ har grad 5, må antallet af reelle rødder således være 3 eller 5. Hvis $f(x)$ havde 5 reelle rødder, måtte ifølge Rolle's sætning $f'(x) = 5x^4 - 4$ have 4 reelle rødder. Da $f'(x)$ kun har 2 reelle rødder, har $f(x)$ netop 3 reelle rødder.

$f(x)$ er altså ikke opløseligt med rodtegn!

Vi viser nu mere alment

Sætning 9. *For ethvert ulige primtal p findes en normal udvidelse af $\mathbb{Q}$ med Galoisgruppe S_p.*

Bevis. Ifl. sætning 8 er det nok at vise, at der findes et i $\mathbb{Q}[X]$ irreducibelt polynomium af grad p med netop $p-2$ reelle rødder.

Polynomiet

$$f(x) = (x^2+1)(x-1)(x-2)\dots(x-(p-2)) + 2/2^{tp}$$

har for alle tilstrækkeligt store hele tal t netop $p-2$ reelle rødder. Det er endvidere irreducibelt i $\mathbb{Q}[X]$. Hertil er det nok at vise, at

$$2^{tp} f(x/2^t) = (x^2 + 2^{2t})(x-2^t)(x-2\cdot 2^t)\dots(x-(p-2)\cdot 2^t) + 2$$

er irreducibelt. Men her kan Eisensteins kriterium anvendes med primtallet 2. □

Sætning 10. *Til enhver endelig gruppe G findes en normal udvidelse M/L , hvor $Gr(M/L) \simeq G$ og L er en endelig udvidelse af $\mathbb{Q}$.*

Bevis. Da der findes uendeligt mange primtal er G ifl. Cayley's sætning isomorf med en undergruppe i den symmetriske gruppe S_p for et passende stort primtal p.

På grund af sætning 9 findes en normal udvidelse M af $\mathbb{Q}$ for hvilken $Gr(M/\mathbb{Q}) \simeq S_p$.

Fixpunktlegemet $L = \mathcal{F}(G)$ er en endelig udvidelse af $\mathbb{Q}$ og M/L er en endelig normal udvidelse med G som Galoisgruppe. □

Ovenstående viser, at det er relativt let at realisere en vilkårlig endelig gruppe G som Galoisgruppe over en endelig udvidelse L af $\mathbb{Q}$. Galoisteoriens omvendingsproblem, dvs. at realisere enhver endelig gruppe som Galoisgruppe over $\mathbb{Q}$, kan derfor betragtes som en art "descente problem". Vi skal "blot" kunne erstatte L med $\mathbb{Q}$. Det er et uhyre vanskeligt problem, hvor man stadig kun har sporadiske resultater. Man ved end ikke om der findes en fast endelig udvidelse L af $\mathbb{Q}$, så enhver endelig gruppe kan realiseres over L. Derimod kan man vise, at der findes en uendelig algebraisk udvidelse af $\mathbb{Q}$, over hvilken enhver endelig gruppe kan realiseres som Galoisgruppe.

And the end of all our exploring
Will be to arrive where we started
And know the place for the first time.

(T.S. Eliot, Little Gidding)

Kapitel VI. Kvadratiske rester

Lad p være et ulige primtal og a et helt tal, der ikke er deleligt med p.

a kaldes "kvadratisk rest modulo p" hvis kongruensen $a \equiv x^2 \pmod p$ har en løsning (eller ækvivalent hermed: hvis restklassen $[a]_p$ er et kvadrat i legemet $\mathbb{F}_p$).

Hvis $a \equiv x^2 \pmod p$ ikke har nogen løsning (dvs: hvis $[a]_p$ ikke er et kvadrat i legemet $\mathbb{F}_p$), kaldes a "kvadratisk ikke-rest modulo p".[1] Nu er $\mathbb{F}_p$ et legeme, hvis multiplikative gruppe $(\mathbb{F}_p \setminus \{0\}, \cdot)$ er cyklisk af orden $p-1$; der findes altså et $[g]_p \in \mathbb{F}_p$, så

$$\mathbb{F}_p \setminus \{0\} = \{[g]_p, [g]_p^2, \ldots, [g]_p^{p-1}\} .$$

Heraf fås

Sætning 1. *Med de ovennævnte benævnelser er $[g]_p^t$ et kvadrat i $\mathbb{F}_p \Leftrightarrow$ eksponenten t er lige.*

Følgelig har $\mathbb{F}_p \setminus \{0\}$ netop $\frac{p-1}{2}$ kvadrater og netop $\frac{p-1}{2}$ ikke-kvadrater. Med andre ord: der er netop $\frac{p-1}{2}$ kvadratiske rester modulo p og netop $\frac{p-1}{2}$ kvadratiske ikke-rester modulo p.

Nu gælder for et helt tal n, at $[g]_p^n = [1]_p$ i $\mathbb{F}_p \Leftrightarrow p-1 \mid n$. Udfra Sætning 1 fås derfor:

$$a \text{ kvadratisk rest modulo } p \Leftrightarrow [a]_p^{\frac{p-1}{2}} = [1]_p \text{ i } \mathbb{F}_p \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod p .$$

For ethvert $[a]_p \in \mathbb{F}_p \setminus \{0\}$ er $[a]_p^{p-1} = [1]$, hvorfor

$$0 = [a]_p^{p-1} - [1]_p = \{[a]_p^{\frac{p-1}{2}} - [1]_p\}\{[a]_p^{\frac{p-1}{2}} + [1]_p\} ,$$

og dermed $[a]_p^{\frac{p-1}{2}} = [1]_p$ eller $[-1]_p$.

Det foregående indebærer, at for et helt tal a, der ikke er deleligt med p, gælder: a kvadratisk rest modulo $p \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod p$ og a kvadratisk ikke-rest modulo $p \Leftrightarrow a^{\frac{p-1}{2}} \equiv -1 \pmod p$. For et *vilkårligt* helt tal a defineres "Legendresymbolet"

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{hvis} \quad p \nmid a \text{ og } a \text{ er kvadratisk rest modulo } p \\ -1 & \text{hvis} \quad p \nmid a \text{ og } a \text{ er kvadratisk ikke-rest modulo } p \\ 0 & \text{hvis} \quad p \mid a . \end{cases}$$

Det ovenstående medfører:

[1] I dette kapitel betegnes restklassen af a modulo et naturligt tal n med $[a]_n$ eller blot $[a]$,hvis der ikke er mulighed for misforståelse.

Eulers Kriterium. *For ethvert helt tal a gælder*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} .$$

Korollar 1. *For alle hele tal a og b er $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*
For restklasser der ikke er 0 modulo p betyder dette:

(kvadratisk rest)·(kvadratisk rest)=(kvadratisk rest)
(kvadratisk rest)·(kvadratisk ikke-rest)=(kvadratisk ikke-rest)
(kvadratisk ikke-rest)·(kvadratisk ikke-rest)=(kvadratisk rest) .

Korollar 2. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
Anderledes udtrykt:

-1 *kvadratisk rest modulo* $p \Leftrightarrow p \equiv 1 \pmod 4$
-1 *kvadratisk ikke-rest modulo* $p \Leftrightarrow p \equiv 3 \pmod 4$.

(Korollar 2 kaldes ofte "Første supplement til den kvadratiske reciprocitetssætning").

Opgave 1. Vis, at enhver ulige primdivisor i en sum af to indbyrdes primiske kvadrattal er $\equiv 1 \pmod 4$.

Angående 2 som kvadratisk rest gælder

Sætning 2. *("Andet supplement til den kvadratiske reciprocitetssætning").*
For et ulige primtal p er:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \textit{hvis} \quad p \equiv 1 \ \textit{eller} \ 7 \pmod 8 \\ -1 & \textit{hvis} \quad p \equiv 3 \ \textit{eller} \ 5 \pmod 8 \end{cases}$$

Dette kan kort udtrykkes ved $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Bevis. Lad M være legemet, der fås ved at adjungere en rod α til polynomiet $x^4 + [1]$ over $\mathbb{F}_p$. Inden for M gælder

$$\alpha^4 = [-1] \qquad\qquad \alpha^8 = [1] .$$

For $p \equiv 1 \pmod 8$	er	$\alpha^p = \alpha$	$(\alpha^{-1})^p = \alpha^{-1}$
For $p \equiv 3 \pmod 8$	er	$\alpha^p = -\alpha^{-1}$	$(\alpha^{-1})^p = -\alpha$
For $p \equiv 5 \pmod 8$	er	$\alpha^p = -\alpha$	$(\alpha^{-1})^p = -\alpha^{-1}$
For $p \equiv 7 \pmod 8$	er	$\alpha^p = \alpha^{-1}$	$(\alpha^{-1})^p = \alpha$.

Endvidere gælder (for alle p), at

$$(\alpha+\alpha^{-1})^2 = [2]+\alpha^2+\alpha^{-2} = [2]+\alpha^{-2}(\alpha^4+1) = [2]+0 = [2]\ ,$$

dvs. $[2]^{\frac{p-1}{2}} = (\alpha+\alpha^{-1})^{p-1}$.

Nu er $(\alpha+\alpha^{-1})^p = \alpha^p+\alpha^{-p}$. For $p \equiv 1$ eller $7 \pmod 8$ er $(\alpha+\alpha^{-1})^p = \alpha+\alpha^{-1}$, hvorfor

$$(\alpha+\alpha^{-1})^{p-1} = [1] \quad \text{altså} \quad [2]^{\frac{p-1}{2}} = [1] \ \text{ i } \ \mathbb{F}_p\ .$$

For $p \equiv 3$ eller $5 \pmod 8$ er $(\alpha+\alpha^{-1})^p = -(\alpha+\alpha^{-1})$, hvorfor

$$(\alpha+\alpha^{-1})^{p-1} = -[1] \quad \text{altså} \quad [2]^{\frac{p-1}{2}} = -[1] \ \text{ i } \ \mathbb{F}_p\ .$$

Dette giver det ønskede resultat. $\square$

Opgave 2. Vis, at -2 er kvadratisk rest modulo et ulige primtal p netop når $p \equiv 1$ eller $3 \pmod 8$.

Opgave 3. Lad x og y være indbyrdes primiske hele tal. Vis, at enhver ulige primdivisor i x^2+2y^2 er $\equiv 1$ eller $3 \pmod 8$.

Inden beviset for den almene kvadratiske reciprocitetssætning kommer nogle lemmaer.

Lemma 1. *Lad $n \in \mathbb{N}$ og $t \in \mathbb{Z}$. Den ved $\varphi_t([k]_n) = [k+t]_n$ definerede afbildning $\varphi_t : \mathbb{Z}_n \mapsto \mathbb{Z}_n$ kan opfattes som en permutation i den symmetriske gruppe S_n.*

Hvis n er ulige, er φ_t en lige permutation for alle $t \in \mathbb{Z}$. Hvis n er lige, er φ_t en lige permutation $\Leftrightarrow$ t er lige.

Bevis. Åbenbart er $\varphi_{s+t} = \varphi_s \circ \varphi_t$, specielt er $\varphi_t = \varphi_1^t$.

Nu er $\varphi_1 = \begin{pmatrix} [0] & [1] & \cdots & [n-1] \\ [1] & [2] & \cdots & [0] \end{pmatrix}$ en cykel af længde n. Derfor er φ_1 lige $\Leftrightarrow$ n ulige. Dette giver lemmaet. $\square$

Lemma 2. *Lad q være et ulige primtal og a et helt tal, der ikke er deleligt med q. Den ved $[x]_q \mapsto [a]_q[x]_q$ definerede permutation ψ_a af elementerne i $\mathbb{F}_q$ er en lige permutation netop når $[a]_q \in \mathbb{F}_q^2$ (dvs. $\left(\frac{a}{q}\right) = +1$).*

Bevis. Åbenbart er $\psi_a([0]_q) = [0]_q$ så ψ_a permuterer de fra $[0]$ forskellige elementer i $\mathbb{F}_q$. Lad $[g]$ være en frembringer for den cykliske gruppe $(\mathbb{F}_q \setminus \{0\}, \cdot)$ og lad $[a] = [g]^t$ og $[x] = [g]^k$. Da er $\psi_a[g]^k = [g]^{k+t}$. Idet $q-1$ er lige, giver Lemma 1 og Sætning 1 det ønskede resultat. $\square$

Ved Galoisteori for endelige legemer giver vi nu et bevis for

Den kvadratiske reciprocitetssætning. *For forskellige ulige primtal p og q gælder*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} .$$

Anderledes udtrykt:

$$\begin{aligned} \left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right) && \textit{hvis enten } p \textit{ eller } q \textit{ er} \equiv 1 \pmod 4 \\ \left(\frac{p}{q}\right) &= -\left(\frac{q}{p}\right) && \textit{hvis både } p \textit{ og } q \textit{ er} \equiv 3 \pmod 4 \end{aligned}$$

Bevis. Lad M være spaltningslegemet for polynomiet $f(x) = x^q - [1]_p$ over $\mathbb{F}_p$. Da $f(x)$ og $f'(x)$ ikke har nogen fælles rod, må $f(x)$ (ifl. Sætning 19 i Kap. 2) have lutter simple rødder. Hvis ε er en fra $[1]_p$ forskellig rod, er samtlige rødder netop $[1]_p, \varepsilon, \varepsilon^2, \dots, \varepsilon^{q-1}$.

$M/\mathbb{F}_p$ er en normal udvidelse og $\mathrm{Gr}(M/\mathbb{F}_p)$ er cyklisk (jfr. Sætning 2 i Kap. 3) og frembragt af "Frobeniusautomorfien" σ, der sender ethvert element over i dets p-te potens. Galoisgruppen $\mathrm{Gr}(M/\mathbb{F}_p)$ er da isomorf med den undergruppe i S_q, der frembringes af

$$\begin{pmatrix} [1] & \varepsilon & \varepsilon^2 & \cdots & \varepsilon^{q-1} \\ [1] & \varepsilon^p & \varepsilon^{2p} & \cdots & \varepsilon^{(q-1)p} \end{pmatrix} .$$

Den her optrædende permutation af eksponenterne

$$\begin{pmatrix} [0]_q & [1]_q & [2]_q & \cdots & [q-1]_q \\ [0]_q & [p]_q & [2p]_q & \cdots & [(q-1)p]_q \end{pmatrix}$$

er netop den i det foregående Lemma 2 omhandlede permutation med $a = p$. Vi slutter heraf, at denne permutation er lige, netop når $\left(\frac{p}{q}\right) = 1$. Med andre ord er $\mathrm{Gr}(M/\mathbb{F}_p)$ betragtet som permutationsgruppe af de q rødder, da og kun da, indeholdt i den alternerende gruppe A_q når $\left(\frac{p}{q}\right) = 1$.

Men ifølge Sætning 12A er $\mathrm{Gr}(M/\mathbb{F}_p) \subseteq A_q$ netop når diskriminanten af $x^q - [1]_p$ er et kvadrat i $\mathbb{F}_p$. Denne diskriminant har vi udregnet (sætning 32 i Kap. 2) til $[q]_p^q(-1)^{\frac{q-1}{2}}$.

Sammenfattet får vi derfor:

$$\mathrm{Gr}(M/\mathbb{F}_p) \subseteq A_q \Leftrightarrow [q]_p^q(-1)^{\frac{q-1}{2}} \in \mathbb{F}_p^2 \Leftrightarrow \left(\frac{q^q(-1)^{\frac{q-1}{2}}}{p}\right) = 1$$

og

$$\mathrm{Gr}(M/\mathbb{F}_p) \subseteq A_q \Leftrightarrow \left(\frac{p}{q}\right) = 1$$

dvs.

$$\left(\frac{p}{q}\right) = \left(\frac{q^q(-1)^{\frac{q-1}{2}}}{p}\right) .$$

Nu er

$$\left(\frac{q^q(-1)^{\frac{q-1}{2}}}{p}\right) = \left(\frac{q}{p}\right)^q \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} ,$$

hvor vi har udnyttet første supplement til reciprocitetssætningen.

Alt i alt får vi nu

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \quad \text{eller} \quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} .$$

□

Historisk bemærkning. Både første og andet supplement til den kvadratiske reciprocitetssætning var kendt af Fermat, men blev først (efter flere fejlslagne forsøg) bevist af Euler. Andet supplement blev også bevist af Lagrange. (Det er ikke helt klart, hvem der har prioriteten.) Euler formodede den kvadratiske reciprocitetssætning, dog ikke helt i den her givne formulering. Den nuværende formulering blev først opstillet af Legendre i 1785, der gav et ufuldstændigt bevis.

Gauss opdagede på egen hånd som 19-årig den kvadratiske reciprocitetssætning og gav (også som 19-årig) det første korrekte bevis herfor, der blev publiceret i 'Disquisitiones Arithmeticae" 1801. Gauss gav ialt 7 beviser for reciprocitetssætningen, byggende på helt forskellige ideer. Senere er der givet flere hundrede beviser, hvoraf dog mange er næsten isomorfe. Den kvadratiske reciprocitetssætning kaldes ofte "Aritmetikkens Perle" og Gauss omtaler den som "TEOREMA AUREUM".

Eksempel 1. $\left(\frac{-3}{p}\right) = \begin{cases} +1 & \text{for} \quad p \equiv 1 \pmod 3 \\ -1 & \text{for} \quad p \equiv -1 \pmod 3 \end{cases} .$

Dette fås umiddelbart af reciprocitetssætningen, idet

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{3-1}{2}\frac{p-1}{2}} = \left(\frac{p}{3}\right)$$

og $\left(\frac{p}{3}\right) = 1$ når $p \equiv 1 \pmod 3$ og $\left(\frac{p}{3}\right) = -1$ når $p \equiv -1 \pmod 3$.

Ved analoge argumenter fås

Eksempel 2. $\left(\frac{3}{p}\right) = \begin{cases} +1 & \text{for} \quad p \equiv \pm 1 \pmod{12} \\ -1 & \text{for} \quad p \equiv \pm 5 \pmod{12} \end{cases} .$

Eksempel 3. $\left(\frac{5}{p}\right) = \begin{cases} +1 & \text{for} \quad p \equiv \pm 1 \pmod 5 \\ -1 & \text{for} \quad p \equiv \pm 2 \pmod 5 . \end{cases}$

Eksempel 4. Hvornår er $F_n = 2^{2^n} + 1$, $n > 1$ et primtal? (Jfr. Gauss' sætning om konstruktion af regulære polygoner med passer og lineal.)
Svar: Netop når $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$

Thi, hvis F_n er et primtal, er 3 ifl. eksempel 2 kvadratisk ikke-rest modulo F_n, hvorfor Eulers kriterium giver den ønskede kongruens.

Hvis $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$, vil den ved 3 bestemte restklasse modulo F_n have orden $F_n - 1$ i gruppen af primiske restklasser modulo F_n (hvorfor?). Der findes da (mindst) $F_n - 1$ primiske restklasser modulo F_n, der således må være et primtal. (Herved er det undertiden muligt at vise, at F_n er et sammensat tal uden at kunne angive nogen ægte divisor i F_n!)

Eksempel 5. Hvis $n > 2$, vil det for enhver primdivisor p i F_n gælde, at $p \equiv 1 (\mathrm{mod}\ 2^{n+2})$.

Thi lad t være ordenen af $[2]_p$ i den multiplikative gruppe af de fra 0 forskellige elementer i legemet $\mathbb{F}_p$. Da $2^{2^n} \equiv -1 (\mathrm{mod}\ p)$ viser en simpel gruppeteoretisk overvejelse viser, at 2^{n+1} må være lig t, dvs. $p \equiv 1 \pmod{2^{n+1}}$. Da $n > 2$, er specielt $p \equiv 1 \pmod 8$, hvorfor Eulers kriterium sammenholdt med Sætning 2 viser, at $2^{\frac{p-1}{2}} \equiv 1 \pmod p$. Men da må $2^{n+1} = t$ være en divisor i $\frac{p-1}{2}$, hvilket medfører, at $p \equiv 1 \pmod{2^{n+2}}$. (Det var på denne måde, at Euler "gættede" primfaktoren 641 i $F_5 = 2^{32} + 1 = 4294967297$.)

Opgave. **Eksempel 6.** Vis, at et naturligt tal n må være et primtal, såfremt $2^n - 1$ er et primtal. Tallene $M_n = 2^n - 1$ kaldes *Mersennetal.* $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$ er primtal, medens $M_{11} = 23 \cdot 89$ er sammensat. Vis, at hvis p er et primtal $\equiv 3 \pmod 4$, da vil $2p + 1$ gå op i M_p hvis og kun hvis $2p + 1$ er et primtal. (Benyt bl.a. "Andet supplement til den kvadratisk reciprocitetssætning".)

Vis, at hvis n er et ulige primtal, vil det for enhver divisor d i M_n gælde, at $d \equiv 1 \pmod n$ og $d \equiv \pm 1 \pmod 8$.

Mersennetallene er bl.a. interessante af to grunde:

1) Relation til "fuldkomne tal": Et naturligt tal N kaldes fuldkomment, hvis $2N = \sum_{d|N} d$, dvs. hvis N er lig summen af sine ægte divisorer. Det kan vises, at et *lige* tal er fuldkomment hvis og kun hvis det har formen $2^{n-1}M_n$, hvor $M_n = 2^n - 1$ er et primtal.

2) Relation til "store" primtal: Igennem det sidste århundrede har til enhver tid det størst kendte primtal været et Mersenneprimtal. I skrivende stund (juni 2002) er det største kendte primtal Mersennetallet $M_{13466917}$, der skrevet i 10-talsystemet har 4 053 946 cifre.

(Det er stadig ukendt om der findes uendeligt mange Mersenneprimtal.)

Den generaliserede reciprocitetssætning for Jacobi symbolet

Det kan ofte være hensigtsmæssigt at generalisere reciprocitetssætningen til sammensatte tal. Legendresymbolet $\left(\frac{a}{p}\right)$ er kun defineret for et ulige primtal p. Jacobi indførte et mere generelt symbol $\left(\frac{a}{P}\right)$, defineret for ethvert med a primisk ulige naturligt tal P på følgende måde. Hvis

$$P = p_1 \cdots p_t$$

er et produkt af (ikke nødvendigvis forskellige) ulige primtal $p_1, p_2, \ldots, p_t$, da defineres

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_t}\right)$$

hvor faktorerne på højre side er Legendre symboler. Hvis $P = 1$ sættes $\left(\frac{a}{p}\right) = 1$.

Hvis kongruensen $a \equiv x^2 \pmod{P}$ har en løsning, er $\left(\frac{a}{p_1}\right) = \cdots = \left(\frac{a}{p_t}\right) = 1$, og dermed $\left(\frac{a}{P}\right) = 1$. Derimod kan man *ikke* omvendt slutte, at $\left(\frac{a}{P}\right) = 1$ medfører, at $a \equiv x^2 \pmod{P}$ har en løsning, idet et lige antal af faktorerne $\left(\frac{a}{p_1}\right), \ldots, \left(\frac{a}{p_t}\right)$ kunne være -1.

Af definitionen fås let:

Sætning 3. *Lad a og b være hele tal og P og Q ulige naturlige tal. Antag a og b er primiske med P og Q. Da gælder*

$$\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$$

$$\left(\frac{a}{P}\right)\left(\frac{a}{Q}\right) = \left(\frac{a}{PQ}\right)$$

$$a \equiv b \pmod{P} \Rightarrow \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right) .$$

Vi viser nu følgende analogier til første og andet supplement til reciprocitetssætningen.

Sætning 4. *For et ulige naturligt tal P gælder*

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$$

Bevis. Lad $P = \prod_i p_i$ hvor hvert p_i er et ulige primtal. Da $P = \prod_i (1 + p_i - 1)$ og hvert $p_i - 1$ er lige, fås $P \equiv 1 + \sum_i (p_i - 1) \pmod{4}$ og hermed

$$\frac{P-1}{2} \equiv \sum \frac{p_i - 1}{2} \qquad \pmod{2} .$$

Ifølge Første supplement til reciprocitetssætningen haves

$$\left(\frac{-1}{P}\right) = \prod_i \left(\frac{-1}{p_i}\right) = (-1)^{\sum_i \frac{p_i-1}{2}} = (-1)^{\frac{P-1}{2}} .$$

□

Sætning 5. *For et ulige naturligt tal P gælder*

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$$

Bevis. Lad $P = \prod_i p_i$ hvor hvert p_i er et ulige primtal. Da $P^2 = \prod_i (1 + p_i^2 - 1)$ og $p_i^2 - 1$ er delelig med 8 og ethvert produkt $(p_i^2 - 1)(p_j^2 - 1)$ er deleligt med 64, fås

$$P^2 - 1 \equiv \sum_i (p_i^2 - 1) \pmod{64}$$

og dermed specielt

$$\frac{P^2-1}{8} \equiv \sum_i \frac{p_i^2 - 1}{8} \pmod{2} ,$$

hvorfor andet supplement til reciprocitetssætningen giver

$$\left(\frac{2}{P}\right) = \prod_i \left(\frac{2}{p_i}\right) = (-1)^{\sum_i \frac{p_i^2-1}{8}} = (-1)^{\frac{P^2-1}{8}} .$$

$\square$

Vi viser nu generaliseringen af reciprocitetssætningen til Jacobi symboler.

Sætning 6. *For to ulige indbyrdes primiske naturlige tal P og Q gælder*

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}} .$$

Bevis. Vi betragter primfaktoropløsningerne af P og P

$$P = \prod_i p_i \quad \text{og} \quad Q = \prod_j q_j .$$

Da er

$$\left(\frac{P}{Q}\right) = \prod_{i,j} \left(\frac{p_i}{q_j}\right) \quad \text{og} \quad \left(\frac{Q}{P}\right) = \prod_{i,j} \left(\frac{q_j}{p_i}\right)$$

og dermed

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{i,j} \left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) ,$$

så vi ifølge reciprocitetssætningen får $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^h$, hvor

$$h = \sum_{i,j} \frac{p_i - 1}{2} \cdot \frac{q_j - 1}{2} = \left(\sum_i \frac{p_i - 1}{2} \right) \left(\sum_j \frac{q_j - 1}{2} \right) .$$

Som tidligere godtgjort (jfr. beviset for Sætning 4) er

$$\sum_i \frac{p_i - 1}{2} \equiv \frac{P-1}{2} \pmod 2 \text{ og } \sum_j \frac{q_j - 1}{2} \equiv \frac{Q-1}{2} \pmod 2 ,$$

hvorfor $h \equiv \frac{P-1}{2} \cdot \frac{Q-1}{2} \pmod 2$. □

Sætning 6 kan være praktisk til numerisk udregning af Legendre symboler.

Eksempel 7. Tallet 1801 er et primtal. [Dette ses hurtigt således: $1801 = 24^2 + 35^2 = 1^2 + 2 \cdot 30^2$ medfører (jfr. Opgave 1 og Opgave 3), at enhver primfaktor i 1801 må være $\equiv 1 \pmod 8$. Man skal derfor blot se, at 17 og 41 ikke går op i 1801, da $\sqrt{1801} = 42,4\cdots$].

Er 546 kvadratisk rest mod 1801? Hertil betragtes

$$\begin{aligned}
&\left(\frac{546}{1801}\right) = \left(\frac{2}{1801}\right)\left(\frac{273}{1801}\right) = \\
&\left(\frac{273}{1801}\right) \quad \text{(ifølge andet supplement til reciprocitetssætningen)} \\
&= \left(\frac{1801}{273}\right) \quad \text{(ifølge Sætning 6)} \\
&= \left(\frac{163}{273}\right) = \left(\frac{273}{163}\right) = \left(\frac{110}{163}\right) = \left(\frac{2}{163}\right) \cdot \left(\frac{55}{163}\right) = \\
&(-1) \cdot \left(\frac{55}{163}\right) = (-1) \cdot (-1) \cdot \left(\frac{163}{55}\right) = \left(\frac{-2}{55}\right) = \left(\frac{-1}{55}\right) \cdot \left(\frac{2}{55}\right) = -1 .
\end{aligned}$$

Altså er 546 ikke kvadratisk rest mod 1801.

Fremstilling som sum af to kvadrater

Hvis et ulige primtal p kan skrives som sum af to kvadrater på hele tal i $p = x^2 + y^2$ må p være $\equiv 1 \pmod 4$; thi x og y kan ikke være delelige med p og $p = x^2 + y^2$ medfører

$$x^2 \equiv (-1)y^2 \pmod p$$

således at -1 er kvadratisk rest modulo p.

Ifølge første supplement til reciprocitetssætningen må p nødvendigvis være $\equiv 1 \pmod 4$. Det er en bemærkelsesværdig sætning (opdaget af Fermat, men det første dokumenterede bevis blev givet af Euler), at ovennævnte kan vendes om, dvs. ethvert primtal $p \equiv 1 \pmod 4$ kan skrives $p = x^2 + y^2$, $x, y \in \mathbb{Z}$.

Der findes adskillige helt forskellige beviser for denne sætning. Vi giver her et konstruktivt bevis, der ud fra p tillader eksplicit beregning af x og y.

Resultatet fås ud fra en række mindre sætninger.

Sætning 7. *For et ulige primtal p gælder:*

$$\sum_{x \bmod p} \left(\frac{x}{p}\right) = 0$$

Bevis. Der er lige mange kvadratiske rester og kvadratiske ikke-rester. □

Sætning 8. *For et ulige primtal p gælder:*

$$\sum_{\substack{x \bmod p \\ y \bmod p}} \left(\frac{xy}{p}\right) = 0$$

Bevis. På grund af Sætning 7 fås

$$\sum_{\substack{x \bmod p \\ y \bmod p}} \left(\frac{xy}{p}\right) = \left(\sum_{x \bmod p} \left(\frac{x}{p}\right)\right) \cdot \left(\sum_{y \bmod p} \left(\frac{y}{p}\right)\right) = 0$$

□

Sætning 9. *Lad p være et ulige primtal og r et naturligt tal. Da gælder:*

$$\sum_{x \bmod p} x^r \equiv \begin{cases} -1 \pmod p & \textit{hvis} \quad p-1 \mid r \\ 0 \pmod p & \textit{hvis} \quad p-1 \nmid r\,. \end{cases}$$

Bevis. Hvis $p-1$ går op i r, følger udsagnet af Fermats “lille sætning”, da i så fald $x^r \equiv 1 \pmod p$ for $x \not\equiv 0 \pmod p$ og $p-1 \equiv -1 \pmod p$.

Hvis $p-1$ ikke går op i r betrager vi et helt tal g så $[g]_p$ frembringer gruppen $(\mathbb{F}_p \setminus \{0\}, \cdot)$. Da er $g^r - 1 \not\equiv 0 \pmod p$, og

$$\sum_{x \bmod p} x^r \equiv \sum_{x \bmod p} (gx)^r \equiv g^r \sum_{x \bmod p} x^r$$

hvoraf $(g^r - 1)(\sum_{x \bmod p} x^r) \equiv 0 \pmod p$. Følgelig er $\sum_{x \pmod p} x^r \equiv 0 \pmod p$. □

Sætning 10. *Lad a og b være hele tal og p et ulige primtal. Da gælder*

$$S = \sum_{x \mod p} \left(\frac{x^2 + ax + b}{p} \right) = \begin{cases} p-1 & \textit{hvis} \quad p \mid a^2 - 4b \\ -1 & \textit{hvis} \quad p \nmid a^2 - 4b \end{cases}$$

Bevis. Vi betragter først tilfældet, hvor $a^2 - 4b$ er deleligt med p. Da Legendresymbolet $\left(\frac{4}{p}\right) = 1$ kan den omhandlede sum S skrives

$$S = \sum_{x \mod p} \left(\frac{4x^2 + 4ax + 4b}{p} \right) = \sum_{x \mod p} \left(\frac{(2x-a)^2 - a^2 + 4b}{p} \right) =$$

$$\sum_{x \mod p} \left(\frac{2x-a}{p} \right)^2 = \sum_{y \mod p} \left(\frac{y}{p} \right)^2 = p - 1$$

Vi betragter dernæst tilfældet, hvor $a^2 - 4b$ ikke er deleligt med p.

Som ovenfor kan S skrives

$$S = \sum_{x \mod p} \left(\frac{(2x-a)^2 - (a^2 - 4b)}{p} \right) = \sum_{y \mod p} \left(\frac{y^2 - (a^2 - 4b)}{p} \right) .$$

Hvert led er 0, 1 eller -1. Her vil 0 forekomme i to led, hvis $a^2 - 4b$ er kvadratisk rest modulo p og ikke i noget, hvis $a^2 - 4b$ er kvadratisk ikke-rest modulo p. Dette indebærer, at S må være et ulige tal.

Vi bestemmer nu S modulo p. Ifølge Eulers kriterium er

$$\left(\frac{x^2 + ax + b}{p} \right) \equiv (x^2 + ax + b)^{\frac{p-1}{2}} \pmod p$$

For passende hele tal $c_1, \ldots, c_{p-1}$ er

$$(x^2 + ax + b)^{\frac{p-1}{2}} = x^{p-1} + c_1 x^{p-2} + \cdots + c_{p-2} x + c_{p-1} .$$

Ved at udnytte ovenstående og summere fås på grund af Sætning 9, at

$$S \equiv -1 + 0 + \cdots + 0 \equiv -1 \pmod p .$$

Endelig bemærker vi, at den numeriske værdi af S højest kan være p, dvs. $-p \leq S \leq p$. Men -1 er det eneste ulige tal, der er $\equiv -1 \pmod p$ og ligger i intervallet $[-p, p]$. Altså må S være -1. $\square$

Inden vi giver den første anvendelse af Sætning 10 indskyder vi følgende

Sætning 11. *Lad a være et helt tal og p et ulige primtal. Da er antallet af løsninger til kongruensen $x^2 \equiv a \pmod{p}$ netop $1 + \left(\frac{a}{p}\right)$.*

Bevis. Hvis a er delelig med p har kongruensen kun 1 løsning, nemlig $x \equiv 0 \pmod{p}$.

Hvis $p \nmid a$ og a er kvadratisk ikke-rest, har kongruensen ingen løsninger og $1 + \left(\frac{a}{p}\right) = 1 + (-1) = 0$. Hvis $p \nmid a$ og a er kvadratisk rest, findes et x_0 så $a \equiv x_0^2 \pmod{p}$. Den omhandlede kongruens kan da skrives $a \equiv x_0^2 \equiv x^2 \pmod{p}$ eller $(x - x_0)(x + x_0) \equiv 0 \pmod{p}$, hvoraf ses, at kongruensen har netop 2 løsninger (nemlig $\pm x_0$) og $2 = 1 + \left(\frac{a}{p}\right) = 1 + 1$. $\square$

Fra Sætning 10 og Sætning 11 fås nu

Sætning 12. *Lad p være et ulige primtal og a og b hele tal. Da er antallet af løsninger (x, y) til kongruensen $y^2 \equiv x^2 + ax + b \pmod{p}$ $2p - 1$ eller $p - 1$ alt eftersom $a^2 - 4b$ er delelig med p eller ikke delelig med p.*

Bevis. Det søgte antal løsninger er ifølge Sætning 11

$$\sum_{x \mod p} \left(1 + \left(\frac{x^2 + ax + b}{p}\right)\right) = p + \sum_{x \mod p} \left(\frac{x^2 + ax + b}{p}\right) .$$

Sætning 10 giver nu det ønskede antal. $\square$

En umiddelbar konsekvens af Sætning 10 er

Sætning 13. *Lad p være et ulige primtal og x og y hele tal der ikke er delelige med p. Da er*

$$\sum_{k=1}^{p-1} \left(\frac{(x^2 + k)(y^2 + k)}{p}\right) = \begin{cases} -2 & \text{når} \quad x^2 \not\equiv y^2 \pmod{p} \\ p - 2 & \text{når} \quad x^2 \equiv y^2 \pmod{p} \end{cases}$$

For et ulige primtal p og et helt tal k der ikke er deleligt med p defineres nu:

$$S(k) = \sum_{x \mod p} \left(\frac{x(x^2 + k)}{p}\right) .$$

Bemærkning. Hvis $p \equiv 3 \pmod{4}$ er $S(k) = 0$; thi

$$S(k) = \sum_{x \mod p} \left(\frac{(-x)(x^2 + k)}{p}\right) = \left(\frac{-1}{p}\right) S(k) = -S(k)$$

ifølge første supplement til reciprocitetssætningen.

$S(k)$ er derfor kun interessant for $p \equiv 1 \pmod 4$ og vi skal vise, at vi ved hjælp af $S(k)$ kan give en eksplicit fremstilling af sådanne primtal som sum af to kvadrattal.

Vi viser først, at $S(k)$ er et lige tal. Det ses af

$$S(k) = \sum_{x=1}^{\frac{p-1}{2}} \left(\frac{x(x^2+k)}{p}\right) + \sum_{x=1}^{\frac{p-1}{2}} \left(\frac{(p-x)((p-x)^2+k)}{p}\right) -$$
$$\sum_{x=1}^{\frac{p-1}{2}} \left(\frac{x(x^2+k)}{p}\right) + \left(\frac{-1}{p}\right) \sum_{x=1}^{\frac{p-1}{2}} \left(\frac{x(x^2+k)}{p}\right) =$$
$$2\sum_{x=1}^{\frac{p-1}{2}} \left(\frac{x(x^2+k)}{p}\right) ,$$

hvor vi har udnyttet, at $\left(\frac{-1}{p}\right) = 1$ når $p \equiv 1 \pmod 4$.

Næste etape er

Sætning 14. *$S(k)^2$ er konstant på alle kvadratiske rester k mod p og $S(k)^2$ er konstant på alle kvadratiske ikke-rester mod p.*

Bevis. For $t \not\equiv 0 \pmod p$ er

$$S(kt^2) = \sum_{x \mod p} \left(\frac{x(x^2+kt^2}{p}\right) = \sum_{x \mod p} \left(\frac{xt(x^2t^2+kt^2)}{p}\right) =$$
$$\left(\frac{t}{p}\right) \sum_{x \mod p} \left(\frac{x(x^2+k)}{p}\right) = \left(\frac{t}{p}\right) S(k) .$$

□

Lad nu r betegne en fast kvadratisk rest (mod p) og n en fast kvadratisk ikke-rest (mod p).

Vi kan nu give den ønskede fremstilling af p som sum af to kvadrater, når p er et primtal der er $\equiv 1 \pmod 4$.

Sætning 15. *Med de ovenfor indførte benævnelser gælder for primtallet $p \equiv 1$ (mod 4):*

$$P = \left(\frac{S(r)}{2}\right)^2 + \left(\frac{S(n)}{2}\right)^2 ,$$

hvor $\frac{S(r)}{2}$ *og* $\frac{S(n)}{2}$ *ifølge tidligere bemærkning er hele tal.*

Bevis. På grund af Sætning 14 er

$$V \underset{\text{def}}{=} \frac{p-1}{2}[S(r)^2 + S(n)^2] = \sum_{k=1}^{p-1} S(k)^2 = \sum_{k=1}^{p-1} \left[\sum_{k=1}^{p-1} \left(\frac{x(x^2+k)}{p} \right) \right]^2$$

Vi foretager nu en udregning af denne sum af kvadrater af summer:

$$V = \sum_{k=1}^{p-1} \left[\sum_{x=1}^{p-1} \left(\frac{x(x^2+k)}{p} \right) \right] \left[\sum_{y=1}^{p-1} \left(\frac{y(y^2+k)}{p} \right) \right] =$$
$$\sum_{\substack{1 \le x \le p-1 \\ 1 \le y \le p-1}} \sum_{1 \le k \le p-1} \left(\frac{xy(x^2+k)(y^2+k)}{p} \right) =$$
$$\sum_{\substack{1 \le x \le p-1 \\ 1 \le y \le p-1}} T(x,y) \,,$$

hvor

$$T(x,y) = \sum_{1 \le k \le p-1} \left(\frac{xy(x^2+k)(y^2+k)}{p} \right) =$$
$$\left(\frac{xy}{p} \right) \sum_{1 \le k \le p-1} \left(\frac{(x^2+k)(y^2+k)}{p} \right) \,.$$

På grund af Sætning 13 får vi nu:

$$T(x,y) = \begin{cases} -2\left(\frac{xy}{p}\right) & \text{for} \quad x^2 \not\equiv y^2 \pmod{p} \\ (p-2)\left(\frac{xy}{p}\right) & \text{for} \quad x^2 \equiv y^2 \pmod{p} \end{cases}$$

Derfor fås

$$V = \sum_{\substack{1 \le x \le p-1 \\ 1 \le y \le p-1 \\ x^2 \equiv y^2 \pmod{p}}} p \left(\frac{xy}{p} \right) - 2 \sum_{\substack{1 \le x \le p-1 \\ 1 \le y \le p-1}} \left(\frac{xy}{p} \right) \,.$$

Her er ifølge Sætning 8 sidste led 0.

Endvidere er

$$x^2 \equiv y^2 \pmod{p} \Leftrightarrow x \equiv \pm y \pmod{p} \Rightarrow \left(\frac{xy}{p} \right) = \left(\frac{\pm 1}{p} \right) = 1$$

da $p \equiv 1 \pmod{4}$, jfr. første supplement til reciprocitetssætningen.

Da der netop er $2(p-1)$ par (x,y) af restklasser $(\neq (0,0))$ modulo p for hvilke $x^2 \equiv y^2 \mod p$ slutter vi

$$V = p \cdot 2(p-1)$$

eller

$$S(r)^2 + S(n)^2 = 4p$$

og dermed $p = \left(\frac{S(r)}{2}\right)^2 + \left(\frac{S(n)}{2}\right)^2$. $\square$

Man kan udtrykke $\frac{S(r)}{2}$ og $\frac{S(n)}{2}$ en smule kortere og får derved

Sætning 15A. *Lad p være et primtal $\equiv 1 \pmod 4$ og n en kvadratisk ikke-rest modulo p. Da gælder*

$$p = \left(\sum_{1 \le x \le \frac{p-1}{2}} \left(\frac{x(x^2+1)}{p} \right) \right)^2 + \left(\sum_{1 \le x \le \frac{p-1}{2}} \left(\frac{x(x^2+n)}{p} \right) \right)^2 .$$

Vi viser nu, at der ikke findes andre fremstillinger af et primtal $\equiv 1 \pmod 4$ som sum af to kvadrattal end den ovenfor angivne.

Sætning 16. *Lad p være et primtal $\equiv 1 \pmod 4$ og antag $p = a^2 + b^2 = c^2 + d^2$, hvor a, b, c og d er hele tal. Da er enten $a^2 = c^2 \wedge b^2 = d^2$ eller $a^2 = d^2 \wedge b^2 = c^2$.*

Bevis. Ifølge første supplement til reciprocitetesætningen findes et helt tal h, så $h^2 \equiv -1 \pmod p$.

Af $p = a^2 + b^2 = c^2 + d^2$ sluttes

$$a^2 \equiv -b^2 \equiv h^2 b^2 \pmod p$$
$$c^2 \equiv -d^2 \equiv h^2 d^2 \pmod p$$

hvorfor

$$a \equiv \pm hb \pmod p$$
$$c \equiv \pm hd \pmod p$$

Ved eventuelt at erstatte b med $-b$ og/eller d med $-d$ kan vi antage

$$a \equiv hb \pmod p$$
$$c \equiv hd \pmod p$$

og dermed

$$ac \equiv h^2 bd \equiv -bd \pmod p$$

dvs. $ac + bd$ er deleligt med p.

Nu er

$$p^2 = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

hvorfor også $ad - bc$ må være deleligt med p. p^2 er da skrevet som sum af to hele ikke-negative tal, der begge er delelige med p^2. Et af disse må være 0.

Hvis $ac + bd = 0$, er $ac = -bd$. Da $(a, b) = (c, d) = 1$ må $a|d$ og $d|a$, dvs. $a = \pm d$, hvorfor $a^2 = d^2$ og dermed $b^2 = c^2$. Hvis $ad - bc = 0$, er $ad = bc$ og som før sluttes, at $a|c$ og $c|a$, dvs. $a = \pm c$ hvorfor $a^2 = c^2$ og dermed $b^2 = d^2$. □

Nogle bemærkninger om højere potensrester

For ethvert naturligt tal m kan man naturligvis analogt med kvadratiske rester indføre m-te potensrester, idet man for et primtal p og et med p ikke deleligt helt tal kalder a for m-te potensrest modulo p hvis kongruensen $a \equiv x^m \pmod p$ har en løsning.

En reciprocitetssætning for m-te potensrester – analog til den kvadratiske reciprocitetssætning – findes ikke inden for de rationale tal. For at opnå en sådan er man nødt til at betragte algebraiske tallegemer indeholdende det m-te cirkeldelingslegeme.

I ganske specielle tilfælde kan man dog udlede resultater inden for $\mathbb{Q}$. Vi giver et eksempel, der går tilbage til Gauss.

For et ulige primtal p og et helt tal a der ikke er deleligt med p siges a at være bikvadratisk rest modulo p hvis kongruensen

$$x^4 \equiv a \pmod p$$

har løsninger; dvs., hvis restklassen $[a]_p$ er en fjerdepotens i legemet $\mathbb{F}_p$.

For at bestemme antallet af bikvadratiske rester betragtes afbildningen

$$\varphi : (\mathbb{F}_p^*)^2 \mapsto (\mathbb{F}_p^*)^4$$

defineret ved $\varphi(x) = x^2$, $x \in (\mathbb{F}_p^*)^2$, der åbenbart er en surjektiv (multiplikativ) homomorfi. Her er

$$\operatorname{Ker}(\varphi) = \{x \in (\mathbb{F}_p^*)^2 \mid x^2 = [1]\} = \{\pm[1]\} \cap (\mathbb{F}_p^*)^2 \ .$$

På grund af første supplement til den kvadratiske reciprocitetssætning er $\operatorname{Ker}\varphi = \{[1]\}$, hvis $p \equiv 3 \pmod 4$ og $\operatorname{Ker}\varphi = \{\pm[1]\}$ hvis $p \equiv 1 \pmod 4$.

Følgelig er for $p \equiv 3 \pmod 4$ enhver kvadratisk rest også bikvadratisk rest, mens for $p \equiv 1 \pmod 4$ netop halvdelen af de kvadratiske rester er bikvadratiske rester. For $p \equiv 1 \pmod 4$ er der altså netop $\frac{p-1}{4}$ bikvadratiske rester.

Helt analogt til Eulers kriterium vises

Sætning 17. *Lad p være et primtal $\equiv 1 \pmod 4$ og a et helt tal der ikke er deleligt med p. Da er a bikvadratisk rest modulo p hvis og kun hvis $a^{\frac{p-1}{4}} \equiv 1 \pmod p$.*

Hvis 2 er bikvadratisk rest modulo p, er 2 specielt kvadratisk rest modulo p og p må ifølge andet supplement til den kvadratiske reciprocitetssætning være $\equiv 1$ eller 7 (mod 8).

Hvis $p \equiv 7 \pmod 8$ er p specielt $\equiv 3 \pmod 4$ og ifølge det foregående er 2 derfor bikvadratisk rest modulo p.

Hvis $p \equiv 1 \pmod 8$ gælder

Sætning 18 (Gauss)**.** *Lad p være et primtal $\equiv 1 \pmod 8$ og $p = a^2 + b^2$ fremstillingen som sum af to kvadrater, hvor b antages at være lige. Da er 2 bikvadratisk rest modulo p hvis og kun hvis b er deleligt med 8.*

Bemærkning. Da $p \equiv 1 \pmod 8$ må b automatisk være deleligt med 4.

Bevis. Da 2 er kvadratisk rest modulo p er $2^{\frac{p-1}{2}} \equiv 1 \pmod p$ og derfor er $2^{\frac{p-1}{4}} \equiv +1$ eller $-1 \pmod p$. Vi skal undersøge, hvornår der gælder $+1$ eller -1 i ovenstående kongruens.

På grund af kongruensen

$$(a+b)^2 \equiv 2ab \pmod p$$

fås

$$(2ab)^{\frac{p-1}{4}} \equiv (a+b)^{\frac{p-1}{2}} \equiv \left(\frac{a+b}{p}\right) \pmod p\,. \qquad (*)$$

Da $p \equiv 1 \pmod 4$ giver Sætning 6, at $\left(\frac{a+b}{p}\right)$ er lig Jacobisymbolet $\left(\frac{p}{a+b}\right)$.

På grund af identiteten

$$(a+b)^2 + (a-b)^2 = 2p$$

og Sætning 3 fås

$$1 = \left(\frac{2p}{a+b}\right) = \left(\frac{2}{a+b}\right)\left(\frac{p}{a+b}\right)\,,$$

hvor Sætning 5 giver

$$\left(\frac{2}{a+b}\right) = (-1)^{\frac{(a+b)^2-1}{8}}$$

og derfor

$$\left(\frac{a+b}{p}\right) = (-1)^{\frac{(a+b)^2-1}{8}} = (-1)^{\frac{p-1}{8}}(-1)^{\frac{ab}{4}}\,.$$

Da $p = a^2 + b^2$ er $b^2 \equiv -a^2 \pmod p$ og derfor $(ab)^2 \equiv -a^4 \pmod p$.

Nu er

$$\begin{aligned}(2ab)^{\frac{p-1}{4}} &= 2^{\frac{p-1}{4}}(a^2b^2)^{\frac{p-1}{8}} \equiv 2^{\frac{p-1}{4}}(-a^4)^{\frac{p-1}{8}} \\ &\equiv 2^{\frac{p-1}{4}}(-1)^{\frac{p-1}{8}}a^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{4}}(-1)^{\frac{p-1}{8}}\left(\frac{a}{p}\right) \pmod{p}\ .\end{aligned}$$

Ifølge Sætning 6 er $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)$ og da $p \equiv b^2 \pmod{a}$ er $\left(\frac{p}{a}\right) = 1$. Altså er $(2ab)^{\frac{p-1}{4}} \equiv 2^{\frac{p-1}{4}}(-1)^{\frac{p-1}{8}} \pmod{p}$. Men ifølge $(*)$ er $(2ab)^{\frac{p-1}{4}} \equiv \left(\frac{a+b}{p}\right) \equiv (-1)^{\frac{p-1}{8}}(-1)^{\frac{ab}{4}} \pmod{p}$. Sammenholdes disse to kongruenser fås $2^{\frac{p-1}{4}} \equiv (-1)^{\frac{ab}{4}} \pmod{p}$. Nu er

$$(-1)^{\frac{ab}{4}} = \begin{cases} -1 & \text{hvis} \quad 8 \nmid b \\ +1 & \text{hvis} \quad 8 \mid b\ . \end{cases}$$

Dette giver det ønskede resultat. □

Nogle slutbemærkninger

Af Sætning 15 slutter vi, at

$$|S(r)| \leq 2\sqrt{p} \ \text{ og } \ |S(n)| \leq 2\sqrt{p}$$

og hermed

$$\left| \sum_{x \mod p} \left(\frac{x(x^2+k)}{p} \right) \right| \leq 2\sqrt{p}$$

for ethvert k.

Dette indebærer ifølge Sætning 11, at antallet N af løsninger (x, y) mod p til kongruensen

$$y^2 \equiv x(x^2+k) \pmod{p}$$

tilfredsstiller

$$|N - p| \leq 2\sqrt{p}\ .$$

Dette er et specielt tilfælde af en almen meget dybtliggende sætning vedrørende antallet af punkter på en algebraisk kurve over et endeligt legeme. Vi skal kort beskrive dette resultat.

Lad $f(X,Y) \in \mathbb{Z}[X,Y]$ og lad $\overline{f}(X,Y)$ være det tilsvarende polynomium i $\mathbb{F}_p[X,Y]$.

Man er da interesseret i antallet N_p af punkter $(x,y) \in \mathbb{F}_p \times \mathbb{F}_p$ på kurven $\overline{f}(X,Y) = 0$, dvs. antallet af løsninger $(x,y) \in \mathbb{F}_p \times \mathbb{F}_p$ til ligningen $\overline{f}(x,y) = 0$.

Det viser sig hensigtsmæssigt at medtage de “uendeligt fjerne” punkter, idet man betragter den projektive plan og den projektive linie over $\mathbb{F}_p$. Den projektive plan fås ved at betragte ækvivalensrelationen af tripler $\{(x,y,z) \neq (0,0,0) \mid x,y,z \in \mathbb{F}_p\}$ defineret ved $(x_1,y_1,z_1) \sim (x_2,y_2,z_2) \Leftrightarrow \exists \lambda \in \mathbb{F}_p \setminus 0$ så $(x_1,y_1,z_1) = \lambda(x_2,y_2,z_2)$.

Den projektive plan er da mængden af de tilsvarende ækvivalensklasser. De "uendeligt fjerne" punkter repræsenteres ved tripler (x,y,z), hvor $z = 0$. Den projektive plan over $\mathbb{F}_p$ har $\frac{p^3-1}{p-1} = p^2+p+1$ punkter. Den projektive linie fås analogt ved ækvivalensrelationen i mængden af par $\{(x,y) \neq (0,0) \mid x,y \in \mathbb{F}_p\}$ defineret ved $(x_1,y_1) \sim (x_2,y_2) \Leftrightarrow \exists \lambda \in \mathbb{F}_p \setminus 0$ så $(x_1,y_1) = \lambda(x_2,y_2)$.

Den projektive linie er da mængden af de tilsvarende ækvivalensklasser. Det "uendeligt fjerne" punkt er repræsenteret ved $(1,0)$. Den projektive linie har $p+1$ punkter.

For et polynomium $\overline{f}(x,y) \in \mathbb{F}_p[X,Y]$ betragtes det tilsvarende homogene polynomium

$$f_{\text{hom}}(X,Y,Z) \underset{\text{def}}{=} Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right) ,$$

hvor d er graden af f. For dette gælder åbenbart

$$f_{\text{hom}}(x,y,z) = 0 \Rightarrow f_{\text{hom}}(\lambda x, \lambda y, \lambda z) = 0 \ \text{ for } \ \forall \lambda \in \mathbb{F}_p .$$

Lad os betragte førnævnte eksempel

$$\overline{f}(X,Y) = Y^2 - X^3 - kX ,$$

hvor vi får

$$\overline{f}_{\text{hom}}(X,Y,Z) = Y^2 Z - X^3 - kXZ^2 .$$

Den tilsvarende kurve har det "uendeligt fjerne" punkt repræsenteret ved $(0,1,0)$.

For antallet N_p^* af punkter på den projektive kurve gælder derfor $|N_p^* - (p+1)| \leq 2\sqrt{p}$. Den almene sætning er nu følgende: Lad $f(X,Y)$ være et polynomium i $\mathbb{Z}[X,Y]$ og $\overline{f}(X,Y)$ det tilsvarende polynomium i $\mathbb{F}_p[X,Y]$. Vi antager, at $\overline{f}(X,Y)$ er absolut irreducibelt, dvs. er irreducibelt under enhver endelig grundlegemsudvidelse og er singularitetsfri. Da gælder for antallet N_p^* af punkter på $\overline{f}(X,Y) = 0$ inklusive de "uendeligt fjerne" punkter, at

$$|N_p^* - (p+1)| \leq 2g\sqrt{p} \tag{$\diamond$}$$

hvor g er kurvens genus. Vi skal ikke give definitionen af g her, blot nævne, at det er en invariant knyttet til kurven. Vi nævner nogle konkrete tilfælde. Hvis

$$\overline{f}(X,Y) = Y^2 - (X^n + a_1 X^{n-1} + \cdots + a_n)$$

hvor $X^n + a_1X^{n-1} + \cdots + a_n$ har lutter simple rødder, er

$$g = \begin{cases} \frac{n-1}{2} & \text{når} \quad n \ \text{ er ulige} \\ \frac{n-2}{2} & \text{når} \quad n \ \text{ er lige .} \end{cases}$$

Hvis $\overline{f}(X,Y) = X^n + Y^n - 1$ og $n > 1$, er genus $\frac{(n-1)(n-2)}{2}$.

Den af os betragtede kurve $Y^2 - X(X^2 - k)$ har genus $g = 1$ så ($\diamond$) stemmer med den ovenfor udledede ulighed.

En lidt svagere formulering, hvor begrebet genus ikke indgår, er følgende.

Weils sætning. *Lad N betegne antallet af nulpunkter for et absolut irreducibelt polynomium $\overline{f}(X,Y) \in \mathbb{F}_p[X,Y]$ af grad $d \geq 1$. Da gælder*

$$|N - p - 1| \leq (d-1)(d-2)\sqrt{q} + d$$

.

Beviset for det almene resultat går langt uden for rammerne af dette kursus. I tilfældet $g = 1$ skyldes det HASSE, i det almene tilfælde A. WEIL. Det kan fortolkes som RIEMANNS Formodning for funktionslegemer med endeligt konstantlegeme.

APPENDIKS 1. QUATERNIONERNE

Lad $\mathbb{H}$ være mængden af komplekse (2×2)-matricer af følgende form:

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \tag{$*$}$$

hvor $\overline{\alpha}$, (resp. $\overline{\beta}$) betegner det med α, (resp. β) komplekst konjugerede tal.

Med sædvanlig matrixaddition og matrixmultiplikation udgør $\mathbb{H}$ en delring af ringen af alle komplekse (2×2)-matricer, idet sum, differens og produkt af to matricer i mængden $\mathbb{H}$ igen ligger i $\mathbb{H}$. Nulmatricen er nulelementet i $\mathbb{H}$ og enhedsmatricen (der har 1-taller i diagonalen og nuller udenfor) er $\mathbb{H}$'s etelement. $\mathbb{H}$ er en ikke-kommutativ ring.

Determinanten af en matrix $(*)$ i $\mathbb{H}$ er lig $\alpha\overline{\alpha} + \beta\overline{\beta} =\mid \alpha \mid^2 + \mid \beta \mid^2$, der er positiv, når blot ikke både α og β er 0, dvs. når matricen $(*)$ ikke er nulmatricen.

Lad nu

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$$

være en fra nulmatricen forskellig matrix i $\mathbb{H}$. Determinanten d er da et positivt reelt tal. Der findes derfor en reciprok matrix, som udregnes til

$$\begin{pmatrix} \overline{\alpha}/d & -\beta/d \\ \overline{\beta}/d & \alpha/d \end{pmatrix}$$

Åbenbart ligger denne matrix igen i $\mathbb{H}$. Ringen $\mathbb{H}$ har altså den egenskab, at ethvert fra nulelementet forskelligt element har et reciprokt. En sådan ring kaldes en divisionsring eller et skævlegeme.

Det her indførte skævlegeme $\mathbb{H}$ kaldes quaternionlegemet og elementerne i $\mathbb{H}$ kaldes quaternioner. [Disse blev indført af den irske matematiker og astronom William Rowan Hamilton (1805-65).]

Hvis vi skriver $\alpha = a_0 + a_1 i, \beta = a_2 + a_3 i$, hvor $i = \sqrt{-1}$ er den imaginære enhed og a_0, a_1, a_2 og a_3 er reelle tal, kan matricen $(*)$ skrives på følgende måde

$$a_0 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + a_1 \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + a_2 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + a_3 \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Lad os nu sætte

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

Åbenbart kommuterer $\mathbf{1}$ med alle matricerne i $\mathbb{H}$ og der gælder

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

og

$$\mathbf{i} \cdot \mathbf{j} = \mathbf{k}, \ \ \mathbf{j} \cdot \mathbf{k} = \mathbf{i}, \ \ \mathbf{k} \cdot \mathbf{i} = \mathbf{j}$$

og $\mathbf{i}, \mathbf{j}$ og $\mathbf{k}$ antikommuterer, dvs.

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

Ethvert element i $\mathbb{H}$ kan således entydigt skrives:

$$a_0\mathbf{1} + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}, \ \ a_0, \ a_1, \ a_2, \ a_3 \in \mathbb{R}.$$

Man kan altså opfatte quaternionerne som vektorer i det 4-dimensionale vektorrum $\mathbb{R}^4$.

Additionen af sådanne foretages koordinatvis, medens multiplikation foretages efter følgende forskrift:

$$(a_0\mathbf{1} + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}) \cdot (b_0\mathbf{1} + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k}) =$$

$$(a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3)\mathbf{1}+$$

$$(a_1b_0 + a_0b_1 - a_3b_2 + a_2b_3)\ \mathbf{i}+$$

$$(a_2b_0 + a_3b_1 + a_0b_2 - a_1b_3)\ \mathbf{j}+$$

$$(a_3b_0 - a_2b_1 + a_1b_2 + a_0b_3)\ \mathbf{k}.$$

Elementerne i $\mathbb{H}$ kan opfattes som par af en reel skalar og en vektor i det 3-dimensionale euklidiske rum: $(a, \mathbf{u}), a \in \mathbb{R}, \mathbf{u} \in \mathbb{R}^3$.

Med denne interpretation kan multiplikationen formuleres mere geometrisk:

$$(a, \mathbf{u}) \cdot (b, \mathbf{v}) = (ab - \mathbf{u} \cdot \mathbf{v}, a\mathbf{v} + b\mathbf{u} - \mathbf{u} \times \mathbf{v}),$$

hvor $\mathbf{u} \cdot \mathbf{v}$ betegner skalarproduktet og $\mathbf{u} \times \mathbf{v}$ det ydre produkt (”krydsproduktet”) af vektorerne $\mathbf{u}$ og $\mathbf{v}$.

APPENDIKS 2. VANDERMONDES DETERMINANT

Idet $n \geqq 2$ og $x_1, x_2, \cdots, x_n$ betegner elementer i et vilkårligt legeme, vil vi vise, at *determinanten* (*VANDERMONDES determinant)*

$$D = \begin{vmatrix} 1 & x_1 & x_1^2 \cdots x_1^{n-1} \\ 1 & x_2 & x_2^2 \cdots x_2^{n-1} \\ \multicolumn{3}{c}{\dotfill} \\ 1 & x_n & x_n^2 \cdots x_n^{n-1} \end{vmatrix}$$

er lig med produktet af de $\frac{n(n-1)}{2}$ *faktorer* $x_r - x_s$, *for hvilke* r *og* s *er to vilkårlige indbyrdes forskellige af tallene* $1, 2, \cdots, n$ *underkastet betingelsen* $r > s$.

Den $(n-1)$'te søjle i ovenstående determinant multipliceres med $-x_1$ og adderes til den n'te søjle; i den derved fremkomne determinant multipliceres den $(n-2)$'te søjle med $-x_1$ og adderes til den $(n-1)$'te o.s.v., indtil vi sluttelig multiplicerer den 1'ste søjle med $-x_1$ og adderer til den 2-den søjle. Derved fås

$$D = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & x_2 - x_1 & (x_2 - x_1)x_2 & \cdots & (x_2 - x_1)x_2^{n-2} \\ \multicolumn{5}{c}{\dotfill} \\ 1 & x_n - x_1 & (x_n - x_1)x_n & \cdots & (x_n - x_1)x_n^{n-2} \end{vmatrix}$$

eller

$$D = (x_2 - x_1)(x_3 - x_1) \cdots (x_n - x_1) \begin{vmatrix} 1 & x_2 & x_2^2 \cdots x_2^{n-2} \\ 1 & x_3 & x_3^2 \cdots x_3^{n-2} \\ \multicolumn{3}{c}{\dotfill} \\ 1 & x_n & x_n^2 \cdots x_n^{n-2} \end{vmatrix} .$$

Vi har dermed reduceret den oprindelige determinant til en determinant af samme form, men af $(n-1)$'te orden, og idet vi bemærker, at

$$\begin{vmatrix} 1 & x_{n-1} \\ 1 & x_n \end{vmatrix} = x_n - x_{n-1} \, ,$$

fører en simpel induktionsbetragtning umiddelbart til det ovenfor omtalte udtryk for D.

Opgavesamling til Mat 3 AL

Opg. 1.

Vis, at for en gruppe G er følgende betingelser ækvivalente:

i) Afbildningen $G \to G$ defineret ved $x \to x^{-1}$ er en isomorfi.

ii) Afbildningen $G \to G$ defineret ved $x \to x^2$ er en homomorfi.

iii) G er abelsk.

Opg. 2.

Lad G være en endelig gruppe for hvilken der findes en automorfi $\alpha \in Aut(G)$ der har orden 2 og kun har det neutrale element e som fixpunkt, (d.v.s. $\alpha(\alpha(x)) = x$ for ethvert $x \in G$ og $\alpha(x) = x \Rightarrow x = e$).

Vis, at ethvert element i G kan skrives på formen $x\alpha(x)^{-1}$.

Vis, at G må være abelsk.

Opg. 3.

Lad a, b og c være elementer i en gruppe G.

i) Vis, at a og a^{-1} har samme orden.

ii) Vis, at ab og ba har samme orden.

iii) Vis, at abc og bca har samme orden. Generaliser.

iv) Vis ved et eksempel, at produktet af to elementer af endelig orden ikke nødvendigvis har endelig orden. (Se på matricerne $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ og $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$.)

Opg. 4.

Lad G være en gruppe af lige orden. Vis, at antallet af elementer af orden 2 er ulige.

Opg. 5.

Lad G være den abelske gruppe bestående af alle følger $(a_1, a_2, \cdots)$, hvor $a_1, a_2, \cdots \in \mathbb{Z}_4$. ($\mathbb{Z}_4$ er den additive gruppe af restklasser modulo 4.) Komposition i G er komponentvis addition. Lad H være den abelske gruppe bestående af alle følger $(b_1, a_2, a_3, \cdots)$, hvor $b_1 \in \mathbb{Z}_2$ og $a_2, a_3, \cdots \in \mathbb{Z}_4$.

Vis, at G er isomorf med en undergruppe i H og at H er isomorf med en undergruppe i G. Undersøg, om G og H er isomorfe.

Opg. 6.

Lad G være en cyklisk gruppe. Vis, at $Aut(G) \simeq \mathbb{Z}_2$, hvis $G = (\mathbb{Z}, +)$.

Vis, at $Aut(G)$ er isomorf med den multiplikative gruppe $(\mathbb{Z}_n^*, .)$ af primiske restklasser modulo n, hvis $G = (\mathbb{Z}_n, +)$.

Godtgør, at enhver undergruppe i en cyklisk gruppe er karakteristisk.

Opg. 7.

Lad n være et naturligt tal. Vis, at antallet af ikke-isomorfe grupper af orden n er $\leqq [(n-1)\,!]^{n-2}$.

Opg. 8.

Lad a og b være ombyttelige elementer i gruppen G. Antag Ord $(a) = m < \infty$ og Ord $(b) = n < \infty$. Vis, at Ord (ab) er en divisor i mn.

Vis, at Ord $(ab) = mn$, hvis m og n er indbyrdes primiske.

Opg. 9.

Vis, at matricerne

$$\left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \; a, b, c \in \mathbb{Z}/\mathbb{Z}3 \right\}$$

med sædvanlig matrixmultiplikation udgør en gruppe af orden 27, hvor ethvert element $\neq e$ har orden 3.

Angiv herved to ikke-isomorfe endelige grupper, hvor elementordnerne stemmer overens med multiplicitet.

Opg. 10.

Lad G være en endelig gruppe og H en normal undergruppe i G. Antag at $|H|$ og $[G : H]$ er indbyrdes primiske. Vis, at H er den eneste undergruppe i G af orden $|H|$. (Benyt Noethers 1. Isomorfisætning.)

Opg. 11.

Lad H og K være undergrupper i gruppen G, så $H \supseteq K$. Vis, at $[G : K] = [G : H][H : K]$.

Opg. 12.

Lad G være en gruppe og H og K to normaldelere i G. Vis, at $hk = kh$ for ethvert h i H og ethvert k i K, hvis $H \cap K = e$.

(Betragt $hkh^{-1}k^{-1}$.)

De efterfølgende opgaver 13–16 benytter lidt mængdelære.

Opg. 13.

Lad p være et ulige primtal. Vis, at der ikke findes nogen gruppe G for hvilken $|Aut(G)| = p$.

Opg. 14.

Vis, at for enhver gruppe G gælder:

$$|G| \leqq 2 \;\Leftrightarrow\; Aut(G) = 1_G \; .$$

Opg. 15.

Vis, at enhver mængde er underliggende mængde for en gruppe.

Opg. 16.

Vis, at $(\mathbb{R}, +) \simeq (\mathbb{C}, +)$.

Opg. 17.

Lad K være en ikke-tom delmængde i en gruppe G. Vis, at K er en venstre sideklasse m.h.t. en undergruppe i G, hvis og kun hvis

$$x, y, z \in K \;\Rightarrow\; xy^{-1}z \in K \; .$$

Tilsvarende fås en karakterisering af højresideklasserne i G.
Vis, at enhver venstresideklasse (m.h.t. en eller anden undergruppe) i G er højresideklasse (m.h.t. en eller anden undergruppe) i G.

Opg. 18.

Vis, at

$$G = \left\{ \begin{pmatrix} \cos\frac{2\pi}{n}k & -\sin\frac{2\pi}{n}k \\ \sin\frac{2\pi}{n}k & \cos\frac{2\pi}{n}k \end{pmatrix} \middle|\; k = 0, 1, 2, \cdots, n-1 \right\}$$

udgør en cyklisk undergruppe i $GL(2, \mathbb{R})$ af orden n.
Lad $\underline{\underline{B}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
Vis, at mængden $G \cup \underline{\underline{B}}G$ udgør en undergruppe i $GL(2, \mathbb{R})$, der er isomorf med Diedergruppen D_n af orden $2n$.

Opg. 19.

Bestem alle undergrupper i Diedergruppen D_4 af orden 8 og disses indbyrdes placering. (Skriv $D_4 = \{e, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$, $\sigma^4 = \tau^2 = e$; $\tau\sigma\tau = \sigma^{-1}$, hvor σ er en drejning på $\frac{\pi}{2}$ og τ en spejling.)

Opg. 20.

Vis, at

$$H = \left\{ \begin{pmatrix} a_{11} a_{12} \\ 0 \quad a_{22} \end{pmatrix} \middle| \; a_{11}, a_{12}, a_{22} \in \mathbb{R}\,,\; a_{11} \neq 0,\; a_{22} \neq 0 \,\right\}$$

udgør en undergruppe i $GL(2, \mathbb{R})$. Bestem de afledede grupper H' H'' etc.

(Udregn kommutatoren $\underline{\underline{A}}\,\underline{\underline{B}}\,\underline{\underline{A}}^{-1}\,\underline{\underline{B}}^{-1}$, hvor $\underline{\underline{A}} = \left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\underline{\underline{B}} = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$.)

Opg. 21.

Lad G være det indre direkte produkt af undergrupperne H og K. Lad A være normaldeler i G, så $A \cap H = A \cap K = \{e\}$. Vis, at A er indeholdt i centret $Z(G)$.

Opg. 22.

Vis, at $\mathbb{Z}/\mathbb{Z}2$ er den eneste endelige gruppe med netop to konjugeretklasser .

Opg. 23.

Bestem de endelige grupper med netop tre konjugeretklasser.

Opg. 24.

Lad G være en gruppe af orden p^n, hvor p er et primtal. Vis, at det for en normaldeler H i G, $(H \neq \{e\})$ gælder, at $H \cap Z(G) \neq \{e\}$.

(Vink: Analyser beviset for, at en p-gruppe har ikke-trivielt centrum).

Vis, at en normaldeler i G af orden p er indeholdt i centret $Z(G)$.

Opg. 25.

Lad G være en cyklisk gruppe af orden n. Vis, at der til enhver divisor d i n findes een undergruppe af orden d.

Opg. 26.

Lad G være en gruppe for hvilken der findes en undergruppe $H \neq G$ med egenskaben, at enhver ægte undergruppe i G er indeholdt i H. Vis, at G er cyklisk af primtalspotensorden. (Betragt et element i $G \setminus H$.)

Opg. 27.

Lad G være en gruppe. Vis, at G er cyklisk af orden p^2, hvor p er et primtal, hvis og kun hvis G har netop een undergruppe $\neq e$ og $\neq G$.

Opg. 28.

Vis, at $Aut(V_4) \simeq Aut(S_3) \simeq S_3$. (Her betegner V_4 Kleins Vierergruppe.)

Opg. 29. $(*)$

Vis, at der ikke findes nogen gruppe, for hvilken den indre automorfigruppe er isomorf med quaterniongruppen af orden 8.

Vis, at en gruppe er abelsk, hvis dens automorfigruppe er isomorf med quaterniongruppen af orden 8.

$(**)$ Undersøg, om der findes en gruppe, hvis indre automorfigruppe er isomorf med $\mathbb{Z}_4 \times \mathbb{Z}_2$.

Opg. 30.

Vis, at enhver endelig gruppe G kan indlejres i en endelig simpel gruppe, (dvs. G er isomorf med en undergruppe i en endelig simpel gruppe). (Angiv en injektiv homomorfi fra S_t til A_{2t}. Anvend Cayley's Sætning og Galois's Sætning.)

Opg. 31.

Lad P være en undergruppe i S_n indeholdende en ulige Permutation. Vis, at $|P|$ er lige og at netop halvdelen af elementerne i P er lige permutationer. (Betragt den indbyrdes placering af A_n og P og benyt Noether's 1. Isomorfisætning.)

Opg. 32.

Vis, at $|P|$ er delelig med n for enhver transitiv undergruppe P i den symmetriske gruppe S_n. {Vis, at undergruppen bestående af de permutationer, der fikser punktet 1 ("stabilitetsgruppen for P i punktet 1") har indeks n i P.}

Opg. 33.

Lad $n = p_1^{a_1} \cdots p_r^{a_r}$ hvor $p_1, \cdots, p_r$ er indbyrdes forskellige primtal. Vis, at $\mathbb{Z}/\mathbb{Z}n \simeq \mathbb{Z}/\mathbb{Z}p_1^{a_1} \times \cdots \times \mathbb{Z}/\mathbb{Z}p_r^{a_r}$. (Kinesiske restklassesætning.)

Opg. 34.

Lad G være en gruppe af orden p^n, hvor p er et primtal. Vis, at der findes en normalrække $G \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{n-1} \triangleright G_n = e$, hvor alle faktorgrupperne har orden p.

(Betragt en kompositionsrække for G.)

Opg. 35.

Lad G være en endelig gruppe af orden n med den egenskab, at der til enhver divisor d i n findes højest én undergruppe i G af orden d.

i) Vis, at for enhver primdivisor p i n findes netop én p-Sylowgruppe i G.

ii) Vis, (v.hj. af Opg. 34 ovenfor og Opg. 26), at Sylowgrupperne i G er cykliske.

iii) Vis (v.hj. af Opg. 33 og Opg. 12), at G er cyklisk.

Opg. 36.

Vis, at for en endelig gruppe G af orden n er følgende betingelser ækvivalente:

i) G er cyklisk.

ii) Til enhver divisor d i n findes højest en undergruppe i G af orden d.

iii) Til enhver divisor d i n findes netop én undergruppe i G af orden d.

Opg. 37.

Vis, at et endeligt legemes multiplikative gruppe er cyklisk.

Opg. 38.

Lad G være en endelig gruppe, hvis orden er delelig med primtallet p. Lad endvidere P være en normaldeler, hvis orden er en potens af p. Vis, at P er indeholdt i enhver p-Sylowgruppe for G.

Opg. 39.

Lad H være en undergruppe i gruppen G og lad P være en p-Sylowgruppe for G. Undersøg, om $H \cap P$ er en p-Sylowgruppe for H.

Opg. 40.

Lad G være en gruppe, hvis orden er delelig med primtallet p, men ej med p^2. Vis, at antallet af elementer i G af orden p er $\equiv -1 \pmod p$.

Anvend dette på den symmetriske gruppe S_p, hvor p er et primtal, og udled Wilson's Sætning: For ethvert primtal p er $(p-1)! \equiv -1 \pmod p$.

Opg. 41.

Lad $\mathcal{P}$ være en abelsk transitiv permutationsgruppe i S_n. Vis, at $|\mathcal{P}| = n$. (Vis, at stabilitetsgruppen for $\mathcal{P}$ i f.eks. punktet (1) er e.)

Opg. 42.

Lad G være en gruppe og H en undergruppe i G af indeks n. Lad $G = \bigcup_{i=1}^n x_i H$ være inddelingen af G i disjunkte højresideklasser. Lad ρ være følgende afbildning fra G til S_n opfattet som gruppen af permutationer af højresideklasserne $x_1H, \cdots, x_nH$ defineret ved

$$\rho(x) = \begin{pmatrix} x_1H & x_2H & \cdots & x_nH \\ xx_1H & xx_2H & \cdots & xx_nH \end{pmatrix}, \quad x \in G\,.$$

Vis, at ρ er en homomorfi med $\operatorname{Ker}(\rho) = \bigcap_{i=1}^{n} x_i H x_i^{-1}$ og vis, at $\operatorname{Ker}(\rho) \subseteq H$.

Opg. 43.

Lad G være en simpel gruppe indeholdende en undergruppe af indeks n, hvor $n > 1$. Vis, at G er isomorf med en undergruppe i S_n. (Benyt opg. 42.)

Opg. 44.

Lad H være en undergruppe i S_n, $H \neq A_n$, $H \neq S_n$ og antag $n \geq 5$.
Vis, (v. hj. af opg. 42) at $[S_n : H] \geq n$.

Opg. 45.

i) Vis, at enhver simpel gruppe af orden < 60 er cyklisk af primtalsorden.
ii) Godtgør, at enhver gruppe af orden < 60 er opløselig. (Betragt en kompositionsrække for en sådan gruppe og udnyt i).)

Opg. 46.

Vis, at enhver gruppe af orden p^2q^2 er opløselig, når p og q er primtal. (Antag $p > q$ og vis, at $\#$ (p-Sylowgrupper) > 1 medfører $q^2 \equiv 1 \pmod{p}$; dette indebærer $q = 2$ og $p = 3$.)

Opg. 47.

Lad n være af formen $p{\cdot}a$, $a < p$, p et primtal. Vis, at enhver undergruppe af orden p^a i den symmetriske gruppe S_n er abelsk. (Vink: Angiv en abelsk undergruppe af orden p^a.)

Opg. 48.

i) Lad $a_1, \cdots, a_n$ være n forskellige hele tal. Vis, at $f(x) = \prod_{i=1}^{n}(x - a_i) - 1$ er irreducibelt i $\mathbb{Q}[X]$.
(Antag $f(x) = g(x)h(x)$, hvor $g(x)$ og $h(x)$ er normerede polynomier i $\mathbb{Z}[X]$ af grad $< n$. Betragt $g(a_i) + h(a_i)$.)

ii) Lad $a_1, \cdots, a_n$ være n forskellige hele tal. Vis, at polynomiet $\prod_{i=1}^{n}(x - a_i)^2 + 1$ irreducibelt i $\mathbb{Q}[X]$.

Opg. 49.

Angiv 2-Sylowgrupperne (antal og isomorfitype) i den symmetriske gruppe S_4.
Samme spørgsmål for 3-Sylowgrupperne.

Opg. 50.

Lad G være en endelig gruppe og N_1 og N_2 to normaldelere i G. Vil G/N_1 og G/N_2 være isomorfe, hvis N_1 og N_2 er isomorfe? Vil N_1 og N_2 være isomorfe, hvis G/N_1 og G/N_2 er isomorfe?

Opg. 51.

Vis, at $X^n + 5X^{n-1} + 3$ er irreducibelt i $\mathbb{Z}[X]$ (og dermed også i $\mathbb{Q}[X]$) for ethvert naturligt tal n. [Denne opgave stammer fra den internationale matematikolympiade juli 1993.]

Opg. 52.

Lad $L \supset K$ være legemer og α og β elementer i L. Antag graden af α over K er m og graden af β over K er n, dvs. $[K(\alpha) : K] = m$ og $[K(\beta) : K] = n$. Vis, at $[K(\alpha, \beta) : K] \leq m \cdot n$.

Vis, at $[K(\alpha, \beta) : K]$ er delelig med m og med n.

Vis, at $[K(\alpha, \beta) : K] = m \cdot n$, hvis m og n er indbyrdes primiske.

Opg. 53.*)

Opg. p. 2.12 i Noterne. (Før beviset indirekte. Antag Grad(Irr $(\alpha + \beta, K)$) $= 1$, p eller q og udled deraf en modstrid.)

Opg. 54.

Vis, at polynomiet $x^3 - x^2 + 1$ er irreducibelt over $\mathbb{Q}$ og lad α være en rod (i $\mathbb{C}$) til dette.

Bestem $[Q(\sqrt{2}\,, \alpha) : \mathbb{Q}]$ og vis, at $Q(\sqrt{2}\,, \alpha) = \mathbb{Q}(\alpha\sqrt{2})$.

[Eftervis og benyt, at $\alpha = -\alpha^4 + \alpha^2 - 1 \in \mathbb{Q}(\alpha\sqrt{2})$.]

Opg. 55.

Vis, at $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$.

(Antag $\sqrt{2} = a + b\sqrt{3}$, $a \in \mathbb{Q}$, $b \in \mathbb{Q}$ og udled heraf en modstrid.)

Angiv en basis for $\mathbb{Q}(\sqrt{2},\, \sqrt{3})$ betragtet som vektorrum over $\mathbb{Q}$.

Godtgør, at $\mathbb{Q}(\sqrt{2},\, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. (Benyt enten beviset for Abel-Steinitz' Sætning eller find rationale tal q_0, q_1, q_2, q_3, så
$\sqrt{2} = q_0 + q_1(\sqrt{2} + \sqrt{3}) + q_2(\sqrt{2} + \sqrt{3})^2 + q_3(\sqrt{2} + \sqrt{3})^3$.)

Vis, at $\mathbb{Q}(\sqrt{2},\, \sqrt{3})/\mathbb{Q}$ er normal og angiv Gr($\mathbb{Q}(\sqrt{2},\, \sqrt{3})/\mathbb{Q}$).

Opg. 56.

Angiv spaltningslegemerne (opfattet som dellegemer af $\mathbb{C}$) over $\mathbb{Q}$ for hvert af følgende polynomier $X^4 + 4$, $X^4 + 16$, $X^4 - 10$, $X^2 + 20$, $X^3 - 2$ og $X^3 - 4$ og bestem spaltningslegemernes dimension over $\mathbb{Q}$.

Opg. 57.

Angiv $[\mathbb{Q}(\sqrt{2},\ \sqrt[3]{2}) : \mathbb{Q}]$. Vis, at $\mathbb{Q}(\sqrt{2},\ \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.

Lad $\epsilon = e^{2\pi i/3} = (-1 + i\sqrt{3})/2$.

Angiv $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q})]$, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$, $[\mathbb{Q}(\sqrt[3]{2}\,\epsilon) : \mathbb{Q}]$ og $[\mathbb{Q}(\sqrt[3]{2},\ \sqrt[3]{2}\,\epsilon) : \mathbb{Q}]$.

(Sammenlign med Opg. 52.)

Opg. 58.

Vis, at $f(X) = X^3 + X + 1$ i $(\mathbb{Z}/5)[X]$ er irreducibelt i $(\mathbb{Z}/5)[X]$.

Vis, at $f(X)$ indenfor $(\mathbb{Z}/5)[X]$ går op i $X^{125} - X$. (Vink: Se på eksistensbeviset vedrørende endelige legemer.)

Opg. 59.

Lad M_1, M_2, M_3, M_4, M_5 og M_6 være spaltningslegemerne over $\mathbb{Q}$ for polynomierne $X^4 - 2$, $X^4 + 2$, $X^3 - 3$, $X^3 + 3$, $X^6 - 3$ og $X^6 + 3$.

Bestem $[M_1 : \mathbb{Q}]$, $[M_2 : \mathbb{Q}]$, $[M_3 : \mathbb{Q}]$, $[M_4 : \mathbb{Q}]$,$[M_5 : \mathbb{Q}]$ og $[M_6 : \mathbb{Q}]$.

Opg. 60.

Vis, at $\mathrm{Aut}(\mathbb{Q}) = \{1_{\mathbb{Q}}\}$. Vis, at $\mathrm{Aut}(\mathbb{R}) = \{1_{\mathbb{R}}\}$. (Lad $\alpha \in \mathrm{Aut}(\mathbb{R})$; vis, at α må være identiteten på $\mathbb{Q}$ og godtgør, at α må være ordenstro, idet de ikke-negative reelle tal kan karakteriseres som mængden af kvadrater i $\mathbb{R}$.)

Opg. 61.

Lad a og b være rationale tal $\neq 0$, så $a \notin \mathbb{Q}^2$, $b \notin \mathbb{Q}^2$, $ab \notin \mathbb{Q}^2$. Lad $M = \mathbb{Q}(\sqrt{a}, \sqrt{b})$. Vis, at $M/\mathbb{Q}$ er normal. Bestem $[M : \mathbb{Q}]$ og $\mathrm{Gr}(M/\mathbb{Q})$.

Opg. 62.

Lad $f(X)$ være et irreducibelt 4de gradspolynomium i $\mathbb{Q}[X]$ og lad M være spaltningslegemet for $f(X)$ over $\mathbb{Q}$. Antag $[M : \mathbb{Q}] = 8$. Vis, at $\mathrm{Gr}(M/\mathbb{Q})$ er isomorf med Diedergruppen D_4 af orden 8. (Benyt f.eks., at enhver undergruppe i S_4 af orden 8 er isomorf med D_4).

Opg. 63.

Lad $f(X)$ være et irreducibelt 4de gradspolynomium i $\mathbb{Q}[X]$ af formen X^4+aX^2+b og lad M være spaltningslegemet for $f(X)$ over $\mathbb{Q}$. Vis, at $\mathrm{Gr}(M/\mathbb{Q})$ må være $\mathbb{Z}/4$, Kleins Vierergruppe V_4 eller D_4.

Opg. 64.

Lad M_1, resp. M_2 være spaltningslegemet over $\mathbb{Q}$ for

$$f_1(X) = X^4 - 4X^2 + 2\,, \quad \text{resp. } f_2(X) = X^4 - 10X^2 + 1\,.$$

Angiv Galoisgrupperne $\mathrm{Gr}(M_1/\mathbb{Q})$ og $\mathrm{Gr}(M_2/\mathbb{Q})$.

Opg. 65.

Den anden opgave p. 3.12 i Noterne (Lad $f(X)$ være et irreducibelt etc.) [Vink til spørgsmål 4: Bemærk, at $X^4 f(1/X) = f(X)$ og slut heraf, at u er rod i $f(X) \Leftrightarrow 1/u$ er rod i $f(X)$, så rødderne må være af formen $u, v1/u, 1/v$.]

Opg. 66.

Lad $f(X)$ være et irreducibelt n-te gradspolynomium i $\mathbb{Q}[X]$ og lad M være spaltningslegemet over $\mathbb{Q}$. Vis, at $[M : \mathbb{Q}] = n$, såfremt $\mathrm{Gr}(M/\mathbb{Q})$ er abelsk. (Benyt, at $\mathrm{Gr}(M/\mathbb{Q})$ abelsk $\Rightarrow$ enhver undergruppe er normaldeler.)

$*$) Undersøg, om ovennævnte implikation kan vendes om.

Opg. 67.

Lad $M/\mathbb{Q}$ være en normal udvidelse, så $\mathrm{Gr}(M/\mathbb{Q}) \simeq Z/4$. Vis, at M ikke kan indeholde $i = \sqrt{-1}$. (Benyt, at $Z/4$ har netop eet element af orden 2 og at overgang til kompleks-konjugeret er en automorfi af orden 2.)

Opg. 68.

Lad M og N være endelige normale udvidelser af $\mathbb{Q}$ (opfattet som dellegemer af $\mathbb{C}$.) Vis, at kompositet MN er en endelig normal udvidelse af $\mathbb{Q}$. (Skriv M og N som spaltningslegemer for polynomier $f(X)$ og $g(X)$ over $\mathbb{Q}$ og betragt $f(X)g(X)$.)

Vis, at der findes en "naturlig" injektiv afbildning af $\mathrm{Gr}(MN/\mathbb{Q})$ ind i $\mathrm{Gr}(M/\mathbb{Q}) \times \mathrm{Gr}(N/\mathbb{Q})$.

Antag $M \cap N = \mathbb{Q}$ og vis, at i dette tilfælde er $\mathrm{Gr}(MN/\mathbb{Q})$ isomorf med det direkte produkt $\mathrm{Gr}(M/\mathbb{Q}) \times \mathrm{Gr}(N/\mathbb{Q})$.

Bestem Galoisgruppen for spaltningslegemet over $\mathbb{Q}$ for polynomiet $(X^3-2)(X^4-2)$.

Opg. 69.

Lad M/K være en endelig normal udvidelse. Vis, at et element $\alpha \in M$ er et primitivt element for M/K hvis og kun hvis $\sigma(\alpha) \neq \alpha$ for ethvert $\sigma \in \mathrm{Gr}(M/K)$, $\sigma \neq 1_M$.

Opg. 70.

Lad $P(X)$, $Q(X)$, $R(X)$ og $S(X)$ være polynomier med reelle koefficienter så $P(X^5) + XQ(X^5) + X^2R(X^5) = (1 + X + X^2 + X^3 + X^4)S(X)$. Vis, at $X - 1$ går op i $P(X)$. (Opgaven stammer fra 5-te USA "Mathematical Olympiad".)

Opg. 71.

Lad M være spaltningslegemet for $X^5 - 2$ over $\mathbb{Q}$. Angiv $[M : \mathbb{Q}]$ og vis, at $\mathrm{Gr}(M/\mathbb{Q})$ ikke er abelsk. Vis, at $\mathbb{Q}(\sqrt{5}) \subset M$. (Benyt, at $\cos 2\pi/5 = (\sqrt{5} - 1)/4$.)

Godtgør, at $M/\mathbb{Q}(\sqrt{5})$ er normal med en Galoisgruppe der er isomorf med D_5 (Diedergruppen af orden 10).

$*$) Angiv et irreducibelt 10de gradspolynomium i $\mathbb{Q}[X]$, hvis spaltningslegeme over $\mathbb{Q}$ er M. (Betragt $\mathrm{Irr}(\sqrt[5]{2} + \sqrt{5}\,, \mathbb{Q})$.)

Opg. 72.

Vis, at for ulige n gælder $\mathbb{Q}_{2n} = \mathbb{Q}_n$. (Vis f.eks. at $\mathbb{Q}_n$ og $\mathbb{Q}_{2n}$ har samme dimension over $\mathbb{Q}$.)

Opg. 73.

i) Vis, at $\mathbb{Q}_{10} = \mathbb{Q}_5$.
ii) Vis, at $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}_5$.
iii) Vis, at $\mathbb{Q}(\sqrt{5})$ er det eneste dellegeme af $\mathbb{Q}_5$, hvis dimension over $\mathbb{Q}$ er 2.
iv) Vis, at $x^{10} - 2$ er irreducibelt over $\mathbb{Q}_{10}$.

(Bevis og benyt, at $2^{t/10} \notin \mathbb{Q}_5$ for $1 \leq t \leq 9$; bemærk, at en ægte divisor i $X^{10} - 2$ måtte være et produkt af faktorer $((X - \sqrt[10]{2})\cdot(\text{10-nde enhedsrod}))$ og se på konstantleddet.)

v) Lad M være spaltningslegemet for $x^{10} - 2$ over $\mathbb{Q}$ og bestem $[M : \mathbb{Q}]$.
vi) Er $\mathrm{Gr}(M/\mathbb{Q})$ abelsk? Er $\mathrm{Gr}(M/\mathbb{Q})$ opløselig?

Opg. 74.

Vis, at $\mathbb{Q}_n \cap \mathbb{R} = \mathbb{Q}(\cos 2\pi/n)$. Angiv $[\mathbb{Q}(\cos 2\pi/n) : \mathbb{Q}]$.

[Benyt, at $\mathbb{Q}_n \cap \mathbb{R}$ er fixpunktslegeme for den automorfi i $\mathrm{Gr}(\mathbb{Q}_n/\mathbb{Q})$, der svarer til kompleks konjugering.]

Opg. 75.

Lad M_n være spaltningslegemet over $\mathbb{Q}$ for polynomiet $x^n + 1$. Bestem Galoisgruppen $\mathrm{Gr}(M_n/\mathbb{Q})$.

Opg. 76.

Lad $f(X)$ være et irreducibelt trediegradspolynomium i $\mathbb{Q}[X]$ med netop een reel rod. Angiv Galoisgruppen for spaltningslegemet over $\mathbb{Q}$.

Opg. 77.

Lad M være spaltningslegemet over $\mathbb{Q}$ for polynomiet x^4+5x^2+5. Undersøg, om M er lig det 5-te cirkeldelingslegeme $\mathbb{Q}_5$.

Opg. 78.

Lad K være et legeme af karakteristik 0, M en endelig normal udvidelse af legemet K og L en endelig udvidelse af K. Antag at $M \cap L = K$ og at kompositet ML er en endelig normal udvidelse af M. Vis, at ML er en normal udvidelse af K. (Vink: Vælg $\alpha \in L$, saa $L = K(\alpha)$ og vis, at $f(x) = Irr(\alpha, K)$ er irreducibelt i $M[X]$. Lad M være spaltningslegeme over K for et polynomium $g(x) \in K[X]$. Da er ML spaltningslegeme over K for $f(x)g(x)$.)

Vis ved et eksempel, at i ovennævnte situation vil L ikke nødvendigvis være normal over K.

Opg. 79.

Lad M/L og L/K være endelige normale udvidelser. Vis ved et eksempel, at M/K ikke nødvendigvis er en normal udvidelse.

Opg. 80.

Lad M/L og L/K være endelige normale udvidelser. Antag, at enhver automorfi i $\mathrm{Gr}(L/K)$ kan fortsættes til en automorfi for M. Undersøg, om dette medfører, at M/K er en normal udvidelse.
(Jfr. punkt 5 i Galoisteoriens Hovedsætning.)

Opg. 81.

Lad α være algebraisk over $\mathbb{Q}$ af grad n, hvor n er ulige. Undersøg, om $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2)$.

(Hvis udsagnet er rigtigt, ønskes givet et bevis. Hvis udsagnet er forkert, ønskes givet et modeksempel.)

Opg. 82.

Lad b være et reelt algebraisk tal af grad t (m.h.t. $\mathbb{Q}$) og lad i være $\sqrt{-1}$. Vis, at graden s (m.h.t. $\mathbb{Q}$) af tallet ib er lig $2t$, hvis i ligger i legemet $\mathbb{Q}(ib)$ og er lig t, hvis i ikke ligger i legemet $\mathbb{Q}(ib)$.

Opg. 83.($*$)

Lad α være et komplekst tal skrevet på formen $\alpha = a + ib$, hvor a og b er reelle tal og $i = \sqrt{-1}$. Vis, at α er algebraisk over $\mathbb{Q}$, hvis og kun hvis a og b er algebraiske over $\mathbb{Q}$.

Antag nu, at $\alpha = a+ib$ er algebraisk over $\mathbb{Q}$ og at dettes grad er n. Vis, at graden af a er højest $n(n-1)/2$ og graden af ib højest $n(n-1)$. Vis, at graden af ib er lig graden af b, hvis i ikke ligger i legemet $\mathbb{Q}(ib)$ og at graden af ib er det dobbelte af graden af b, hvis i ligger i legemet $\mathbb{Q}(ib)$.

Opg. 84.(∗)

Lad $\mathbb{Q}_n = \mathbb{Q}(e^{\frac{2\pi i}{n}}) = \mathbb{Q}(cos\frac{2\pi}{n} + isin\frac{2\pi}{n})$ være det n-te cirkeldelingslegeme. Vis, at for $n > 2$ er $[\mathbb{Q}(cos\frac{2\pi}{n}) : \mathbb{Q}] = \phi(n)/2$. Vis, at når n ikke er delelig med 4, er $\mathbb{Q}(isin\frac{2\pi}{n}) = \mathbb{Q}_n$ og har således dimensionen $\phi(n)$ over $\mathbb{Q}$. Når n ikke er delelig med 4, har $sin\frac{2\pi}{n}$ graden $\phi(n)/2$ over $\mathbb{Q}$.

Vis, at i $(= \sqrt{-1})$ ligger i $\mathbb{Q}_n$, netop når n er delelig med 4.

Vis, at $\mathbb{Q}(cos\frac{2\pi}{n}) = \mathbb{Q}(sin\frac{2\pi}{n})$ netop når n er delelig med 8.

Vis,at når $n > 4$ og $n \equiv 4 \pmod 8$ er $\mathbb{Q}(sin\frac{2\pi}{n})$ et ægte dellegeme af $\mathbb{Q}(cos\frac{2\pi}{n})$ og $[\mathbb{Q}(cos\frac{2\pi}{n}) : \mathbb{Q}(sin\frac{2\pi}{n})] = 2$.

Opg. 85.

Vis, at summen a_n af de primitive n'te enhedsrøddder er lig $\mu(n)$, hvor μ betegner Möbiusfunktionen. [Vink: Bemærk, at for $n > 1$ er summen af alle n'te enhedsrødder lig 0. Slut heraf, at for $n > 1$ er $\sum_{d|n} a_d = 0$. Bevis nu (under benyttelse af sætning 27 i Kap.II), at $a_n = \mu(n)$ for alle n ved induktion efter n.]

Opg. 86.

Lad $f(x)$ være et irreducibelt 5-te gradspolynomium med netop 3 reelle rødder, og lad M være spaltningslegemet over $\mathbb{Q}$ for $f(x)$.

Lad α, β, γ og δ være fire indbyrdes forskellige rødder i $f(x)$.

Vis, at $\alpha + \beta \neq \gamma + \delta$. (Betragt først tilfældet, hvor netop tre af disse rødder er reelle og udnyt derefter strukturen af $Gr(M/\mathbb{Q})$ som permutationsgruppe af de fem rødder i $f(x)$.)

Bestem $Gr(M/\mathbb{Q}(\alpha + \beta))$ og $Gr(M/\mathbb{Q}(\alpha - \beta))$ og undersøg, om $\mathbb{Q}(\alpha + \beta)$ er indeholdt i $\mathbb{Q}(\alpha - \beta)$.

Opg. 87.

Lad M/K være en endelig normal udvidelse med Galoisgruppe G. Lad L være et mellemlegeme mellem K og M og lad H være undergruppen i G bestående af de automorfier $\sigma \in G$ for hvilke $\sigma L = L$. Vis, at H er normalisatoren af TL i G.

Stikordsliste

A

Abelsk gruppe 1.1
Abelsk udvidelse 5.5
Abel-Steinitz's sætning 2.22
absolut normalrække 1.28
adjunktion af rod 2.12
afledet gruppe 1.10
algebraens fundamentalsætning 2.14
algebraisk element 2.8
algebraisk hylster 2.11
algebraisk udvidelse 2.9
alternerende gruppe 1.20
$\mathrm{Aut}(G)$ 1.5
$\mathrm{Aut}_i(G)$ 1.5
automorfi for gruppe 1.5
automorfi for legeme 3.1

B

basis 1.42
Burnside's Verlagerungssætning 1.38

C

Cardanos formel 5.10
Cayley's sætning 1.18
centralisator af element 1.12
centralisator af undergruppe 1.9 og 1.39
centrum 1.2
cirkeldelingslegeme 4.5
cirkeldelingspolynomium 4.1
cykel 1.20
cyklisk gruppe 1.2
cyklisk udvidelse 5.5

D

diedergruppe 1.11
direkte faktor, produkt 1.8

direkte sum	1.52
Dirichlets sætning	4.4
diskriminant	2.26
divisor, største fælles	2.16
dobbelt transitiv gruppe	1.18
D_n	1.11

E

Eisensteins irreducibilitetskriterium	2.4
elementærdivisorsætningen	1.44
enhedsrod	4.1
Eulers kriterium	6.2

F

$\mathcal{F}$ (fixpunktslegeme)	3.1
faktorgruppe	1.4
Fermat'ske primtal	4.10
fixpunktslegeme	3.1
fjerdegradsligning	5.11
forfining	1.24
forkortningssætningen	1.53
formel differentiation	2.19
Freshman's Dream	2.18
fri	1.42
Frobeniusautomorfien	2.18
fuldkommen gruppe	1.6
fuldkomment legeme	2.21

G

Galoisfelt	2.24
Galoisgruppe	3.6
Galois' sætning ang. A_n	1.22
Galoisteoriens hovedsætning	3.8
Gauss' sætning om primitive polynomier	2.2
Gauss' sætning om konstruktion af regulære polygoner	4.8
Gr, relativ automorfigruppe, Galoisgruppe	3.1

H

hexaedergruppe	1.18

Hilbert Satz 90 5.2
homomorfi 1.3
homomorfisætningen 1.4
hovedideal 2.1
hovedidealområde 2.1
hovedsætning ang. opløselighed ved rodtegn 5.8
hovedsætning om endeligt frembragte abelske grupper 1.52
højreækvivalent 1.3

I

ideal 2.1
ikosaedergruppe 1.18
index 1.3
indre automorfi 1.5
$\mathrm{Irr}(\alpha, K)$ 2.8
isomorfe normalrækker 1.25
isomorfe grupper 1.3

J

Jacobisymbolet 6.7
Jordan-Hölders sætning 1.25

K

kanonisk homomorfi 1.4
karakteristik af legeme 2.17
karakteristisk undergruppe 1.5
Ker, kerne for homomorfi 1.4
klasseligningen 1.13
Kleins Vierergruppe 1.11
kohomologigruppe 5.1
kommutativ gruppe 1.1
kommutativ ring 2.1
kommutator 1.10
kommutatorgruppe 1.10
komposition 1.1
kompositionsrække 1.24
kompositum af legemer 3.9
konjugerede elementer 1.12
konjugerede undergrupper 1.32
Kronecker-Webers sætning 4.6

krydset homomorfi	5.1
kvadratisk rest	6.1
kvadratiske reciprocitetssætning	6.3
kvotientgruppe	1.4

L

Lagranges sætning	1.2
legeme	2.1
Legendresymbolet	6.1

M

maksimalt ideal	2.1
Mersennetal	6.6
meta-abelsk	5.5
multipel rod	2.19
Möbius-funktion	2.25

N

nilpotent	1.30
Noethers isomorfisætninger	1.9 og 1.10
normal undergruppe	1.4
normal udvidelse	3.2
normaldeler	1.4
normalisator af undergruppe	1.32
normalrække	1.24

O

opløselig gruppe	1.28
opløselighed ved rodtegn	5.7
orden	1.2
overopløselighed	1.30

P

p-gruppe	1.12
p-Sylow gruppe	1.31
PID (= hovedidealområde)	2.1
permutationsgruppe	1.18
praktisk lemma	3.2

primitiv enhedsrod	4.1
primitivt element	2.22
primitivt polynomium	2.2
primideal	2.1

Q

$\mathbb{Q}_n$, det n'te cirkeldelingslegeme	4.5
quaterniongruppen	1.14

R

radikaludvidelse	5.5
relativ automorfigruppe	3.1

S

Schreiers forfiningssætning	1.25
Schönemann-Eisensteins sætning	2.4
separabel	2.21
sideklasse	1.3
simpel algebraisk udvidelse	2.22
simpel gruppe	1.6
simpel rod	2.19
S_n, den n'te symmetriske gruppe	1.18
spaltningslegeme	2.14
spor	3.5
stabilitetsgruppe	1.16
største fælles divisor for polynomier	2.16
Sylows sætninger	1.31
symmetrisk gruppe	1.18
symmetriske polynomier	2.5

T

tetraedergruppen	1.16
torsion	1.42
transcendent	2.8
transitiv	1.18
transitivitetssætningen	2.10
translationssætningen	3.12
transposition	1.20
trediegradsligning	5.10

U

UFD (= faktoriel ring) 2.2
unimodulær 1.43

V

venstreækvivalent 1.3
Ver, verlagerung 1.36
V_4, Kleins Vierergruppe 1.11

Z

Zassenhaus' lemma 1.25
$Z(G)$, centrum for G 1.2