Kapitel I. Grupper

Def. G mængde med kompositionsforskrift $\circ$. G kaldes gruppe, hvis

1) $\circ$ associativ ($\wedge$: $(a \circ b) \circ c = a \circ (b \circ c)$ $\forall a,b,c \in G$)

2) $\exists$ neutralt element e ($\wedge$: $e \circ g = g \circ e = g$ $\forall g \in G$)

3) $\forall g \in G$ har et inverst element g^{-1} ($\wedge$: $g \circ g^{-1} = g^{-1} \circ g = e$) .

Bem. Det neutrale element e i ovenstående er nødvendigvis entydigt bestemt.

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

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

Da gælder potensreglerne

$$g^{n+m} = g^n \circ g^m \qquad \forall, n,m \in \mathbb{Z}$$

$$(g^n)^m = g^{nm} \qquad \forall n,m \in \mathbb{Z} .$$

Derimod gælder $(a \circ b)^n = a^n \circ b^n$ normalt ikke.

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

Def. En gruppe kaldes kommutativ (eller abelsk), hvis alle elementerne er indbyrdes ombyttelige.

Def. $(G,\circ)$ gruppe. S delmængde i G. S kaldes undergruppe af

(G,o), hvis S med o udgør gruppe i henhold til ovenstående definition.

Sætning. (G,o) gruppe. S delmængde i G. Da gælder S undergruppe hvis og kun hvis $a,b \in S \Rightarrow a \circ b^{-1} \in S$.

Bevis. Simpel øvelse.

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

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

Definition. G kaldes cyklisk, hvis G frembragt af et enkelt element. hvis $\exists g \in G$ så $G = \{g^n | n \in \mathbb{Z}\}$.

Kendt fra Mat. 1 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 Ord a af et element $a \in G$ forstås ordenen af den af a frembragte undergruppe.

Lagrange's sætning. Hvis G endelig, vil Ord a $||G|$ for alle $a \in G$.

Bemærkning. Klart, at G endelig $\Rightarrow$ alle elementer i G har endelig orden.

Eksempel. Ej $\Leftarrow$. Mængden af alle komplekse enhedsrødder $\{e^{\frac{2\pi}{n}a}$, $n \in \mathbb{N}$, $a \in N$ udgør med sædvanlig multiplikation en uendelig gruppe, hvor alle elementer har endelig orden.

Sætning. 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 $Z(G) = G \Leftrightarrow G$ 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 $f(g_1 \circ g_2) = f(g_1) \circ f(g_2)$ $\forall g_1\ g_2 \in G$. Øjensynlig gælder $f(e)$ = neutralt element i G og $f(g^{-1}) = f(g)^{-1}$ for en homomorfi f. Hvis desuden f er bijektiv, kaldes f en isomorfi og G og H isomorfe grupper. Isomorfe grupper er "i det væsentlige" ens.

Eksempel. Enhver cyklisk gruppe er isomorf med $\mathbb{Z}_n$ for passende $n \in \mathbb{N}$ eller $\mathbb{Z}$.

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 a_v indeholdende a består af elementerne $\{sa \mid s \in S\}$, hvilket kort skrives $a_v = Sa$. 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 side-klasser med hensyn til S. Tilsvarende for "$\underset{h}{\sim}$".

Hvis $\{a_i\}$ udgør fuldstændigt repræsentationssystem for venstre side-klassen vil $\{a_i^{-1}\}$ udgøre fuldstændigt repræsentationssystem for højre side-klasser. Følgelig findes lige mange venstre side-klasser og højre side-klasser.

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

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

Sætning. 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) ⇒ 2) 1) ⇒ 3) 1) ⇒ 4) 3) ⇒ 4) 4) ⇒ 5) 5) ⇒ 1).

1) ⇒ 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) ⇒ 3). Analogt.

2) ⇒ 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) ⇒ 4). Analogt.

4) ⇒ 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) ⇒ 1). Antag $a \underset{v}{\sim} b$ $ab^{-1} \in S$ og dermed $ba^{-1} \in S$ hvorfor analogt ses, at $a \underset{h}{\sim} b \Rightarrow a \underset{v}{\sim} b$.

Definition. En undergruppe S i gruppen G kaldes normaldeler (eller normal undergruppe) i G, hvis en 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 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 $a \cdot b = a \cdot b$ defineres en komposition på mængden af sideklasser. Disse udgør herved 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 $\kappa g = \textcircled{g}$ er en surjektiv homomorfi. κ betegner den kanoniske homomorfi fra G på G/S.

For en homomorfi f fra en gruppe G til en gruppe H vil kernen, $\mathrm{Ker}\, f = \{g \in G \mid f(g) = e\}$ være 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 $\mathrm{Ker}\, f \lhd G$ og $G/\mathrm{Ker}\, f \sim H$. Mere præcist: der findes netop een isomorfi $\bar{f}$ fra G/Ker f til H så $f = \bar{f} \circ \kappa$ hvor κ er den kanoniske homomorfi fra G på G/Ker f.

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

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

$$f^* \circ \kappa(g) = f^*(g) = f(g) \quad \forall g \supset : f^* = \bar{f}. \qquad \|$$

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

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, $\mathrm{Aut}_i(G)$, i $\mathrm{Aut}(G)$.

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

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

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

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

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, $k_g(H) \subseteq H \ \forall k_g$. I den forbindelse indføres begrebet karakteristisk undergruppe:

Definition. En undergruppe H i gruppen G kaldes karakteristisk, hvis $\varphi H \subseteq H$ for alle automrofier $\varphi \in \mathrm{Aut}(G)$.

Enhver karakteristisk undergruppe er således specielt normaldeler.

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 (: K karakteristisk i H og H karakteristisk i G $\Rightarrow$ K karakteristisk i G). Det tilsvarende gælder ikke for normale undergrupper.

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

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

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

Sætning. Automorfigruppen 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. $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) = (aba^{-1})b \in A \cap B$

$\therefore (ab) = a^{-1}b^{-1} = e$ og dermed $ab = ba$.

Vi skal vise, at Aut(G) har trivielt centrum og at enhver automorfi for Aut(G) er indre.

Vi viste p. 6 at $\mathrm{Aut}_i(G) \triangleleft \mathrm{Aut}\ G$.

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

Bevis. $\alpha k_g[x] = \alpha(gxg^{-1}) = \alpha g \alpha x (\alpha g)^{-1}$,

$k_g \alpha[x] = g\alpha(x)g^{-1}$.

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

1^o indebærer specielt, at Aut(G) har trivielt centrum.

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

Bevis. $\psi(\mathrm{Aut}_i(G)) < \mathrm{Aut}(G)$, dermed $\psi(\mathrm{Aut}_i(G)) \cap \mathrm{Aut}_i(G) < \mathrm{Aut}_i(G) \simeq G/Z(G) \simeq G$. (Jfr. p. 6). Da G 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^o. Altså gælder $\psi(\mathrm{Aut}_i(G)) \supseteq \mathrm{Aut}_i(G)$.

Dette gælder for alle ψ, dermed $\psi^{-1}(\mathrm{Aut}_i(G)) \supseteq \mathrm{Aut}_i(G)$, 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.

Bevis. Lad $\beta \in \mathrm{Aut}\ G$. Da er (p. 6) $\beta k_g \beta^{-1} = k_{\beta g}$. Heraf $\psi(\beta)\psi(k_g)\psi(\beta)^{-1} = \psi(k_{\beta g})$, der på grund af forudsætningen reduceres til $\psi(\beta)k_g\psi(\beta)^{-1} = k_{\beta g}$. For ethvert $x \in G$ er således $\psi(\beta)k_g\psi(\beta)^{-1}[x] = k_{\beta g}[x]$ eller

$$\psi(\beta)[g\psi(\beta)^{-1}xg^{-1}] = \beta g x(\beta g)^{-1}$$
$$\| \qquad\qquad\qquad\qquad \|$$
$$\psi(\beta)(g)x(\psi(\beta)g)^{-1}, \quad \text{hvoraf}$$

$(\beta g)^{-1}\psi(\beta)(g)x = x(\beta g)^{-1}\psi(\beta)g$, og hermed $(\beta g)^{-1}\psi(\beta)g \in Z(G)$ så $\beta(g) = \psi(\beta)(g) \forall g$ dvs. $\beta = \psi(\beta)$. ∎

4°. 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 (jfr. sætn. p. 6) 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 $Z(G) = e$ og sætn. p.6 ses α at være injektiv. På grund af 2° er α også

surjektiv $\supset$: α er bijektiv.

Vi mangler at vise, 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 $\alpha(g_1 g_2) = \alpha g_1 \cdot \alpha g_2$. ‖

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

Bevis. På grund af $\underline{4^o}$ 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 ifølge p.6 $k_{\alpha g} = \alpha k_g \alpha^{-1}$.

Hermed er beviset for Sætning p.7 afsluttet.

- - - - - - - - - - -

Lad H og K være undergrupper i Gruppen G. Med HK betegner vi delmængden $\{hk \mid h \in H, k \in K\}$.

Sætning. For undergrupper H og K i G gælder:

HK er undergruppe i $G \Leftrightarrow HK = KH$.

Bevis. $\Rightarrow$: Vi viser $KH \subseteq HK$ og $HK \subseteq KH$.

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

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

$\Leftarrow$ 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 $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. ‖

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

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

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

Sætning. Hvis $H \triangleleft G$, $K \triangleleft G$, $HK = G$, $H \cap K = e$, da kan ethvert $g \in G$ på entydig vis skrives $g = hk$ ($h \in H$, $k \in H$), 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 $g = hk = \tilde{h}\tilde{k}$, $h, \tilde{k} \in H$, $k, \tilde{k} \in K$. Da var $\tilde{h}^{-1}h = \tilde{k}k^{-1} \in H \cap K = e$, dvs. $h = \tilde{h}$, $k = \tilde{k}$.

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 $(h_1k_1)(h_2k_2) = h_1(h_2k_1)k_2$. ∎

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.

Sætning. 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 $H < G$. Afbildningen $h \to ghg^{-1}$ er derfor en automorfi for H. Da H er fuldkommen findes ethver g entydig 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: $K = \{k \in G \mid hk = kh \text{ for alle } h \in H\}$.

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 $G = HK \Leftrightarrow G = KH$]. Endvidere da centrum for H er $\{e\}$, bliver $H \cap K = \{e\}$. Mangler blot at vise $K \lhd G$.

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. ∎

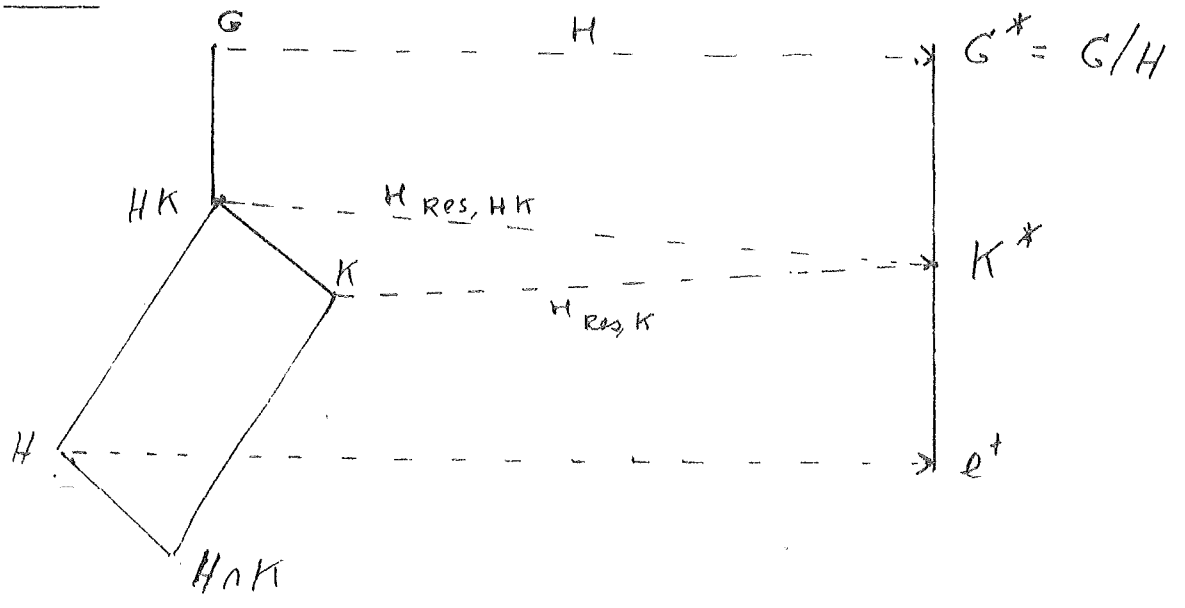
Bemærkning. Man kan omvendt vise, at en gruppe med trivielt centrum er fuldstændig, såfremt den er direkte faktor i enhver gruppe der indeholder den som normaldeler.

- - - - -

Nu to vigtige isomorfisætninger.

Noethers 1. isomorfisætning. Lad H og K være undergrupper i gruppen G og antag $H \lhd G$; da er $H \cap K \lhd K$ og $HK/_H \cong K/_{H\cap K}$.

Bevis.



Lad κ betegne den kanoniske homomorfi af G på G/H, her betegnet G^*. Da er $\kappa(HK) = \kappa(K)$, $\kappa(HK) \supseteq \kappa(K)$ 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, $\kappa_{Res,K}$; homomorfisætningen anvendt på $\kappa_{Res,K}$ giver: $K^* \simeq K/_{Ker(\kappa_{Res,K})}$. Nu er

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

Følgelig er $H \cap K < K$ og $K/_{H\cap K} \simeq K^*$.

Dernæst betragtes $\kappa_{Res,HK}$. Her er $Ker(\kappa_{Res,HK}) = H$ 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 $K \to \kappa K \subseteq G^*$ og $K^* \to \kappa^{-1}(K^*)$ en $|-|$ korrespondance mellem undergrupperne K i G indeholdende H og undergrupperne K^* i G^*. Ved denne korrespondance gælder $K \trianglelefteq G \Leftrightarrow \kappa K \trianglelefteq G^*$. Hvis $K \trianglelefteq G$, da er $G/K \simeq G^*/\kappa K$. (Hvis κK skrives K/H, kan isomorfien formuleres $G/K \simeq G/H/K/H$.)

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

Ad ii) $\kappa\kappa^{-1}K^* \subseteq K^*$ 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 $\kappa^{-1}(K^*)$ $\supset$: $k^* \in \kappa\kappa^{-1}(K^*)$.

$$K \lhd G \Rightarrow_K g_K k_K g^{-1} = \kappa(gkg^{-1}) \in \kappa K \text{ for } \forall k \in K, \ \forall g \in G$$

$$\kappa K \lhd G^*.$$

Antag $K^* \lhd G^*$; 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. $\kappa^{-1}K^* < G$.

Hvis $K \lhd G$ 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 $\text{Ker } \kappa^*\kappa = K$. Homomorfisætningen giver da $G/K \simeq G^*/K^*$.

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 $a_1^{n_1} \cdots a_r^{n_r}$, $a_1, \ldots, a_r \in A$, $n_1, \ldots, n_r \in \mathbb{Z}$, $r \in \mathbb{N}$. (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 $G' < G$.

Den følgende sætning giver en karakterisering af kommutatorgruppen.

Sætning. For en undergruppe H i G gælder:

$$H \supseteq G' \Leftrightarrow H < G \text{ og } G/H \text{ abelsk.}$$

Specielt er G' den mindste normaldeler med abelsk faktorgruppe.

Bevis. "$\Rightarrow$" ved $G' < G$; endvidere er ifølge Definitionen af G' $aba^{-1}b^{-1} \in G'$ for $\forall a,b$ $\supset$: $\overline{a}\,\overline{b}\,\overline{a}^{-1}\,\overline{b}^{-1} = \overline{e}$ i G/G' (her betegner $\overline{a}$ a's sideklasse i G/G'). Altså er $\overline{a}\overline{b} = \overline{b}\overline{a}$ $\supset$: G/G' er abelsk.

Lad κ være den kanoniske homomorfi $G \to G/G'$. Da enhver undergruppe i den abelske gruppe G/G' er normaldeler, er $\kappa H < G/G'$ for enhver undergruppe H G med $H \supseteq G'$. Ifølge 2. isomorfisætning er $H \lhd G$, og G/H er homomorft billede af en abelsk gruppe og derfor selv abelsk.

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

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

- - - - -

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 en gruppe af orden n, nemlig den cykliske $\mathbb{Z}_n$.

For ethvert lige tal $2n$, $n \geq 3$, 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 og betegnes D_n.

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

Bevis. Ethvert fra e forskelligt element i G vil frembringe G. ∎

Sætning. 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. Klart, at $\mathbb{Z}_4$ og V_4 er ikke-isomorfe grupper af orden 4. Nok at vise, at der højest findes en ikke-cyklisk gruppe af orden 4. G ej cyklisk $\Rightarrow$ ordenen af ethvert element = 1 eller 2 $\supset$: ifølge sætning p.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 højest en mulighed for gruppetavlen.

Sætning. Lad p = 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. 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 $2p$.

1^0. 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. $|G/A| = p$ ⁘: G/A cyklisk. Lad (g) være frembringerelement, altså $(g) \neq (e)$ $(g^p) = (e)$; ⁘: for en repræsentant g gælder $g \notin A$, $g^p \in A$. Men ethvert kvadrat i G er e, ⁘: $g^2 = e$; følgelig $g = g^p(g^2)^{\frac{p-1}{2}} \in A$. Modstrid:

2^0. G har et element af orden 2. Vises analogt med 1^0. (Her benyttes, at en undergruppe af orden p har index 2 og derfor er normaldeler i G.)

3^0. Lad nu a være et element af orden p og b et element af orden 2. G består netop af elementerne $e,a,a^2,\ldots,a^{p-1}$, b, ba, $ba^2,\ldots,ba^{p-1}$. 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 $A \triangleleft G$ og G/A cyklisk af orden 2. Sideklassen (ab) i G/A har orden 2, hvorfor ord(ab) indenfor G er 2 eller $2p$. Her er $2p$ udelukket, da G ellers var cyklisk i strid med den gjorte antagelse. ⁘: $(ab)^2 = e$ eller $ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{p-1}$.

Hermed fastlægges entydigt hvorledes elementerne i G multipliceres, dvs. kun een 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 ej nødvendigvis p-gruppe) indføres følgende ækvivalensrelation: Lad a og b være elementer i G. Da defineres $a \sim b \Leftrightarrow \exists g \in G$ 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. Vi spørger nu: Hvor mange elementer indeholder ækvivalensklassen (a) indeholdende a? Hertil indføres $N_a = \{g \in G | ga = ag\}$. N_a er undergruppe i G og betegnes normalisatoren for a.

Elementerne i (a) er $\{gag^{-1} | g \in G\}$. For disse gælder

$$g_1 a g_1^{-1} = g_2 a g_2^{-1} \Leftrightarrow g_2^{-1} g_1 a = a g_2^{-1} g_1 \Leftrightarrow g_2^{-1} g_1 \in N_a$$

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

Vi bemærker, at $[G:N_a] = 1 \Leftrightarrow N_a = G \Leftrightarrow ag = ga \ \forall g \in G \Leftrightarrow$ $a \in$ Centrum for G. Ækvivalensklassen a består altså kun af elementet a netop når $a \in$ Centrum for G.

Antag nu atter, at G er en p-gruppe. Vi betragter den ovenfor indførte ækvivalensrelation. Hvis $a \notin$ centrum, er $[G:N_a] > 1$ og da $|G| = [G:N_a] \cdot |N_a| =$ p-potens vil $p | [G:N_a]$. Ved direkte optælling fås:

$$|G| = |\text{Centrum}| + \sum_{\substack{\text{visse } a \\ [G:N_a]>1}} [G:N_a]$$

hvor sidste summation udstrækkes over et repræsentantsystem for de ækvivalensklasser der indeholder mere end 1 element. For disse vil $p \mid [G:N_a]$. Idet $p \mid \mid G \mid$ fås $p \mid \mid \text{Centrum} \mid$, dvs. centrum ej triviel. Vi har altså vist

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

Vi giver nu en anveldelse.

Sætning. Hvis p = primtal findes netop to ikke-isomorfe grupper af orden p^2, nemlig den cykliske $\mathbb{Z}_{p2}$ og gruppen af diagonalmatricer af formen

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

Disse er begge abelske.

Bevis. Klart, at de to 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 vise, at der højest er en ikke-cyklisk gruppe af orden p^2.

Lad G være ikke-cyklisk gruppe af orden p^2. Ifølge omstående sætning findes et element $a \neq e$, G's centrum. Da G ej er cyklisk, er $a^p = e$. Undergruppen $A = \{e, a, a^2, a^{p-1}\}$ er normal i G, og G/A er cyklisk af orden p. Lad $\textcircled{b}$ være frembringer for G/A, d: $\textcircled{b}^p = e$ $\textcircled{b} \neq e$. Da G ej cyklisk, har b orden p. Idet $G/A = \{e, b, b^2, \ldots, b^{p-1}\}$ kan ethvert element i G entydigt skrives $a^i b^j$, $0 \leq i \leq p-1$, $0 \leq j \leq p-1$. Da $a \in$ G's centrum gælder $(a^{i_1} b^{j_1}) a^{i_2} b^{j_2}) = a^{i_1+i_2} b^{j_1+j_2}$. Idet som ovenfor nævnt $a^p = b^p = e$ er gruppetavlen for G hermed entydigt bestemt. ∎

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 siden 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) Diedergrupperne D_4 (: alle drejninger og spejlinger der fører et kvadrat over i sig selv).

V) Quaterniongruppen : de quaternioner $a_0+a_1 i+a_2 j+a_3 k$, hvor én af koefficienterne er ± 1 og de øvrige 0 dvs. $\pm 1, \pm i, \pm j, \pm k$.

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 - på nær 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 ej 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. $g^2 = e$ $\forall g \in G$. 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 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). $(b^2) =$ (e) dvs. $b^2 \in A$. Hvis b^2 var = a eller a^3, ville G være cyklisk med b som fremrbinger 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 normalt. Vi kan nu fuldstændiggøre skemaet p. 18

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 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

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

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

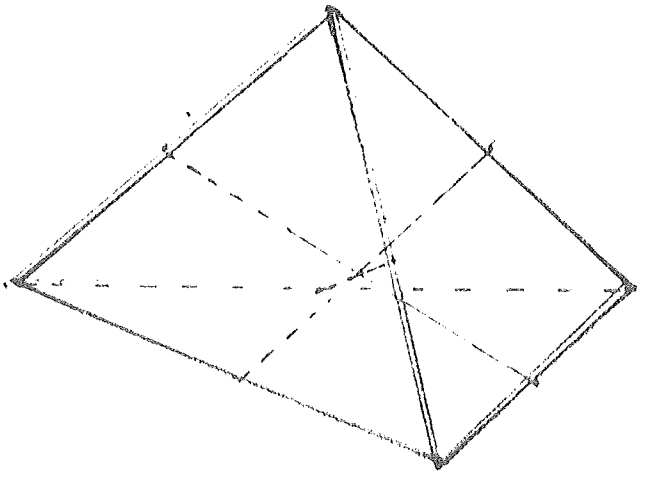
Vi skal nu betragte visse endelige grupper der har en simpel geometrisk interpretation.

Tetraeder gruppen 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 $T = A_4$. Bestemmelsen af normaldelerne i T kan ske ved følgende almene

Sætning. Lad M være en abstrakt mængde og G en gruppe af transformationer (: bijektive afbildninger) af M. For $a \in M$ lad $G_a = \{\varphi \in G | \varphi(a) = a\}$ ("Stabilitetsgruppen for a"). Da gælder for ethvert $\psi \in G$: $\psi \cdot G_a \cdot \psi^{-1} = G_{\psi(a)}$.

Bevis: Trivielt. ∎

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



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

Heraf sluttes specielt:

$$\mathcal{H}' = T$$
$$\mathcal{K}'' = T' = V_4$$
$$\mathcal{K}''' = T'' = V_4' = e.$$

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, $\mathcal{I} \cong$ Alternerende gruppe A_5 (se model).

Ved argumenter udnyttende sætning p. 23 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 endelig drejningsgrupper i rummet. Anderledes udtrykt udgør disse (på nær ortogonal ækvivalens) de eneste endelige undergrupper i den egentligt ortogonale gruppe $O^+(\mathbb{R})$. $O^+(\mathbb{R})$ kan vises at være simpel og 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.

Vi giver nu nogle små sætninger vedrørende dobbelt transitive permutationsgrupper.

Sætning. 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 $\tilde{\sigma}(c) = d$ for passende $\tilde{\sigma} \in N$.

Da G dobbelt transitiv findes $\tau \in G$ så $\tau(c) = a$ og $\tau(d) = b$. Men så gælder $\tau\bar{\sigma}\tau^{-1}(a) = b$. Da $N \lhd G$ er $\tau\bar{\sigma}\tau^{-1} \in N$ ∋ $\tau\bar{\sigma}\tau^{-1}$ er et brugbart σ. ∎

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

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

Bevis. Lad $\mathcal{H}$ være undergruppe i G og antag $\mathcal{H} \supsetneq G_a$. 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. $\rho^{-1}\sigma\tau \in G_a \subseteq \mathcal{H}$; 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. 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 $\{\sigma K \sigma^{-1} | \sigma \in G\}$.

Bevis. Antag $E \neq N \triangleleft G$; vi skal da vise, at $N = G$. Vælg et $a \in \Omega$ så (ii) gælder. G_a er maximal så G_aN er $= G_a$ eller G. Da N ifølge Sætning p. 25 er transitiv og G_a ikke er transitiv (idet $|\Omega|>1$) er muligheden $G_aN = G_a$ udelukket. Dvs. $G = G_aN$. Vi påstår nu, at $NK \triangleleft G$. (Bemærk NK er undergruppe, da $N \triangleleft G$). Da $G = G_aN$ $(= NG_a)$, kan ethvert element i G skrives $\nu\sigma$, hvor $\nu \in N$, $\sigma \in G_a$, og vi har, da $N < G$ og $K < G_a$

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

Da $K \subseteq NK \triangleleft G$, gælder

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

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

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 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 $N \triangleleft G$. 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: $A_n \triangleleft S_n$.

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

Sætning. 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 $\begin{pmatrix} a & \sigma a & \dots & \sigma^{k-1}a \\ \sigma a & \sigma^2 a & \dots & a \end{pmatrix}$ og vi er færdige; hvis $k < n$ vælge 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

$$\sigma = \begin{pmatrix} a & \dots,\sigma^{k-1}(a) \\ \sigma a & a \end{pmatrix}\begin{pmatrix} b & \dots,\sigma^{\ell-1}(b) \\ \sigma b & b \end{pmatrix}$$

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 indb. disjunkte cykler (bemærk faktorernes rækkefølge er ligegyldig, da cykler af indb. 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

$\tau_1 = \begin{pmatrix} a & \dots & \sigma^{k-1}a \\ \sigma a & & a \end{pmatrix} = \tau_i$; etc. ∎

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

Bevis. Ved at betragte cykler:

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

Bemærkning. En cykel af lige længde er ulige permutation.

En cykel af ulige længde er lige permutation.

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

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

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

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 $\tau\sigma(2) = 2$.

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: $\forall \sigma \in S_n \setminus \{e\}$ $\exists \tau \in S_n$ ses $\sigma\tau \neq \tau\sigma$. ∎

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

Bemærkning. Man kan vise, at for $n \neq 2$, $n \neq \sigma$ er S_n fuldstændig ⊃: $\mathrm{Aut}(S_n) = S_n$. Nu vigtig sætning:

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

Bevis. Lad $N \trianglelefteq A_n$, $N \neq \{e\}$. Skal da vise $N = A_n$. Da $N \trianglelefteq A_n$ 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 cykler af indbyrdes disjunkte elementer. 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)

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

Påstand: $\begin{pmatrix}a&b&c&d\\b&a&d&c\end{pmatrix} \in N \quad \forall a,b,c,d \in \{1,\ldots,n\}$.

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

$\begin{pmatrix}a&b\\b&a\end{pmatrix}\begin{pmatrix}1&2&3&4&\ldots\\a&b&c&d&\ldots\end{pmatrix} = \begin{pmatrix}1&2&3&4&\ldots\\b&a&c&d&\ldots\end{pmatrix}$ kan vi antage, at $\tau = \begin{pmatrix}1&2&3&4&\ldots\\a&b&c&d&\ldots\end{pmatrix}$ er lige. Da er $\tau\begin{pmatrix}1&2&3&4\\2&4&3\end{pmatrix}\tau^{-1} = \begin{pmatrix}a&b&c&d\\b&a&d&c\end{pmatrix} \in N$.

Følgelig indeholder N samtlige produkter af to transpositioner af indbyrdes forskellige elementer. Da ethvert $\sigma \in A_n$ er produkt af lige total 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 tal. Men dette følger af:

$(xy)(yz) = (xy)(uv)(uv)(yz)$, hvor u og v er valgt forskellige fra x,y og z. (Her udnyttes $n \geq 5$). ∎

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

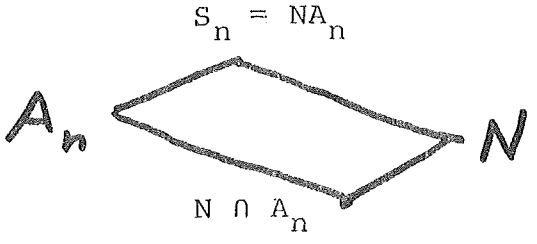
Sætning. For $n \geq 5$ er A_n eneste ikke-trivielle normaldeler i S_n.

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

1) $N \subseteq A_n \Rightarrow N \triangleleft A_n \overset{\Rightarrow}{(\text{Galois' sætn.})} N = A_n$ eller e.

2) $N \not\subseteq A_n \Rightarrow NA_n \supsetneq A_n \Rightarrow NA_n = S_n$.

Vi anvender Noethers 1. isomorfisætning på:



$A_n \cap N < A_n \Rightarrow A_n \cap N = e$ eller $A_n \cap N = A_n$.

$A_n \cap N = A_n \Rightarrow A_n \subseteq N$, hvilket på grund af $N \not\subseteq A_n$ 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 Sætn. p. 29 har S_n trivielt centrum. ∎

Korollar. For $n \geq 5$ 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 $\Omega = \{1,2,...\} = \mathbb{N}$ 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 $A_{\mathbb{N}} = \bigcup_{n=1}^{\infty} A_n$ og benyt Galois' sætning).

Opgave. Giv eksempel på følge $G_1 \supseteq G_2 \supseteq G_3 \supseteq \ldots$ af simple grupper for hvilken $\bigcap_{n=1}^{\infty} G_n$ ej er simpel.

- - - - - - - -

Normalrækker og opløselighed.

Ved en normalrække i gruppen G forstås en følge af undergrupper

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

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

$$G = G_0 > \tilde{G}_1 > \tilde{G}_2 > \ldots > \tilde{G}_t = \{e\} \qquad (\dagger)$$

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

Definition. En normalrække i G kaldes en kompositionsrække, hvis den er uden gentalgelser og ikke tillader nogen ægte forfining uden gentagelser. Ved hjælp af Noethers 2. isomorfisætning vises let:

Sætning: Hvis (*) er en normalrække uden gentagelser, gælder

(*) er kompositionsrække $\Leftrightarrow$ faktorerne er simple grupper.

Desuden gælder trivielt

Sætning: G endelig $\Rightarrow$ G har en kompositionsrække.

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

Imidlertid gælder:

Sætning. For abelske grupper G gælder: G endelig $\Leftrightarrow$ G har kompositionsrække.

Bevis. Benyt at en simpel abelsk gruppe er endelig (endda af primtalsorden). ∎

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 p. 31 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-Hölder.

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 $H_1 \lhd H_2$, $K_1 \lhd K_2$. 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) $H_1(H_2 \cap K_1) \lhd H_1(H_2 \cap K_2)$

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

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 $H_1 \lhd H_2$ og $K_1 \lhd K_2$.

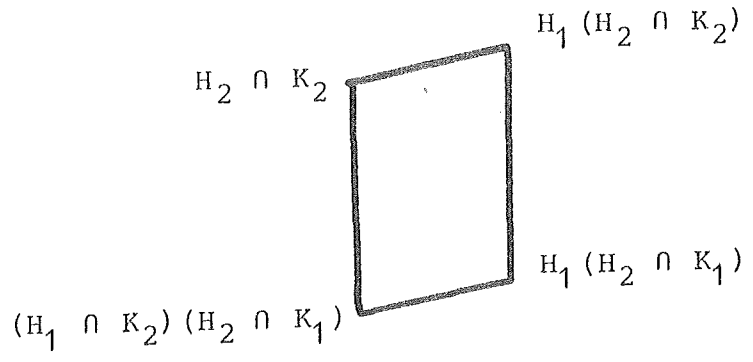
Et element i $H_1(H_2 \cap K_1)$ kan skrives hx, $h \in H_1$; $x \in H_2 \cap K_1$ og et element i $H_1(H_2 \cap K_2)$ kan skrives $\tilde{h}y$, $\tilde{h} \in H_1$; $y \in H_2 \cap K_2$. Elementet

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

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 $H_1(H_2 \cap K_1) < H_1(H_2 < K_2)$. Vi anvender Noether's 1. isomorfisætning på:



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:

$$H_1(H_2 \cap K_2)/H_1(H_2 \cap K_1) \simeq H_2 \cap K_2/(H_1 \cap K_2)(H_2 \cap K_1) \qquad (\dagger)$$

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

$$K_1(H_2 \cap K_2)/K_1(H_1 \cap K_2) \simeq H_2 \cap K_2/(H_1 \cap K_2)(H_2 \cap K_1) \qquad (\dagger\dagger)$$

$(\dagger)$ og $(\dagger\dagger)$ giver den ønskede isomorfi i (iii). ∎

Vi er nu i stand til at vise Schreier's forfiningssætning:

Lad $G = H_0 \rhd H_1 \rhd \ldots \rhd H_s = \{e\}$ (*)

og

$G = K_0 \rhd K_1 \rhd \ldots \rhd K_t = \{e\}$ (**)

være to vilkårlige normalrækker i G.

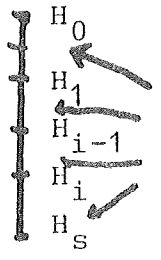
Vi angiver nu følgende forfining af (*) idet (**) "indplantes" mellem H_{i-1} og H_i for alle $i = 1,\ldots,s$:

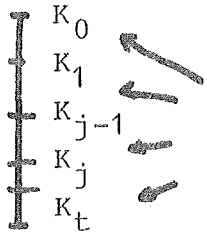
$$H_{i-1} = H_i(H_{i-1} \cap K_0)$$
$$\vdots$$
$$H_i(H_{i-1} \cap K_{j-1})$$
$$H_i(H_{i-1} \cap K_j)$$
$$\vdots$$
$$H_i = H_i(H_{i-1} \cap K_t)$$

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

$$K_{j-1} = K_j(H_0 \cap K_{j-1})$$
$$\vdots$$
$$K_j(H_{i-1} \cap K_{j-1})$$
$$K_j(H_i \cap K_{j-1})$$
$$\vdots$$
$$K_j = K_j(H_s \cap K_{j-1})$$

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) $\leq s$, 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-Hölder's sætning?

Opløselighed

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

Sætning. Lad G være en gruppe der har en kompositionsrække. Da er G opløselig hvis og kun hvis en (og dermed samtlige) kompositionsrækker har cykliske faktorer af primtalsorden.

Bevis. "hvis" klart.

"kun hvis": Benyt Noether's 2. isomorfisætning og korollar 2 øverst på siden. ∎

Sætning. G vilkårlig gruppe. Da gælder:

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

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

$$G_1' \subseteq G_2 \supset G'' \subseteq G_1' \subseteq G_2 \quad \text{og helt ament:}$$

$$G^{(i)} \subseteq G_i \quad \text{og følgelig} \quad G^{(s)} = e.$$

"⇐" $G' \lhd G$ og G/G' abelsk

$G'' \lhd G'$ og G'/G'' abelsk.

$\supset$: $G \rhd G' \rhd G'' \rhd \cdots \rhd G^{(n)} = e$ er 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 $\Rightarrow$ G har en "absolut" normalrække (: Undergrupperne er normaldelere ikke blot i foregående gruppe, men i hele G) med abelske faktorer.

Sætning. G opløselig $\Rightarrow$ enhver undergruppe i G er opløselig.
G opløselig $\Rightarrow$ ethvert homomorft billede af G er opløselig.

Bevis. Umiddelbart ved hjælp af ovenstående sætning.

Sætning. G 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 Noether's 2. isomorfisætning. Samtykning giver da normalrække i G med abelske faktorer. $\supset$: G er opløselig. ∎

Sætning. 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-gruppen af orden $< p^n$. Ifølge sætning p. 17 er $|\text{Centrum for } G| \geq p$. Centrum $\triangleleft G$, centrum opløselig $|G/\text{Centrum}| \leq p^{n-1}$ ⇒: ifølge induktionsantagelsen er G/Centrum opløselig. Foregående sætning viser, at G er opløselig. ∎

Sætning. Den symmetriske gruppe S_n er opløselig for $n \geq 4$ og ikke-opløselig for $n \geq 5$.

Bevis. $n = 1,2$ triviel, $n = 3$, $S_3' = A_3$, $S_3'' = A_3' = \{e\}$, $n = 4$ $S_4 \simeq$ (jfr. p. 22) $S_4''' = \{e\}$: S_n opløselig for $n \leq 4$. For $n \geq 5$ 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 $n \geq 5$ kan bevises direkte (uden brug af Galois' sætning). Nok at vise $A_n = A_n'$ for $n \geq 5$. Hertil godtgør vi:

1) Enhver 3-cykel er en kommutator,

2) 3-cyklens frembringer hele A_n.

Ad 1) (abc) givet; da $n \geq 5$ 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:

$$(ab)(bc) = (abc)$$

$$(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd). \quad \blacksquare$$

I bemærkning p. 35 øverst så vi, at G opløselig G har "absolut" normalrække med abelske faktorer.

Definition. Gruppen G kaldes overopløselig, hvis G har 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 absolut normalrække

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

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

Eksempel. S_3 er overopløselig, men ej nilpotent.

Beviset for Sætning p. 35 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)

abelsk $\Rightarrow$ nilpotent $\Rightarrow$ overopløselig $\Rightarrow$ 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 og undergrupper har samme længde.

Opgave. Vis, at mængden af alle følger af hele tal $(a_1, a_2, \ldots)$ med kompositionen

$$(a_1, a_2, \ldots, a_n, \ldots)\ (b_1, b_2, \ldots, b_n, \ldots) =$$

$$(a_1+b_1, (-1)^{b_1} a_2+b_2, (-1)^{b_1+b_2} a_3+b_3, \ldots, (-1)^{b_1+\ldots+b_{n-1}} a_n+b_n, \ldots)$$

udgør en gruppe G. Er G

i) opløselig?

ii) overopløselig?

iii) nilpotent?

Opgave. Vis, at $(Q,+)$ er nilpotent, men ej overopløselig. (Bevis og benyt, at et fra 0 forskelligt homomorft billede af $(Q,+)$ aldrig er cyklisk).

Sylows Gruppesætninger

Definition: G endelig gruppe , p primdivisor i $|G|$. Antag $|G| = p^r \cdot m$, $p \nmid m$ .En undergruppe i G af orden p^t kaldes en p-Sylowsgruppe.

Inden Sylows sætninger et lille lemma.

Lemma. Lad G være endelig abelsk , 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 = cykliske undergruppe frembragt af a . $|A| = \text{Ord } a = t$, $t > 1$. Vi skelner mellem to tilfælde.

i) $p \mid t$; da er $a^{\frac{t}{p}}$ et element af orden p .

ii) $p \nmid t$; da vil $p \mid \frac{n}{t} = |G/A|$.

Ifølge induktionsantagelsen findes et element (b) i G/A af orden p . (Idet $|G/A| < n$) d.v.s. for en repræsentant b for (b) gælder $b^p \in A$, $b \notin A$ og derfor $b^p = a^i$ for passende i . Da 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 $p \mid t$ i stand med antagelsen ii) . □

Sylows 1. Sætning. Lad G være endelig gruppe , p primdivisor i $|G|$. Da findes en p-Sylowsgruppe 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 $p \nmid [G:H]$

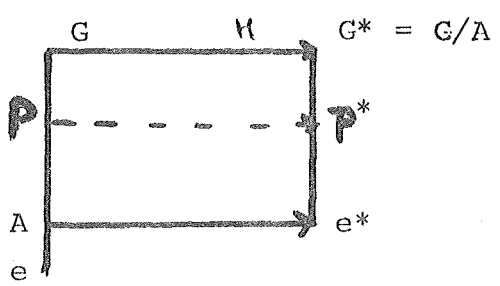
2) For alle ægte undergrupper H i G gælder $p \mid [G:H]$.

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

ad 2) Vi inddeler elementerne i G i ækvivalensklasser m.h.t. konjugering (jfr. p. 18). Da gælder

$$|G| = |\text{centrum}| + \sum_{\text{visse } a} [G:N_a]$$
$$[G:N_a] > 1$$

hvoraf sluttes, at $p \mid |\text{centrum}|$. Ifølge lemmaet p.42 findes et element $a \in$ centrum af orden p . Den af a frembragte cykliske undergruppe A er normaldeler i G . Vi betragter nu den kanoniske afbildning κ af G på $G/A (= G^*)$



Da $|G/A| < |G|$ findes på grund af induktionsantagelsen en p-Sylowgruppe P^* i G^* . D.v.s. hvis $|G| = p^r \cdot m$, $p \nmid m$, da er $|p^*| = p^{r-1}$. Ifølge Noether's 2. isomorfisætning er $P = \kappa^{-1}(p^*)$ en undergruppe i G så $P/A \simeq P^*$, $\exists$:
$|P| = p^{r-1}p = p^r$. P er altså p-Sylowgruppe i G . $\square$

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

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

Inden Sylows 2. sætning indfører vi for en undergruppe H i G normalisatoren N_H som $N_H = \{g \in G | gHg^{-1} = H\}$ N_H bliver undergruppe i G; klart, at $H \lhd N_H$. (Iøvrigt 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 passende $g \in G$. Man ser let, at "konjugeret" er en ækvivalensrelation. I analogi med et tidligere argument ses, at antallet af med H konjugerede undergrupper er $[G:N_H]$.

Sylows 2. sætning. G endelig gruppe, p 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 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 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 $S \cap P_i = S \cap N_{P_i}$.

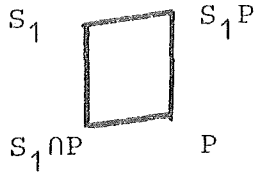
Ved optælling fås derfor en relation

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

$[S:(S \cap P_i)]$ = potens af p (evt. 1). $p \nmid [G:N_p]$ indebærer derfor $[S:(S \cap P_i)] = 1$ for mindst et i og dermed $S \subseteq P_i$. Beviset derfor færdigt modulo:

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

Bevis Sæt $S_1 = S \cap N_p$. Klart, at $S_1 \supseteq S \cap P$, $P \lhd N_p$ og S_1P undergruppe i N_p. Noethers 1. isomorfisætning anvendes:



$$S_1P/P \simeq S_1/_{S_1 \cap P}$$

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 $S \cap N_p = S \cap P$. □

Sylows 3. sætning. G endelig gruppe, p primdivisor i $|G|$. Antallet af p-Sylowgrupper i G er 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) $[P:(P \cap P_i)] = 1 \Leftrightarrow P = P_i$ (da $|P| = |P_i|$).
Følgelig forekommer på højre side af (*) netop en addend 1, mens resten er delelige med p. D.v.s. $[G:N_p] \equiv 1 \pmod{p}$ □

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

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

karakteristisk undergruppe i G .

Anvendelser.

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

Bevis. Kan antage (jfr. sætning p. 19) $p \neq q$ f.eks. $p > q$. Ifølge ovenstående bemærkning findes netop én p-Sylowgruppe, der er normaldeler og sammen med G og $\{e\}$ udgør normalrække med abelske faktorer.

Sætning. Lad p og q være forskellige primtal som $p \not\equiv 1 \pmod{q}$ og $q \not\equiv 1 \pmod{p}$. Da er enhver gruppe G af orden pq cyklisk.

Bevis. Ved anvendelsen af Sylows 3. sætning og ovenstående bemærkning ses, at G indeholder cykliske normaldelere P og Q af orden p , resp. q . Lad a (resp. b) være frembringere for P (resp. Q) . Da $P \trianglelefteq G$, $Q \trianglelefteq G$ vil $aba^{-1}b^{-1} \in P \cap Q$. Idet $|P \cap Q| \mid p$ og $|P \cap Q| \mid q$ er $P \cap Q = e$ d.v.s. a og b er ombyttelige. Derfor er $(ab)^p = b^p \neq e$ og $(ab)^q = a^q \neq e$. Følgelig er $\mathrm{Ord}(ab) = pq$, d.v.s. G er cyklisk med ab som frembringer. □

Sætning. Hvis gruppen G har roden p^2q , p og q primtal, er G opløselig.

Bevis: Vi kan antage $p \neq q$ (jfr. sætning p. 36). Der er nok at vise, at der kun findes én p-Sylowgruppe eller 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 analogt optællingsargument fås:

Sætning. Hvis gruppen G har orden pqr, hvor p, q 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 $p^q.q^b$, p og q primtal, da er G opløselig.

Sætning. (Feit & Thompson, Pac. J. Math. 7963, 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.

Vi stiler nu mod at vise en generel sætning af Burnside, der bl.a. indebærer, at en gruppe af kvadratfri orden ($\supset$: 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" $Ver(x)$, $x \in G$, fra G til H . Lad $g_1,\ldots,g_n$ være et fuldstændigt repræsen-

tantsystem for højresideklasserne til H, altså:

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

For ethvert $x \in G$ er også $xg_1,\ldots,xg_n$ et fuldstændigt repræsentantsystem for højresideklasserne til H, d.v.s.

$\forall_{g_i} \exists | g_j$, $j = x(i)$, så $x_{g_i} H = g_j H$ eller $xg_i = g_{x(i)} \cdot h_{x,i}$

hvor $i \to x(i)$ er en permutation af $\{1,2,\ldots,n\}$.

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

Da H 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 $g_1\tilde{h}_1,\ldots,g_n\tilde{h}_n$, hvor $\tilde{h}_1,\ldots,\tilde{h}_n \in H$. For hvert i, $1 \le i \le n$, fås

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

således at

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

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

Vi viser nu, at <u>Ver er en homomorfi fra G ind i H</u>. Lad $g_1,\ldots,g_n$ være fuldstændigt repræsentantsystem for højresideklasserne til H og lad x og y være vilkålige elementer i G.

Hvis

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

vil

$$xy\, g_i = x\, g_{y(i)}^{h_{y,i}} = g_{x(y(i))}^{h_{x,y(i)}\cdot h_{y,i}} \quad (1 \le i \le n)$$

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

$\mathrm{Ver}(x) \cdot \mathrm{Ver}(y)$. □

I stedet for højresideklasser kunne vi have betragtet venstresideklasserne

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

og have indført $\hat{\mathrm{Ver}}(x) = \prod_{i=1}^{n} \hat{h}_{x,i}$, når $g_i x = \hat{h}_{x,i} g_{x(i)}$ for entydigt bestemt $x(i) \in \{1,\ldots,n\}$ og $\hat{h}_{x,i} \in H$. Ver vil da som før være veldefineret og en homomorfi fra G til H . Vi hævder, at $\underline{\mathrm{Ver}(x) = \hat{\mathrm{Ver}}(x) \quad \forall x \in G}$; thi når $G = \bigcup_{i=1}^{n} Hg_i$ (disjunkt form), vil $G = \bigcup_{i=1}^{n} g_i^{-1} H$ (disjunkt forening) . Af $g_i x = \hat{h}_{x,i} g_{x(i)}$ følger $x^{-1} g_i^{-1} = g_{x(i)}^{-1} \cdot h_{x,i}^{-1}$ og derfor

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

Da Ver er en homomorfi, fås heraf $\mathrm{Ver}(x) = \hat{\mathrm{Ver}}(x)$. □

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

Endelig viser vi, at for ethvert $x \in G$ kan $\mathrm{Ver}(x)$ skrives $\mathrm{Ver}(x) = \prod_{k=0}^{n} y_k^{-1} x^{t_k} y_k$, hvor $y_k \in G$, $t_k \in \mathbb{N}$, $(1 \leq k \leq n)$ og $\sum_{t=0}^{n} t_k = [G:H]$ og $y_k^{-1} x^{t_k} y_k \in H$, $\forall k \ (0 \leq k \leq n)$. Hertil angiver vi først et bestemt (af x afhængig) 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 $x^{t_1} y_1 \in y_1 H$. 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 $y_2 \in G$, $y_2 \notin \bigcup x^j H \quad \bigcup x^j y_1 H$. Lad da t_2 være mindste naturlige tal med $x^{t_2} y_2 \in y_2 H$. Da er $H, xH, \ldots, x^{t_0-1}H, y_1 H, \ldots, x^{t_1-1} y_1 H, y_2 H, \ldots, x^{t_2-1} y_2 H$ 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 $t_0+t_1+\ldots+t_r = [G:H]$. For dette repræsentantsystem ses let, at

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

Vi vender nu tilbage til Sylowgrupperne. Først et

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

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

$$N_b = xN_a x^{-1}$$

Af $P \subseteq N_a$ følger $xPx^{-1} \subseteq xN_a x^{-1} = N_b$.
P og xPx^{-1} er nu begge p-Sylowgrupper i N_b er ifølge Sylows 2. sætning konjugerede inden for N_b, d.v.s. der

findes $y \in N_b$ så $P = y(xPx^{-1})y^{-1}$. Dette viser, at $yx \in N_p$. Men ligningen $b = yby^{-1} = y(xax^{-1})y^{-1} = (xy)a(xy)^{-1}$ viser, at a og b er konjugerede inden for N_p . □

Burnside's sætning. Lad G være en endelig gruppe og P en p-Sylowgruppe (p primdivisor i $|G|$) . Hvis $P \subseteq$ centrum for N_p , da findes normaldeler N i G som $G/N \simeq P$.

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

Lad $x \in P$. Ved bemærkning p. 49-50 er

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

De i P liggende faktorer $y_k x^{t_k} y_k^{-1}$ er inden for G konjugerede med x^{t_k} og derfor ifølge lemma også konjugerede med x^{t_k} inden for N_p ; D.v.s. 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 $\mathrm{Ver}(x) = x^{\sum_k t_k} = x^{[G:P]}$ $\forall x \in P$. 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 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 Burnside's sætning indfører vi

et nyt begreb. Lad H være undergruppe i en gruppe G. Centralisatoren ζ_H defineres som $\zeta_H = \{x \in G | xh = hx \ \forall h \in H\}$. Klart, at ζ_H er undergruppe i G og $\zeta_H \subseteq N_H$. Hvis specielt $H = G$ er centralisatoren gruppens centrum.

Lemma. Lad G være en endelig gruppe og P en undergruppe. Da er $[N_P : \zeta_P]$ 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 ζ_P. Følgelig er N_P/ζ_P isomorf med en undergruppe i $\mathrm{Aut}(P)$, hvoraf lemmaet følger. □

Ved hjælp af Burnside's sætning og lemmaet kan vi vise

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

Bevis: Lad os skrive $|G| = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, hvor $p_1 \ldots p_r$ 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 $r-1$ primtal.

Lad p_1 være mindste primdivisor i $|G|$ og lad P være en p_1-Sylowgruppe. P er 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 $p_1^{\alpha_1} - p_1^{\alpha_1 - 1} = p_1^{\alpha_1 - 1}(p_1 - 1)$. Ifølge lemmaet er $[N_P : \zeta_P]$ divisor i $p_1^{\alpha_1 - 1}(p_1 - 1)$. Da P specielt er

abelsk, er $P \subsetneq \zeta_P$; da P er p_1-Sylowgruppe, er $[N_P : \zeta_P]$ primisk med p_1 og da p_1 er mindste primdivisor i $|G|$, indebærer $[N_P : \zeta_P] \mid p_1^{\alpha_1 - 1}(p_1 - 1)$, at $[N_P : \zeta_P] = 1$, $\therefore N_P = \zeta_P$. Dette betyder, at P er indeholdt i centrum for N_P. Ifølge Burnside's sætning medfører dette, at der findes normaldeler N i G som $G/N \simeq P$. Idet $|N| = p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ vil enhver Sylowgruppe i N også være Sylowgruppe i G og derfor være cyklisk. Ifølge induktionsantagelse er N således opløselig. Eftersom N og $G/N \simeq P$ er opløselig, er G opløselig ifølge sætning p. 36. □

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. (jfr. p. 47). En endelig gruppe af kvadratfri orden er opløselig.

Endnu en lille anvendelse:

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

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

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

Sætning. 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 $N \trianglelefteq G$ så $G/N \simeq \mathbb{Z}_2$. Dette strider mod, at G er simpel, men ej cyklisk. Altså må $4 \mid |G|$, d.v.s. $|G| = 4k$, $k \in \mathbb{N}$. Vor opgave er at vise k ulige $\Rightarrow 3 \mid k$.

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 beviset for sætningen p. 52 indeholdt normaldeler N med $G/N \simeq \mathbb{Z}_4$ i strid med, at G er simpel. Altså må P være isomorf med Kleins Vierergruppe $\mathcal{V}_4$. Da $\mathrm{Aut}(\mathcal{V}_4) = S_3$ (hvorfor?) må $[N_p : \mathcal{C}_p]$ ifølge lemmaet p. 48 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 (Burnside's sætning), at G indeholdt normaldeler N , så $G/N \simeq \mathcal{V}_4$ i strid med, at G er simpel. Altså er $[N_p : \mathcal{C}_p] = 3$ hvorfor $3 \mid |G|$ og derfor $3 \mid k$. □

Bemærkning. Ovenstående sætning skyldes Burnside. Han formodede, at forudsætningen "$|G|$ er lige" kunne undværes. Dette blev bekræftet i 1963 af Feit-Thompson (jfr. p. 43). 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 16 , 12 eller 56 .

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 - vise lineære grupper, hvorved vi specielt lærer en ny familie af simple grupper at kende.

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

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

Da gælder:

$(n+m)a = na + ma \qquad \forall n,m \in \mathbb{Z}$

$n(ma) = (nm)a$

$n(a+b) = na + nb$ (← her benyttes kommutativiteten)

For en abelsk gruppe G defineres <u>torsionen</u> G_+ ved $G_T = \{g \in G \mid ng = 0 \text{ for passende } n \in \mathbb{Z} \setminus \{0\}\}$, d.v.s. 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.

<u>Eksempel</u>. G endelig $\Rightarrow$ G torsionsgruppe

$(\mathbb{Z}_1, +)$ og $(\mathbb{R}_1, +)$ er torsionsfri.

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

<u>Definition</u>. Endelig mange elementer i en abstrakt gruppe G

$a_1,\ldots,a_n$ kaldes uafhængige, hvis
$h_1a_1 + \ldots + h_n a_n = 0, h_1 \ldots h_n \in \mathbb{Z} \Rightarrow h_1 = \ldots = h_n = 0$.
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, d.v.s. en familie af elementer $\{e_i\}$ som 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: $\mathbb{Z}^n$ d.v.s. 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. G abelsk gruppe. Da gælder G fri $\Rightarrow$ G torsionsfri.

Bevis: Simpel øvelse. □

Eksempel. $(\mathbb{Q}, +)$ er torsionsfri men ej fri.

Opgave. Er den multiplikative gruppe $(\mathbb{Q}^+, \cdot)$ af positive rationale tal fri?

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

Sætning. 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

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

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

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

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

d.v.s. $\underline{\underline{B}}\,\underline{\underline{A}} = E$. 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

$\begin{Bmatrix} u_1 \\ u_n \end{Bmatrix} = A^{-1} \begin{Bmatrix} v_1 \\ v_n \end{Bmatrix}$ d.v.s. $v_1,\ldots,v_n$ er tillige frembringersæt for G og dermed basis for G . []

Bemærkning. En heltals matrix med determinant ± 1 kaldes "unimodulær".

Sætning. Lad G være en fri abelsk gruppe af (endelig) rang u . 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 $\mathbb{Z}a$, d.v.s. fri af rang 1 (hvis $a \neq 0$) eller af rang 0 (hvis $a = 0$) .

$n-1 \to n$: Lad $u_1,\ldots,u_n$ være basis for G . Ethvert $a \in A$ kan entydigt skrives $a = h_1u_1 +\ldots+ h_nu_n, h_1,\ldots,h_n \in \mathbb{Z}$. 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 $A \subseteq \mathbb{Z}u_1 +\ldots+ \mathbb{Z}u_{n-1}$: ifl. induktionsantagelsen

er A fri af rang $\leqq n-1 < n$.

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

i) $v_1,\ldots,v_\rho,v$ frembringer A ; thi lad $a \in A$ have fremstillinger $a = h''_1u_1 +\ldots+ h''_{n-1}u_{n-1} + h\gamma u_n$. Da er $a-hv \in A \cap (\mathbb{Z}u_1 +\ldots+ \mathbb{Z}u_{n-1})$: $a-hv$ er $\mathbb{Z}$-linearkombination af $v_1,\ldots,v_\rho$. Dermed er a en $\mathbb{Z}$-linearkombination af $v_1,\ldots,v_\rho,v$.

ii) $v_1,\ldots,v_\rho$, v er uafhængige; thi antag $k_1v_1 +\ldots+ k_\rho v_\rho + kv = 0$, hvor $k_1,\ldots,k_\rho$, $k \in \mathbb{Z}$. Ved at skrive $v_1,\ldots,v_\rho,v$ som $\mathbb{Z}$-linearkombination af $u_1,\ldots,u_n$ og se på koefficienterne til u_n ses, da $\gamma \neq 0$, at $k = 0$. Da $v_1,\ldots,v_\rho$ er uafhængige, må $k_1 =\ldots= k_\rho = 0$. Altså er $v_1,\ldots,v_\rho,v$ en basis for A . Antallet er $\rho+1 \leq (n-1) + 1 = n$ □

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 u og G en (ifølge foregående sætninger nødvendigvis) fri undergruppe af rang $m(\leq n)$. Lad $u_1,\ldots,u_n$ være basis for F , $v_1,\ldots,v_m$ 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 (ↄ : Nuller uden for diagonalen). Alternativ formulering:

Der findes unimodulær $(m\times m)$, resp. $(n\times n)$ matricer $\underline{P}$ resp. $\underline{Q}$ så (jfr. sætning p. 57)

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

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

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

2) erstatter vi med $v_i + \gamma v_j$ $(i \neq j)$, $\gamma \in \mathbb{Z}$. Dette svarer til, at man i $\underline{A}$ adderer γ (j^{te} række) til den i^{te} række.

Uden indskrænkning kan $\underline{A}$ antages $\neq 0$. Betragter nu alle de matricer der fås ud fra $\underline{A}$ 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 Euklid's algoritme på velkendt måde) .

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

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

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

$$\begin{matrix} \varepsilon_1 & 0 & \dots & 0 \\ 0 & & & \\ & \underline{\underline{A}}_2 & & \\ 0 & & & \end{matrix}$$, hvor $\underline{\underline{A}}_2$ er $(m-2)\times(n-2)$ 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 elementærdivisionssætningen: 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 $(i,j)^{te}$ 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: 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

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

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: $\begin{pmatrix} 1 & 0 \\ 0 & ab \end{pmatrix} =$

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

Ved successiv anvendelse af dette lemma fås umiddelbart

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

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

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

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

For en vilkårlig kommutativ ring R med et element defineres den generelle lineære gruppe af Grad n $GL(n,R)$ 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 af grad n $SL(n,R)$.

defineres som undergruppen i $SL(n,R)$ bestående af matricerne med determinant 1 .

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

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

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

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

Bevis: På grund af sætningen p. 61 og (tilføjelsen) findes elementære matricer $\underline{\underline{E}}_1' \dots \underline{\underline{E}}_\mu'$, $\underline{\underline{E}}_1'', \dots, E_\nu''$ så

$$\underline{\underline{E}}_1' \dots \underline{\underline{E}}_\rho' \underline{\underline{A}} E_1'' \dots E_\nu'' = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$$

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

Ifølge lemma 2, p. 57 kan $\begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$ ved multiplikation med elementære matricer føres over i

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

Da den reciprokke 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. Hvis $R = \mathbb{Z}$ eller et vilkårligt legeme gælder for $n \geq 3$ $SL(n,R) = SL(n,R)'$. Specielt er $GL(n,R)' = SL(n,R)$ for $n \geq 3$.

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

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

Sætning. Hvis R et et legeme med mindst 3 elementer gælder $GL(2,R)' = SL(,2R)$.

Bevis: Skal blot godtgøre, at $SL(2,R) \leq GL(2,R)'$. Ved samme argument som i foregående sætning er det nok at vise, at enhver elementær (2×2) matrix er en kommutator i $GL(2,R)$. 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 $GL(2,R) = SL(2,R) \simeq S_3$ og $SL(2,R)' = GL(2,R)'$ dermed en ægte undergruppe i $GL(2,R) = SL(2,R)$. Forudsætningen i foregående sætning angående R er således nødvendig.

Sætning. Hvis R er et legeme med mindst 4 elementer gælder $SL(2,R)' = SL(2,R)$.

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 $a(b^2-1)$, $a \in R$, alle elementerne i R . Følgelig er enhver elementær matrix kommutator i $SL(2,R)$. □

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

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(SL(n,K)) = matricerne

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & .. & \lambda \end{pmatrix}$$, $\lambda \in K$, $\lambda^n = 1$. (Benyt, at matricerne i centrum kommuterer med alle elementære matricer). Den projektive specielle lineære gruppe $PSL(n,K)$ af grad n over K defineres som $SL(n,K)/centrum(SL(n,K))$.

Vi stiler mod at vise, at $PSL(n,K)$ er simpel for $n \geq 3$ 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 $\underline{a} \sim \underline{b} \Leftrightarrow \exists \lambda \in K \setminus \{0\}$ 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 $\underline{\underline{A}} \in SL(n+1,K)$ 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 $\lambda \underline{\underline{E}} \in SL(n+1,K)$ d.v.s. centrum for $SL(n+1,K)$.

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

Lemma. $PSL(n+1,K)$ er en dobbelt-transitiv permutationsgruppe på $P(n,K)$.

Bevis. Lad $(\underline{a}_1)$, $(\underline{a}_2)$ og $(\underline{b}_1)$, $(\underline{b}_2)$ være punktpar i $P(n,K)$ $(\underline{a}_1) \neq (\underline{a}_2)$ og $(\underline{b}_1) \neq (\underline{b}_2)$. 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 $\underline{\underline{A}} \in SL(n+1,K)$ 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 $\rho_{\underline{\underline{A}}}((\underline{a}_1)) = (\underline{b}_1)$ og $\rho_{\underline{\underline{A}}}(\underline{a}_2) = \lambda(\underline{b}_1) = (\underline{b}_2)$. □

Vi kan nu vise

Sætning. Grupperne $PSL(n,K)$ er simple for alle $n \geq 2$ og alle legemer K undtagen for $n = 2$ og K = legeme med 2

eller 3 elementer.

Bevis: På nær i de to nævnte undtagelsestilfælde er $SL(n,K) = SL(n,K)'$ ifølge sætning p. 64 og 65. Da gælder også $PSL(n,K) = PSL(n,K)'$ $PSL(n,K)$ er en dobbelt-transitiv permutationsgruppe på $P(n-1,K)$.

Vi ønsker nu at anmode simpelhedskriteriet p. 26. For et punkt $(\underline{a}) \in P(n-1,K)$ skal vi angive en abelsk normaldeler $\mathcal{K}$ i stabilisatorgruppen for (a) så $PSL(n,K)$ 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

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

Man bemærker, at den til en elementær matrix svarende lineære afbildning er en transvektion. Specielt vil transvektionerne frembringe hele $SL(n,K)$ (jfr. sætning p. 63).

For fast $\underline{a}$ udgør transvektionerne $\{T_{\mu,\underline{a}} \mid \mu$ lineærform , $\mu(\underline{a}) = 0\}$ en undergruppe i $SL(n,K)$. Denne undergruppe $\tilde{\mathcal{K}}$ er abelsk, idet $T_{\mu,\underline{a}}\ T_{\nu,\underline{a}} = T_{\mu+\nu,\underline{a}}$.

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

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

hvoraf ses:

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

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

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

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

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

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 - og 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 $GL(n,q)$, $SL(n,q)$ og $PSL(n,q)$ grupperne $GL(n,K)$, $SL(n,K)$, $PSL(n,K)$, hvor K er det entydigt bestemte legeme med q elementer.

Ved et elementært kombinatorisk argument findes

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

og herved

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

Fra definition af PSL er det klart, at

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

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

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

(1) $PSL(2,2) = SL(2,2) = GL(2,2) \simeq S_3$.

(2) $PSL(2,3) \simeq A_4$

(3) $PSL(2,4) \simeq PSL(2,5) \simeq A_5$

(4) $PSL(2,7) \simeq PSL(3,2)$

(5) $PSL(4,2) \simeq A_8$

(6) $PSL(2,9) \simeq A_5$

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

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 $(a_1, a_2, \ldots, a_n)$, $a_i \in A_i$, $1 \leq i \leq n$, udgør en abelsk gruppe med komponentvis addition. Denne kaldes den (ydre) direkte sum af $A_1, A_2, \ldots, A_n$ og betegnes $A_1 \oplus A_2 \oplus \ldots \oplus A_n$. Hvis alle A_i , $1 \leq c \leq n$, er samme gruppe A , skrives kort A^n .

Et vigtigt eksempel er givet i

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

Bevis: Definer homomorfi $\varphi: \mathbb{Z} \to \mathbb{Z}_{p_1^{a_1}} \oplus \ldots \oplus \mathbb{Z}_{p_r^{a_r}}$ ved $\varphi(h) = (\overline{h}_{p_1^{a_1}}, \ldots, \overline{h}_{p_r^{a_r}})$. Her er $\operatorname{Ker} \varphi \simeq n\mathbb{Z}$, hvorfor ifølge homomorfisætningen $\mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}_n \simeq \varphi\mathbb{Z} \subseteq \mathbb{Z}_{p_1^{a_1}} \oplus \ldots \oplus \mathbb{Z}_{p_r^{a_r}}$.

Da $\varphi\mathbb{Z}$ og $\mathbb{Z}_{p_1^{a_1}} \oplus \ldots \oplus \mathbb{Z}_{p_r^{a_r}}$ således har samme orden $n = p_1^{a_1} \ldots p_r^{a_r}$, må $\varphi\mathbb{Z} = \mathbb{Z}_{p_1^{a_1}} \oplus \ldots \oplus \mathbb{Z}_{p_r^{a_r}}$. □

Hovedsætning. 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 $\varphi(h_1, \ldots, h_n) = h_1 a_1 + \ldots + h_n a_n$ definerede homomorfi fra $\mathbb{Z}^n$ til A . φ er surjektiv, da $a_1, \ldots, a_n$ er frembringersystem for A . $K = \operatorname{Ker} \varphi$ er undergruppe i F og derfor (sætning p .58)

fri af rang $m \leq n$. Ifølge elementærdivisorsætningen findes baser $u_1,\ldots,u_n$, $v_1,\ldots,v_m$ for F , henholdsvis K , så

$$v_1 = \varepsilon_1 u_1$$

$$v_m = \varepsilon_m u_m$$

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

$$G = \mathbb{Z}_{\varepsilon_1} \oplus\ldots\oplus \mathbb{Z}_{\varepsilon_m} \oplus \underbrace{\mathbb{Z} \oplus\ldots\oplus \mathbb{Z}}_{(n-m) \text{ eksempler}}$$

ved

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

ψ er oplagt surjektiv.

$\operatorname{Ker}\psi = \{x \in F \mid h_1 \equiv 0 \mod \varepsilon_1,\ldots,h_m \equiv 0 \mod \varepsilon_m , h_{m+1}=\ldots=h_n= 0\}$ $= K$. Ifølge homomorfisætningen har vi derfor

$$G \simeq F/_{\operatorname{Ker}\psi} = F/_K = F/_{\operatorname{Ker}\varphi} \simeq A .$$

d.v.s. $A \simeq G$, 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 $(\mathbb{Q},+)$). Kombination af de viste sætninger giver umiddelbart.

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

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

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

Bevis. Existensudsagnet 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 $a = a_1 +\ldots+ a_n$, $a_1 \in A_1,\ldots,a_n \in A_n$. I så fald skriver man $A = A_1 \oplus\ldots\oplus A_n$. Forbindelsen mellem den tidligere indførte (ydre) direkte sum og den indre direkte sum er:
Lad $A = A_1 \oplus\ldots\oplus A_n$ (indre direkte sum), da er
$A \simeq A_1 \oplus\ldots\oplus A_n$ (En isomorfi fra den ydre til den indre di-
(ydre direkte sum)
rekte sum er givet ved

$$(a_1,\ldots,a_n) \mapsto (a_1 +\ldots+ a_n))$$

Omvendt, lad A være ydre direkte sum $A = A_1 \oplus\ldots\oplus A_n$.
(ydre direkte sum)
Undergrupperne $A_i' = \{(0,\ldots,a_i,0\ 0\ 0) \mid a_i \in A_i\}$ er isomorfe med A_i og man ser let, at $A = A_1' \oplus\ldots\oplus A_n'$ (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 ν være den kanoniske homomorfi: $B \to B/_A$ og lad $c \in B$ være et element så νc 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 ethvert $b \in B$ findes helt tal h så $\nu b = h \nu c$
$\supset: b-hc \in \operatorname{Ker} \nu = A \quad \supset: b = (\text{element i } A) + (\text{element i } K)$.
Endvidere, hvis $0 = a+hc$, $a \in A$, $h \in C$, da må
$0 = \nu a + h \nu c = h \nu c \Rightarrow h = 0 \Rightarrow a = 0$. 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 $V \wedge H \neq \{0\} \Leftrightarrow p^{n-1}g \in H$.

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 $b = p^i a$,
$0 \leq i < n$ $p \nmid a$. 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 existensudsagnet i hovedsætningen p. 70 er det åbenbart tilstrækkeligt at vise forkortningssætningen i tilfældet hvor F er uendelig cyklisk ($\supset : \simeq \mathbb{Z}$) eller er cyklisk af primtalspotensorden.

Oversat til indre direkte summer skal vi vise:
Lad E være abelsk gruppe så $E = A \oplus G = B \oplus H$ (indre direkte summer) og enten $A \simeq B \simeq \mathbb{Z}$ eller $A \simeq B \simeq \mathbb{Z}p^n$ (p^n en 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. lemma p. 73).
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 (jfr. bemærkning p. 73. linie 2. f.o.) dermed $E/_D \simeq A \simeq B \oplus V$ eller $\mathbb{Z} \simeq \mathbb{Z} \oplus \mathbb{Z}$, hvilket er umuligt (jfr. sætning p. 57 øverst).

2) Nu tilfældet $A \simeq B \simeq \mathbb{Z}_{p^n}$, hvor p^n er en primtalspotens.
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 .

Hvis $A \cap H = 0$ kan a bruges som u .
Hvis $B \cap G = 0$ kan b bruges som u .

Antag derfor $A \cap H \neq \{0\}$ og $B \cap G \neq \{0\}$. Ifølge lemmaet p. 73 er da $p^{n-1}a \in H$ og $p^{n-1}b \in G$. For $a+b$ gælder:

$$p^n(a+b) = 0 \ , \ p^{n-1}(a+b) = (p^{n-1}a + p^{n-1}b) \notin H$$
$$\in H \qquad \notin H \qquad \notin G$$
$$\notin G \qquad \in G$$

hvorfor $a+b$ er brugbart som u .

For det således konstruerede u og tilsvarende cykliske undergruppe U af orden p^n gælder:
$U+G/G \simeq U/U\cap G \simeq U$, $|U+G/G| = p^n$. 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 (jfr. bemærkning p. 73 , linie 2 f.n.) $G \simeq E/U \simeq H$.
Forkortningssætningen er nu fuldstændig 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 $n = p_1^{a_1} \ldots p_r^{a_r}$ være n's primfaktoropløsning. Da giver hovedsætningen, at $\mathcal{A}(n) = \mathcal{A}(p_1^{a_1}) \ldots \mathcal{A}(p_r^{a_r})$ og for en primtalspotens p^a gælder: $\mathcal{A}(p^a) = p(a)$, hvor $p(a)$ er antallet af "partitioner" af a : Antallet af måder a kan skrives som sum af naturlige tal.

Endelig et kriterium for cykliske grupper.

Sætning. 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) ⇒ (ii) umiddelbar, da $G \simeq \mathbb{Z}_n$ for passende n .
(ii) ⇒ (iii) her bemærkes blot, at for $p \mid |G|$ findes elementer af orden p (benyt enten p. 72 eller hovedsætningen om endeligt frembragte abelske grupper)
(iii) ⇒ (i) (iii) 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 (*) p. 71 og dette $\ell_{i,j} = 1$. Sætningen p. 70 øverst viser da, at G er cyklisk. □

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

Bevis: Ligningen $x^p = 1$ har højest p rødder. (Et polyno-

mium over et legeme har højest så mange rødder som graden angiver). □

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