Matematik 2 AT, 1970–71

Thøger Bang
Algebra og Talteori

Suppleret med noter fra Mat 1 AG II og Mat 3, II, 1

§ 0. Afrunding af bekendt fundamental algebra.

De vigtigste tidligere betragtede algebraiske strukturer er grupper, ringe og legemer. I betegnelsen for en sådan struktur indgår både mængden af betragtede objekter og de relevante kompositioner (og evt. relationer), således at f.eks. en ring får en betegnelse som $(M,+,\cdot)$.

I hver af disse strukturer kan man have delmængder, som med de anvendte kompositioner udgør en struktur af samme art. Vi kan således i en gruppe $(G,\cdot)$ have en undergruppe H (hvor vi tillader os at udelade kompositionsbetegnelsen ved undergruppen, idet det er underforstået at det er kompositionen fra $(G,\cdot)$).

Lad $(G,\cdot)$ være en gruppe, skrevet multiplikativt; nødvendigt og tilstrækkeligt for at en ikke-tom delmængde H af G udgør en undergruppe er det, at H er stabil ved division. At betingelsen er nødvendig er klart; den er tilstrækkelig, thi når den er opfyldt vil H med a indeholde $aa^{-1} = e$ (neutralelementet), og dermed $ea^{-1} = a^{-1}$ (det inverse), og så med a og b indeholde $a(b^{-1})^{-1} = ab$ (altså stabil ved multiplikation).

Lad $(R,+,\cdot)$ være en ring; nødvendigt og tilstrækkeligt for at en ikke-tom delmængde S af R udgør en delring er det, at S er stabil ved subtraktion og multiplikation. Det følger umiddelbart af det foregående, ligesom også: Lad $(L,+,\cdot)$ være et legeme; nødvendigt og tilstrækkeligt for at en delmængde M af L udgør et dellegeme er det, at M er stabil ved subtraktion, og at $M \setminus \{\text{nulelem.}\}$ er ikke-tom og stabil ved division.

Hvis man i en mængde A med kompositionen * har delmængder B_j som er stabile ved *, så er $\bigcap_j B_j$ også stabil ved *. Heraf fås umiddelbart: I en gruppe (hhv. ring, legeme) er fællesmængden af endelig eller uendelig mange undergrupper (hhv. delringe, dellegemer) igen en undergruppe (hhv. delring, dellegeme).

Man ser, at "$(H,\cdot)$ er en undergruppe i $(G,\cdot)$" er en partiel reflexiv ordningsrelation på mængden af grupper, og analogt for delringe og dellegemer.

Lad os minde om at en ordningsrelation på en mængde er en relation, som er transitiv og asymmetrisk, og desuden enten reflexiv eller irreflexiv (i det reflexive tilfælde benyttes ofte en betegnelse hvori indgår et lighedstegn, som f.eks. $\leqq$, i det irreflexive tilfælde benyttes betegnelser uden lighedstegn som f.eks. $<$; til enhver reflexiv ordningsrelation findes en tilsvarende irreflexiv og omvendt). En ordningsrelation $\rightarrow$ kan være total, d.v.s. at $a \neq b \Rightarrow (a \rightarrow b) \vee (b \rightarrow a)$; hvis man vil betone at en ordning ikke er (eller ikke vides at være) total kan man kalde den partiel.

En ordnet gruppe $(G,\cdot,\leqq)$ er en gruppe $(G,\cdot)$, hvor der på elementmængden G er defineret en total ordningsrelation $\leqq$, som er koblet til kompositionen $\cdot$ ved betingelsen $(a \leqq b) \Rightarrow (ac \leqq bc) \wedge (ca \leqq cb)$; man bemærker, at der også gælder den tilsvarende implikation, selvom lighedstegnet overalt udelades.

En ordnet ring (hhv. legeme) $(M,+,\cdot,\leqq)$ er en ring (hhv. legeme) $(M,+,\cdot)$, hvor der på elementmængden M er defineret en total ordningsrelation $\leqq$, som er koblet med kompositionen + ved kravet om at

$(M,+,\leqq)$ skal være en ordnet gruppe, og desuden er koblet med kompositionen $\cdot$ ved kravet om $(c \geqq 0 \wedge a \leqq b) \Rightarrow (ac \leqq bc \wedge ca \leqq cb)$; her betegner 0 det i gruppen $(M,+)$ befindtlige neutralelement. Man bemærker, at for legemer vil der på grund af nulreglen også gælde den tilsvarende implikation i hvilken lighedstegnet overalt er udeladt, men for ringe behøver dette ikke at være tilfældet (tager man f.eks. en ordnet abelsk gruppe $(M,+,\leqq)$ og definerer multiplikation ved at alle produkter er lig 0 fremkommer en ordnet ring).

Lad os iøvrigt minde om at for ringe er nulreglen: $ab = 0 \Rightarrow (a = 0) \vee (b = 0)$ ensbetydende med forkortningsreglen: $(ab = ac) \wedge (a \neq 0) \Rightarrow b = c$ (og den tilsvarende, hvor a er faktor på højre side), som jo også kan udtrykkes: division med et fra 0 forskelligt element er højst entydig.

Et legeme kan karakteriseres som en ring, hvori division med et fra 0 forskelligt element altid er mulig, idet dette medfører nulreglen, og altså at divisionen er entydig. Bevis: Lad a,b og c være vilkårlige $\neq 0$; ligningen $ax = c$ er løselig, og endvidere er $by = x$ løselig, og ved indsættelse fås $c = ax = a(by) = (ab)y$, og da $c \neq 0$ fås, at $ab \neq 0$, altså nulreglen.

Legemer skal pr. definition indeholde mindst to elementer (nemlig ihvertfald 0 og et derfra forskelligt etelement), dette krav kan synes urimeligt, men viser sig at være en for senere sætningsformuleringer nyttig konvention. Iøvrigt vil de legemer vi skal møde her i forelæsningerne alle være kommutative, men der eksisterer som bekendt ikke-kommutative legemer, f.eks. kvaternionerne. En ring må gerne nøjes med at indeholde ét element (men er så selvfølgelig ret

uinteressant), og ringe er ofte ikke-kommutative, f.eks. matrixringe.

Ved en homomorfi forstås en afbildning φ af en mængde med kompositioner $(M,*,\ldots)$ ind i en mængde med ligesåmange kompositioner $(\hat{M},\hat{*},\ldots)$, og således at der for vilkårlige $a,b \in M$ gælder $\varphi(a * b) = \varphi(a) \hat{*} \varphi(b)$ og tilsvarende for de øvrige kompositioner. Ved sammensætning af to homomorfier fremkommer igen en homomorfi (så at relationen "homomorf med" er en transitiv relation). En bijektiv homomorfi kaldes en ismorfi (og relationen "isomorf med" ses at være refleksiv, symmetrisk og transitiv).

Lad os i det følgende antage, at homomorfien er surjektiv, så at ethvert element i $\hat{M}$ kan skrives på formen $\hat{a} = \varphi(a)$. Hvis en komposition $*$ er kommutativ, så er den tilsvarende komposition $\hat{*}$ i billedet også kommutativ, thi man har $\varphi(a) \hat{*} \varphi(b) = \varphi(a * b) = \varphi(b * a) = \varphi(b) \hat{*} \varphi(a)$, og analogt ses, at associativ komposition går over i associativ komposition, og at hvis en komposition er distributiv m.h.t. en anden så gælder det samme for de tilsvarende kompositioner i billedet. Ligeledes ses, at hvis e er neutralelement ved en komposition $*$, så er $\varphi(e)$ neutral ved $\hat{*}$, idet $\varphi(e) \hat{*} \varphi(a) = \varphi(e * a) = \varphi(a)$. Hvis en komposition er således at ved den er division altid mulig, så gælder det samme for den tilsvarende komposition i billedet. Bevis: Vi skal vise, at for alle $\varphi(a)$ og $\varphi(b)$ er ligningen $\varphi(a) \hat{*} \varphi(x) = \varphi(b)$ løselig, men når ligningen $a * x = b$ er forudsat løselig fås umiddelbart at $\varphi(b) = \varphi(a * x) = \varphi(a) \hat{*} \varphi(x)$.

Af de nævnte egenskaber følger umiddelbart, at ved en homomorfi vil en gruppe afbildes på en gruppe, og således at etelement går o-

ver i etelement, og hvis gruppen er abelsk bliver billedet abelsk. Ligeledes ses, at ved en homomorfi vil en ring afbildes på en ring og således at nulelement går over i nulelement og etelement går over i etelement. For legemer bliver forholdene særlig simple, idet en homomorf afbildning af et legeme er enten en isomorfi, eller også således at billedringen består af ét eneste element. Bevis: Hvis φ ikke er en isomorfi er den ikke injektiv, altså findes $a \neq b$ så $\varphi(a) = \varphi(b)$ og dermed $\varphi(a-b) = nul$; sættes $a-b = d$ kan ethvert $c \in$ legemet skrives på formen $c = dx$ (fordi $d \neq 0$), og vi får $\varphi(c) = \varphi(d) \cdot \varphi(x) = nul$.

Derimod må det fremhæves, at ved homomorf afbildning af en ring på en ring gælder intet om nulreglens gyldighed, den kan gælde i originalringen og svigte i billedet eller svigte i originalringen og gælde i billedet, og desuden er det trivielt at man kan have samme forhold i originalringen og i billedet (eksempler nævnes senere).

Begrebet ækvivalensrelation er velkendt (reflexiv, symmetrisk og transitiv, bemærk den alfabetiske rækkefølge). En ækvivalensrelation $\sim$ siges at harmonere med en komposition $*$ såfremt $a\sim a_1 \wedge b\sim b_1$ medfører $a*b \sim a_1*b_1$ (altså at ækvivalente komponenter giver ækvivalente kompositionsresultater).

Lad nu φ være en homomorf afbildning af $(M,*,\ldots)$ på $(\hat{M},\hat{*},\ldots)$. Vi definerer en relation $\sim$ ved $x\sim x_1 \iff \varphi(x) = \varphi(x_1)$, og man ser umiddelbart, at det er en ækvivalensrelation, og at der er bijektiv forbindelse mellem ækvivalensklasserne og elementerne i $\hat{M}$. Ækvivalensrelationen vil harmonere med de forekommende kompositioner.

Bevis: Lad $x \sim x_1 \wedge y \sim y_1$, altså $\varphi(x) = \varphi(x_1)$ og $\varphi(y) = \varphi(y_1)$, så er $\varphi(x * y) = \varphi(x) \hat{*} \varphi(y) = \varphi(x_1) \hat{*} \varphi(y_1) = \varphi(x_1 * y_1)$, hvilket viser at $x * y \sim x_1 * y_1$.

Dersom der omvendt på $(M,*,\ldots)$ er givet en ækvivalensrelation $\sim$ der harmonerer med de forekommende kompositioner $*,\ldots,$ så eksisterer der en homomorf afbildning φ af $(M,*,\ldots)$ således at $x \sim x_1$ netop når $\varphi(x) = \varphi(x_1)$. Bevis: Vi sætter $\varphi(x)$ lig den ækvivalensklasse (delmængde af M) som indeholder x, således at $\hat{M} = \{\varphi(x)\}$, og definerer $\hat{*}$ på $\hat{M}$ ved at $\varphi(x) \hat{*} \varphi(y) = \varphi(x * y)$, og tilsvarende for de øvrige kompositioner, hvormed vi jo netop (tilsyneladende da) har fået opfyldt kravene for at det er en homomorfi. Men for at beviset skal være i orden må vi efterse, at det anførte virkelig definerer en komposition $\hat{*}$ på $\hat{M}$; sagen er, at det samme element $\varphi(x) \in \hat{M}$ kan fremkomme for forskellige x, men disse vil kun afvige indbyrdes ved ækvivalensen, og analogt med $\varphi(y)$, og når $\sim$ harmonerer med $*$ vil alle de fremkomne $x * y$ også være indbyrdes ækvivalente, og dermed give samme $\varphi(x * y)$, og vi har altså virkelig defineret en komposition. Dermed er beviset fuldført.

Hvis en anden homomorfi Ψ: $(M,*,\ldots) \to (\bar{M},\bar{*},\ldots)$ giver anledning til den samme ækvivalensrelation $\sim$ på M, så vil ethvert element i $\bar{M}$ også svare til en ækvivalensklasse, og vi har dermed en bijektiv afbildning χ: $\bar{M} \to \hat{M}$ for hvilken $\chi \circ \Psi = \varphi$. Dette χ er endda en isomorfi mellem $(\bar{M},\bar{*},\ldots)$ og $(\hat{M},\hat{*},\ldots)$ thi $\chi(\Psi(x) \bar{*} \Psi(y)) = \chi(\Psi(x * y)) = \varphi(x * y) = \varphi(x) \hat{*} \varphi(y) = \chi(\Psi(x)) \hat{*} \chi(\Psi(y))$, så det er en homomorfi fra $(\bar{M},\bar{*},\ldots)$ til $(\hat{M},\hat{*},\ldots)$ og dermed en isomorfi.

Vi har altså følgende almindelige homomorfisætning: En homomorf afbildning φ af en mængde med kompositionsforskrifter giver anledning til en ækvivalensrelation $\sim$ på mængden, harmonerende med kompositionerne, og således at $x \sim y$ netop når $\varphi(x) = \varphi(y)$. Hvis man omvendt har en mængde med kompositioner og en på mængden defineret ækvivalensrelation $\sim$, som harmonerer med kompositionerne, så eksisterer der homomorfe afbildninger φ af mængden med kompositionerne, således at $\varphi(x) = \varphi(y)$ netop når $x \sim y$, og billedet ved en sådan homomorfi er bestemt entydigt pånær isomorfi (nemlig isomorft med strukturen af mængden af ækvivalensklasser organiseret ved de kompositioner der fås ved at regne med repræsentanter fra klasserne).

Vi skal nu betragte homomorfe afbildninger φ af en gruppe $(G,\cdot)$, d.v.s. undersøge på G de ækvivalensrelationer $\sim$ som harmonerer med $\cdot$.

Ved at multiplicere med $y \sim y$ eller med $y^{-1} \sim y^{-1}$ ser man umiddelbart, at $x \sim y \iff xy^{-1} \sim e \iff y^{-1}x \sim e$, og dermed at relationen $\sim$ er bestemt ved $H = \{h \mid h \sim e\}$, hvor $h \in G$ og hvor e er gruppens etelement. Mængden H bestemmer altså homomorfien entydigt (pånær isomorfi i billedet), og kaldes homorfiens kerne, og den pånær isomorfi entydigt bestemte billedgruppe betegnes som faktorgruppen eller kvotientgruppen $(G,\cdot)/H$.

Da $x \sim e \wedge y \sim e) \Rightarrow xy^{-1} \sim e$ ses, at H er stabil ved division, og altså er en undergruppe i $(G,\cdot)$. For et vilkårligt fast x er $\{y \mid y \sim x\} = \{y = xh\} = \{y = hx\}$, hvor $h \in H$, og vi har altså, at for alle x er $xH = Hx \iff xHx^{-1} = H \iff xH = Hx = HxH$ (idet $H = HH$, og alt-

så $Hx = HHx = H(Hx) = H(xH) = HxH$).[+])

Dersom omvendt H er en undergruppe i $(G,\cdot)$ som for alle x opfylder $xHx^{-1} = H$ ensbetydende med $xH = Hx = HxH$, så er H kerne for en homomorfi, nemlig en afbildning $x \to xH$ af G ind i mængden af delmængder A af G, og hvor vi som komposition for delmængderne A og B tager AB. Thi afbildningen er en homomorfi da $x \mapsto xH$ og $y \mapsto yH$ medens $xy \mapsto xyH = xHy = xHHy = (xH)(Hy) = (xH)(yH)$, og dens kerne er H da $x \in H \iff xH = H$ = etelementet i billedet = billedet af etelementet i $(G,\cdot)$.

Vi har: <u>En homomorf afbildning af en gruppe er (pånær isomorfi i billedet) bestemt entydigt ved sin kerne H, og billedgruppen betegnes som et eksemplar af faktorgruppen $(G,\cdot)/H$. De mulige homomorfikerner kaldes normale undergrupper i $(G,\cdot)$</u>.

At <u>H er en normal undergruppe i $(G,\cdot)$</u> betegnes ved skrivemåden $H \lhd (G,\cdot)$. <u>Nødvendigt og tilstrækkeligt for at</u> $H \lhd (G,\cdot)$ <u>er det at</u>

[+]) Hvis man på en mængde M har givet en komposition $*$, og hvis A og B er delmængder af M, så sætter man som bekendt $A * B = \{a * b \mid a \in A \wedge b \in B\}$; specielt benyttes skrivemåden $a * B$ dersom A kun består af ét element a; analogt $A * b$. <u>Dersom kompositionen er kommutativ eller associativ eller distributiv m.h.t. en anden komposition, så gælder det tilsvarende for kompositionen anvendt på delmængderne</u>. Lad os f.eks. bevise associativ: $(A * B) * C = \{(a * b) * c \mid a \in A \wedge b \in B \wedge c \in C\}$, medens $A *(B * C) = \{a *(b * c)\}$, og den elementvise associativitet viser det ønskede.

for alle $x \in G$ gælder $xHx^{-1} = H$ ensbetydende med at $xH = Hx = HxH$.

Man ser umiddelbart, at i enhver gruppe $(G,\cdot)$ er de trivielle undergrupper $\{e\}$ og G normale. Langtfra alle undergrupper er normale, det fremgår senere, men det er klart, at i en abelsk gruppe er enhver undergruppe normal.

Relationen $\lhd$ er ikke transitiv, man kan altså ikke af H normal i K og K normal i $(G,\cdot)$ slutte at H normal i $(G,\cdot)$, det fremgår af senere eksempler. Derimod: Hvis $H \lhd (G,\cdot)$, og K er en undergruppe så $H \subset K \subset G$, så er $H \lhd (K,\cdot)$. Det er klart, da $xHx^{-1} = H$ gyldig for alle $x \in G$ umiddelbart giver, at det er gyldigt for alle $x \in K$. Endvidere: I en gruppe er fællesmængden af normale undergrupper igen en normal undergruppe, thi når man for alle H_j har $xH_jx^{-1} = H_j$, fås at $x(\bigcap H_j)x^{-1} \subseteq \bigcap H_j$, og ved at erstatte x med x^{-1} ses at der her gælder lighedstegn.

Lad os betragte en gruppe $(G,\cdot)$ og i denne en vilkårlig undergruppe H (ikke nødvendigvis normal).

Vi kan på mængden G definere en relation $\sim$ ved $x \sim y \iff x^{-1}y \in H$. Relationen bliver en ækvivalensrelation, thi den er reflexiv da $x^{-1}x = e \in H$, og den er symmetrisk da $x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} = y^{-1}x \in H$, og den er transitiv da $x^{-1}y \in H \wedge y^{-1}z \in H \Rightarrow (x^{-1}y)(y^{-1}z) = x^{-1}z \in H$. Da $x^{-1}y \in H \iff y \in xH$ ses, at den ækvivalensklasse som indeholder et fast element x netop er mængden xH, og denne mængde kaldes en venstre sideklasse til H, så ækvivalensklasserne bliver netop de venstre sideklasser til undergruppen. Hvis vi som definition af relationen hav-

de benyttet $yx^{-1} \in H$, var ækvivalensklasserne blevet af formen Hx, hvilket kaldes højre sideklasser til H. Man ser, at betingelsen for at $H \lhd G$ netop er, at højre-sideklasserne og venstre-sideklasserne er identiske.

Dersom $(G,\cdot)$ er endelig vil enhver sideklasse indeholde ligeså mange elementer som H, og da G er opdelt i ækvivalensklasser har vi dermed

Lagrange's sætning: For en endelig gruppe $(G,\cdot)$ vil ordenen af en vilkårlig undergruppe H være divisor i gruppens orden. (Lagrange, 1736-1813).

Eksempel: En gruppe hvis orden er et primtal har ikke andre undergrupper end de to trivielle, nemlig gruppen selv og {etelementet}.

Antallet af sideklasser til en undergruppe kaldes undergruppens index, og man ser at i en endelig gruppe må ethvert undergruppeindex også være divisor i gruppens orden. Det må her bemærkes, at for bestemmelsen af index er det ligegyldigt om man regner med højre eller venstre sideklasser, thi der er bijektiv forbindelse mellem disse, da mængden af inverse elementer til klassen xH er klassen Hx^{-1} (for $(xH)^{-1} = H^{-1}x^{-1} = Hx^{-1}$). Eksempel: $(\mathbb{Q} \setminus \{0\},\cdot)$ er en gruppe med $(\mathbb{Q}_+,\cdot)$ som undergruppe, og dennes index er 2 da der findes de to sideklasser $\mathbb{Q}_+$ og $\mathbb{Q}_-$.

Gruppen $(\mathbb{Z},+)$ og dens logiske baggrund behandles udførligt i næste §. Har man en vilkårlig gruppe $(G,\cdot)$ med etelement e og et vilkårligt element $a \in G$, kan det vises, at der findes netop én ho-

momorf afbildning af $(\dot{Z},+)$ ind i $(G,\cdot)$ ved hvilken tallet $1 \mapsto a$, og ved denne betegnes billedet af tallet n som a^n. Beviset føres ved induktion: for $n > 0$ definerer man a^{n+1} som $a \cdot a^n$, for $n = 0$ sætter man $a^0 = e$, og for $n < 0$ definerer man a^n som $a^{-1} \cdot a^{n+1}$; det ses, at man alment faar $a^{n+1} = a \cdot a^n$. At det er en homomorfi udtrykkes ved første potensregel $a^m \cdot a^n = a^{m+n}$, og dennes rigtighed ses ved et lignende induktionsbevis, idet man holder n fast og for $m > 0$ faar $a^{m+1} \cdot a^n = a \cdot a^m \cdot a^n = a \cdot a^{m+n} = a^{m+n+1} = a^{(m+1)+n}$, og for $m < 0$ foretager man induktionen nedad fra 0 (ligesom ovenfor).

Et homomorft billede af $(\dot{Z},+)$ betegnes som en cyklisk gruppe, og billedet ved den ovenfor omtalte afbildning betegnes som den cykliske gruppe frembragt af a. Man ser at det er den mindste undergruppe af $(G,\cdot)$ som indeholder a, og endvidere bemærker man, at den er abelsk, ogsaa selvom $(G,\cdot)$ ikke er det.

Første potensregel giver at $(a^n)^{-1} = a^{-n}$. Alment faar man anden potensregel $(a^m)^n = a^{mn}$. Her betegner mn produktet i $(\dot{Z},\cdot)$ af tallene m og n, og hvorledes dette defineres (ved induktion) omtales nærmere i næste §, og i overensstemmelse hermed bevises reglen ved induktion efter n idet m holdes fast: For $n = 0$ gælder den, og omskrivningen $(a^m)^{n+1} = a^m \cdot (a^m)^n = a^m \cdot a^{mn} = a^{m+mn} = a^{m(n+1)}$ beviser den for de positive n hvorefter $(a^m)^{-n} = a^{-mn}$ ved at opløfte til '-1' potens viser den for de negative n.

I en abelsk gruppe gælder desuden tredie potensregel $(ab)^n = a^n \cdot b^n$, der ogsaa let ses ved induktion, idet $(ab) \cdot (ab)^n = a \cdot a^n \cdot b \cdot b^n$.

For abelske grupper bruges ofte additiv skrivemaade, og saa skriver man f.eks. første potensregel som $ma + na = (m+n)a$, hvilket ser ud som en distributiv lov, men er noget helt andet - nemlig første potensregel. Udtrykket ma, hvori m er et tal og a er et gruppeelement er ikke noget produkt, men derimod (for m positiv) et udtryk $a+a+\ldots+a$ (m addender). Men det er altsaa saa "heldigt", at selv i flertydige situationer vil formel regning ikke føre til nogen fejl.

Lad os betragte cykliske grupper $(C,\cdot) = (\{a^n\},\cdot)$. Vi bemærker, at $a^p = a^n \Leftrightarrow a^{p-n} = e$.

Dersom det gælder, at i suiten $\ldots,a^{-2},a^{-1},e=a^0,a,a^2,\ldots$ forekommer neutralelementet e kun paa den viste plads, saa er homomorfien $(\dot{Z},+) \to (C,\cdot)$ injektiv ifølge det nævnte, altsaa en isomorfi. Afbildningens kerne er undergruppen $\{0\}$ i $(\dot{Z},+)$. Man siger, at <u>ordenen af a er uendelig</u>, og <u>den af a frembragte cykliske gruppe er</u> altsaa <u>isomorf med $(\dot{Z},+)$</u>.

I modsat fald findes et $m \neq 0$ hvor $a^m = e$; da $a^m = e \Leftrightarrow a^{-m} = e$ findes der et positivt m, og lad os tage det mindste positive. Da er $a,a^2,\ldots,a^{m-1},a^m = e$ alle forskellige (hvis $a^p = a^n$ bliver $a^{p-n} = e$ og $0 < |p-n| < m$) og da $a^h = a^{h+m} = a^{h-m}$ ses, at suiten $\ldots,a^{-2},a^{-1},e,a,a^2,\ldots$ bliver periodisk med perioden m. Billedmængden bestaar altsaa af m elementer, saa den cykliske gruppe er af m'te orden, og man siger at <u>ordenen af a er m</u>. Kernen for den homomorfe afbildning af $(\dot{Z},+)$ ses at bestaa af mængden af multipla af m, og denne mængde betegnes som (m). Da denne kerne er fælles for alle afbildninger som

fører til cykliske grupper af orden m ses, at alle cykliske grupper af orden m er isomorfe, og hvis man ser bort fra isomorfi kan man derfor tale om "den cykliske gruppe af m'te orden". Omvendt ses, at for ethvert naturligt tal m er (m) en undergruppe i $(\dot{Z},+)$, da den er stabil ved subtraktion, ma-mb = m(a-b), man ser endda heraf at den er isomorf med $(\dot{Z},+)$; da $(\dot{Z},+)$ er abelsk bliver $(m) \triangleleft (\dot{Z},+)$, altsaa afbildningskerne, og der eksisterer altsaa en cyklisk gruppe af orden m.

Alt i alt: Ordenen af et gruppeelement a defineres som ordenen af den cykliske gruppe frembragt af a. Denne orden er enten et naturligt tal eller den er uendelig (og i sidste tilfælde er det et "numerabelt uendeligt"). Ethvert naturligt tal kan forekomme som orden af en cyklisk gruppe. Alle cykliske grupper af m'te orden er isomorfe, og hvis en cyklisk gruppe er uendelig, saa er den isomorf med $(\dot{Z},+)$.

Da vi har bestemt samtlige afbildningskerner har vi dermed ogsaa fundet samtlige undergrupper i $(\dot{Z},+)$ (for i en abelsk gruppe er jo enhver undergruppe normal): Undergrupperne i $(\dot{Z},+)$ er af formen (m), d.v.s. mængden af multipla af et naturligt tal m, og saa den trivielle $\{0\}$ (som jo iøvrigt kan opfattes som mængden af multipla af 0; den anden trivielle undergruppe, $\dot{Z}$ selv, er lig (1)).

Gruppen $(\dot{Z},+)$ har altsaa uendelig mange ikke-trivielle undergrupper, alle isomorfe med gruppen selv, og uendelig mange ikke-trivielle homomorfibilleder, af hvilke ingen er isomorfe med gruppen selv. OBS: For en uendelig gruppe kan en ægte undergruppe altsaa godt være isomorf med hele gruppen, og

der findes iøvrigt ogsaa eksempler paa uendelige grupper for hvilke billedet ved en homomorfi som ikke er en isomorfi (altsaa med kerne med flere elementer) bliver isomorft med hele originalgruppen.

Ordenen af a kan betegnes ord a. For ord a = m har vi $a^k = e \Leftrightarrow k \in (m) \Leftrightarrow m|k$. Endvidere $(\ell) \supseteq (m) \Leftrightarrow \ell|m$; taleksempel: $(6) \supseteq (18)$.

Lad $(C,\cdot)$ være en cyklisk gruppe og H en undergruppe i den. Da er baade H og kvotientgruppen $(C,\cdot)/H$ cykliske.

(da alt er abelsk er $H \lhd (C,\cdot)$, saa kvotientgruppen eksisterer). Bevis: Først kvotientgruppen, den er homomorft billede af $(C,\cdot)$, som igen er homomorft billede af $(\dot{Z},+)$, og den er altsaa selv homomorft billede af $(\dot{Z},+)$ og dermed cyklisk. Saa beviset for at H er cyklisk: Der findes en surjektiv homomorfi $\varphi:(\dot{Z},+)\to(C,\cdot)$. Mængden $\varphi^{-1}(H)$ bliver stabil ved subtraktion, da $\varphi(n_1) = h_1 \in H \wedge \varphi(n_2) = h_2 \in H$ medfører $\varphi(n_1-n_2) = h_1h_2^{-1} \in H$, og den er altsaa undergruppe i $(\dot{Z},+)$. Men saa er den enten uendelig og dermed isomorf med $(\dot{Z},+)$ eller den er $\{0\}$ og dermed trivielt homomorft billede af $(\dot{Z},+)$. I begge tilfælde findes altsaa en surjektiv homomorfi $\psi: (\dot{Z},+)\to(\varphi^{-1}(H),+)$, og dermed en surjektiv homomorf afbildning $\varphi\circ\psi$ af $(\dot{Z},+)$ paa $(H,\cdot)$, hvilket viser at H er cyklisk.

I en vilkaarlig gruppe $(G,\cdot)$ vil et element a frembringe en cyklisk undergruppe, og af Lagrange's sætning (s.10) faar vi saa det vigtige resultat: I en endelig gruppe er ethvert element af endelig orden, og denne er divisor i gruppens orden.

Eksempel: En gruppe af primtalorden p maa være cyklisk, fordi ethvert fra e forskelligt element maa have orden p. Ethvert saadant element frembringer altsaa hele gruppen. Heraf ses yderligere, at hvis man i en større gruppe har to undergrupper af p' orden, og de har mere end e fælles, saa er de identiske. Taleksempel: Den symmetriske gruppe S_5 bestaar af de 120 permutationer af 5 ting; i gruppen findes elementer af ordener 1,2,3,4,5,6 (stemmer med Lagrange). Der findes 24 elementer af orden 5, og heraf slutter vi, at der findes netop 6 undergrupper af orden 5, idet enhver af disse indeholder 4 fra e forskellige elementer, og ligeledes indser man, at antallet af elementer af 3' orden maa være lige (antallet er 20). Forekomsten af elementer a af orden 6 medfører forekomsten af elementer af orden 2, idet ord(a^3) = 2, men man kan ikke slutte noget nærmere om deres antal, for dels kunde mange forskellige a give samme a^3, og dels kunde der findes elementer af orden 2 som ikke er 3' potens af et element af orden 6.

Den ikke-trivielle homomorfi $(\dot{Z},+) \rightarrow (\dot{Z},+)/(m)$ har som kerne delmængden (m) af $\dot{Z}$. Den til homomorfien svarende ækvivalensrelation i $\dot{Z}$ bliver at a og b er ækvivalente hvis og kun hvis $a-b \in (m)$. Dette historisk første eksempel paa en ækvivalensrelation harmonerende med en komposition har fra gammel tid (Gauss, 1777-1855) sin egen betegnelse, idet man siger at "a er kongruent med b modulo m" og skriver det $a \equiv b \pmod{m}$. De foregaaende resultater viser, at der paa $(\dot{Z},+)$ ikke findes andre ækvivalensrelationer harmonerende med +.

De tilsvarende ækvivalensklasser kaldes restklasser modulo m, og en restklasse er altsaa mængden af hele tal som giver samme rest r_o ved division med m. Faktorgruppen $(\dot{Z},+)/(m)$ betegnes som den additive gruppe af restklasser modulo m og skrives $(\dot{Z}_m,+)$.

I de næste §§ begrundes udførligt hvorledes de hele tal har struktur som en ring $(\dot{Z},+,\cdot)$. Det viser sig endda at blive det der betegnes som en integritetsring (eller integritetsomraade), hvilket defineres som en ring der har et etelement og hvori nulreglen gælder og hvor multiplikationen er kommutativ.

Men i den specielle integritetsring $(\dot{Z},+,\cdot)$ af de hele tal gælder ydermere, at alle de ækvivalensrelationer som harmonerer med + ogsaa harmonerer med $\cdot$. For den trivielle ækvivalens hvor ethvert element kun er ækvivalent med sig selv er det klart. I det ikke-trivielle tilfælde skal vi vise, at $a \equiv a' \pmod m \wedge b \equiv b' \pmod m$ medfører at $ab \equiv a'b' \pmod m$, men det ses let, idet omskrivningen $ab - a'b' = (a-a')b + a'(b-b')$ viser, at denne størrelse er delelig med m.

Kongruens $a \equiv a' \pmod m$ harmonerer altsaa baade med + og $\cdot$, og ifølge den almindelige homomorfisætning betyder det, at ringen $(\dot{Z},+,\cdot)$ kan afbildes homomorft paa en restklassering $(\dot{Z}_m,+,\cdot)$. Taleksempel: m = 2 giver en restklassering med 2 elementer, der kan betegnes som "lige" og "ulige", og med hvilke man kan regne efter reglerne "lige"+"lige"="lige", "lige"+"ulige" ="ulige",...,"ulige"·"ulige"="ulige".

Regning i en restklassering sker i praksis ved at regne med repræsentanter fra restklasserne. F.eks. finder man at i $(\dot{Z}_6,+,\cdot)$ bliver produktet af restklasserne der indeholder repræsentanterne 2 hhv. 3 lig restklassen der indeholder restklassen 6, altsaa ringens nulelement. I denne ring gælder nulreglen altsaa ikke, og man ser umiddelbart, at det samme er tilfældet i ethvert $(\dot{Z}_m,+,\cdot)$, hvor m er et sammensat tal. Da restklasseringen er homomorft billede af ringen $(\dot{Z},+,\cdot)$ i hvilken nulreglen gælder, har vi dermed det tidligere lovede eksempel paa at en ring med nulregel ved homomorf afbildning kan give en ring uden nulregel.

Hvis p er et primtal vil derimod nulreglen gælde i $(\dot{Z}_p,+,\cdot)$. Thi dersom et repræsentantprodukt ab er deleligt med p maa enten a eller b være delelig med p. Heraf følger atter, at <u>for et primtal p er $(\dot{Z}_p,+,\cdot)$ et legeme</u>. Der gælder nemlig almindeligt, at <u>en endelig ring (mindst 2 elementer) hvori nulreglen gælder er et legeme.</u> For at indse det skal vi blot vise, at hvis $x \neq 0$ er division med x altid mulig (side 3); vi viser det for venstredivision: vi multiplicerer x med ringens forskellige elementer xy', xy'', ... og p.g.a. nulreglen bliver produkterne alle forskellige, det maa derfor være samtlige elementer, og en ligning xy = z er derfor altid løselig, hvormed beviset er ført. (Paa side 3 vistes, at nulreglen følger af at division med $x \neq 0$ altid er mulig; for endelige ringe har vi her vist den modsatte implikation, for uendelige ringe gaar det ikke, f.eks. opfylder $(\dot{Z},+,\cdot)$ jo nulreglen, men er ikke noget legeme).

Lad os endnu bemærke, at et <u>tallegeme</u> defineres som et dellegeme af $(\dot{C},+,\cdot)$, det fremgaar senere, at mange saadanne eksisterer. Ogsaa: <u>I ethvert legeme gælder den lineære algebra.</u>

Tetraedergruppen.

(Til supplering og erstatning af undersøgelsen s. 22-25).

Ved tetraedergruppen T forstås gruppen af flytninger af et regulært tetraeder ind på sig selv. Ved den udvidede tetraedergruppe T_d forstås gruppen af isometrier, hvorved et regulært tetraeder afbildes ind på sig selv. Hvis f og g er to af de nævnte flytninger, vil gruppekompositionen g∘f, eller kortere skrevet gf, altså betegne den flytning der fås ved først at udføre flytningen f og dernæst flytningen g.

Ved de nævnte flytninger vil tetraedrets midtpunkt blive liggende, og vælges dette punkt som begyndelsespunkt for et ortogonalt koordinatsystem, kan en flytning tilhørende T altså angives som en ortogonal 3×3-matrix (med determinant +1), medens et element fra T_d kan angives som en egentlig eller uegentlig ortogonal 3×3-matrix (med determinant +1 eller -1), og gruppekompositionen bliver matrixmultiplikation. Man ser altså, at T og T_d er isomorfe med undergrupper i gruppen af (egl. eller uegl.) 3-dimensionale ortogonalmatricer.

Lad tetraedrets hjørner hedde A_1, A_2, A_3, A_4; enhver af de nævnte flytninger bevirker en permutation af de 4 hjørner, men omvendt ser man også, at enhver permutation af de 4 hjørner fremkommer ved en isometrisk afbildning af tetraedret på sig selv, og gruppen T_d er derfor isomorf med den symmetriske gruppe S_4 af permutationer af 4 elementer. Ved en transposition vil to hjørner A_i og A_j ombyttes, medens de øvrige bliver liggende, og den tilsvarende ortogonale determinant må have værdien -1 (for hvis vi havde valgt et koordinatsystem med en akse i retningen

A_iA_j ville denne akse skifte orientering og de øvrige være uændrede, så at isometriens determinant er -1). Heraf ses, at enhver ulige permutation af hjørnerne får determinanten -1 og altså er en uegentlig flytning, medens de lige permutationer af hjørnerne giver (egentlige) flytninger, og gruppen T er derfor isomorf med den alternerende gruppe A_4. Undersøgelsen nedenfor af tetraedergrupperne kan derfor også opfattes som en undersøgelse af S_4 og A_4.

Da afbildningen $\underline{\underline{B}} \to$ det $\underline{\underline{B}}$ afbilder en gruppe af matricer med matrixmultiplikation homomorft ind i gruppen af determinantværdier med simpel multiplikation, ses, at de matricer som har determinanten 1 udgør en normal undergruppe, nemlig afbildningens kerne; i vort tilfælde ser vi altså, at T er en normal undergruppe af T_d (og iøvrigt gælder alment, at for ethvert n er A_n en normal undergruppe i S_n, thi afbildes permutationer f ved $f \to$ sign f vil afbildningens kerne jo netop være mængden af lige permutationer. Iøvrigt endnu mere alment: i en vilkårlig gruppe vil en undergruppe af index 2 være normal, thi afbildes undergruppens elementer på +1 og dens sideklasses elementer på -1 ser man let, at det er en homomorf afbildning over på gruppen $(\{1,-1\},\cdot)$, og undergruppen er kerne).

At en undergruppe N er normal undergruppe i en gruppe G betegner man kort med skrivemåden $N \lhd G$. Og vi har ovenfor fundet, at ord T = 12 og ord T_d = 24 og $T \lhd T_d$.

Vi skal nu undersøge strukturen af gruppen T eller den dermed isomorfe gruppe A_4. Ved opskrivningen af permutationerne af hjørnerne vil vi benytte cykelfremstillingen (se mat 1x, §5), og for at simplificere betegnelserne vil vi kun angive deres indices,

således at f. eks. (423) eller (423)(1) betyder, at hjørnet A_4 erstattes med A_2, A_2 erstattes med A_3, A_3 erstattes med A_4 og A_1 bliver liggende.

Identiteten (1)(2)(3)(4) er neutralelementet i T, betegnes e. Hvis vi drejer tetraedret 120° om en af dets højder, f. eks. den gennem A_1, får vi et element af T, nemlig (1)(234); det er af 3. orden, og dets anden potens er (1)(243); elementerne af denne type vil vi kalde a, og det er netop dem hvis cykelfremstilling er af formen $(\cdot)(\cdot\cdot\cdot)$; der er 4 muligheder for højden, og for hver af disse 2 drejningsmuligheder. Hvis vi lægger en linie gennem midtpunkterne af to modstående kanter af tetraedret, f. eks. kanterne A_1A_2 og A_3A_4, og drejer det 180° om linien, får vi et element af T, nemlig (12)(34); elementerne af denne type vil vi kalde b, og det er netop dem, hvis cykelfremstilling er af formen $(\cdot\cdot)(\cdot\cdot)$; der er 3 par modstående kanter.

Vi får altså følgende gruppeelementer i T:

type	cykler	orden	antal
e	$(\cdot)(\cdot)(\cdot)(\cdot)$	1	1
a	$(\cdot)(\cdot\cdot\cdot)$	3	8
b	$(\cdot\cdot)(\cdot\cdot)$	2	3

I alt 12 = ord T.

Lad os bestemme undergrupperne i T. Der er for det første de to trivielle, $\{e\}$ og hele T. Et element a frembringer en cyklisk 3. ordens gruppe bestående af elementerne e,a og a^2, og den samme gruppe frembringes af a^2, idet $(a^2)^2 = a^4 = a$; dens struktur er som $(\mathbb{Z}_3,+)$, og antallet af sådanne undergrupper bliver altså $8/2 = 4$. Analogt vil de 3 elementer b frembringe 3

undergrupper af 2. orden, altså af struktur $(\dot{Z}_2,+)$. Der er yderligere en undergruppe af 4. orden, bestående af e og de tre elemneter af type b, det kan vi se således: Lad X,Y og Z betegne linierne som hver forbinder to modstående kanters midtpunkter (de er iøvrigt indbyrdes ortogonale, thi hvis tetraedret indskrives i en terning bliver det linierne gennem midtpunkterne af modstående sideflader i terningen), og man ser, at enhver flytning tilhørende T bevirker en permutation af disse linier, og sammensætning af flytninger betyder sammensætning af de tilsvarende permutationer; vi har altså en homomorf afbildning af T ind i gruppen af permutationer af X,Y og Z, og man ser at netop e og elementerne b lader X,Y og Z ligge fast, og udgør afbildningens kerne og dermed en undergruppe, endda normal, i T. Undergruppen er af 4. orden og ikke cyklisk, d.v.s. at dens struktur er som "firgruppen" (smlgn. øv. 28).

Idet vi nedenfor viser, at vi hermed har udtømt alle muligheder, vil vi tabellægge det fundne.

Undergrupper i tetraedergruppen T (eller i A_4):

orden	elementer	antal	struktur	normal
1	{e}	1	e	$\lhd$ T
2	{e,b}	3	$(\dot{Z}_2,+)$	
3	$\{e,a,a^2\}$	4	$(\dot{Z}_3,+)$	
4	{e,b,b'.b''}	1	firgr.	$\lhd$ T
6	---	0	-	
12	alle	1	A_4	$\lhd$ T

I alt 10

Ifølge Lagrange's sætning (første side 22) vil ordenen af en undergruppe være divisor i gruppens orden, og det samme gælder for ethvert elements orden. En undergruppe må altså have en af de anførte ordener. En undergruppe af 2. orden må være cyklisk og frembragt af et element af 2. orden, og der er altså ikke andre muligheder end de anførte; tilsvarende gælder for undergrupper af 3. orden. En 4. ordens undergruppe kan kun indeholde elementer, hvis orden går op i 4, d.v.s. elementer af type e og b, og der er altså netop den anførte. At der ikke er nogen af 6. orden gemmer vi et øjeblik.

Vi minder om, at en undergruppe er normal, hvis og kun hvis den kan være kerne ved en homomorf afbildning af hele gruppen. For enhver gruppe G er de to trivielle undergrupper $\{e\}$ og G normale, nemlig kerne for hhv. en isomorfi og en afbildning hvorved hele G afbildes på ét element. I den specielle undersøgelse ovenfor er det vist, at den 4. ordens undergruppe er normal. Vi mangler at vise, at der ikke er andre normale.

Vi vil først vise et par almene sætninger om endelige grupper. Hvis $N \triangleleft G$ og H er undergrupper i G, så er $(N \cap H) \triangleleft H$ og faktorgruppen $H/(N \cap H)$ er (pånær isomorfi) en undergruppe i G/N og ord H · ord N går op i ord G · ord $(N \cap H)$. Beviset er let: Lad φ være en homomorf afbildning af G med N som kerne, billedgruppen er et eksemplar af G/N. Betragter vi restriktionen af φ til H bliver billedet en gruppe, som er en delmængde af den forrige billedmængde, altså en undergruppe i G/N, og man ser, at kernen netop er $N \cap H$; ordenen af G/N er ord G/ord N, og den er ifølge Lagrange delelig med ordenen af undergruppen, som er ord H/ord $(N \cap H)$, og hvis man heri ganger overkors får man sætningens sidste påstand,

hvormed beviset er fuldført.

Specielt giver sætningen en begrænsning nedad af ord$(N \cap H)$, men den er et specialtilfælde af en almindeligere sætning, hvori der ikke længere er tale om normal undergruppe: Hvis en gruppe G har undergrupper H og K, så er ord $(H \cap K) \geq$ ord H · ord K/ord G. Bevis: $H \cap K$ er en undergruppe og indeholdt i K, altså en undergruppe i K. Så er K foreningsmængde af disjunkte sideklasser $x(H \cap K)$, $y(H \cap K)$,..., og da alt dette udspilles i K vil $x,y \in K$, og dermed $x^{-1}y \in K$; men når sideklasserne er forskellige vil $x^{-1}y \notin H \cap K$, hvoraf ses at $x^{-1}y \notin H$, hvilket viser, at xH og yH er forskellige sideklasser til H i G. Altså har H mindst ligeså mange forskellige sideklasser i G som $H \cap K$ har i K, eller ord G/ord H $\geq$ ord K/ord $(H \cap K)$, hvilket er det påstående.

Lad os endelig bemærke, at hvis φ er en homomorf afbildning af en gruppe, så vil ord $\varphi(x)$ gå op i ord x. Lad m betegne ord x, så er $\varphi(x)^m = \varphi(x^m) = \varphi(e)$ = etelement i billedgruppen, hvilket viser, at m er et multiplum af ord $\varphi(x)$.

Lad os nu vise, at der ikke er nogen undergruppe H af 6'orden. Vi tager en 3'ordens undergruppe som K og bruger sætningen ovenfor, som viser at ord $(H \cap K) \geq 6 \cdot 3/12 = 3/2$, så $H \cap K$ omfatter mere end e, og dermed et element a og så også a^2; som K kan benyttes enhver af de 3'ordens undergrupper, så H må indeholde alle 8 elementer af type a, hvilket er en modstrid.

En 3'ordens undergruppe i T kan ikke være normal: ved en tilsvarende homomorfi vil to elementer af type a ligge i kernen og gå over i etelementet, og for de øvrige 6 af type a vil ord $\varphi(a)$ gå op i ord a = 3, og billederne altså være af 3'orden, hvilket ifølge Lagrange strider mod, at billedgruppens orden er 12/3 = 4.

Analogt ses, at en 2'ordens undergruppe ikke kan være normal: de 8 elementer af type a ville give 4 billedelementer af 3'orden, men det kan ikke findes i en gruppe af 6'orden; thi de ville frembringe (mindst) to forskellige cykliske undergrupper af 3'orden med kun etelementet fælles, og indsættes det i sætningen med H og K ovenfor fås $1 \geq 3 \cdot 3/6 = 3/2$, altså modstrid.

Dermed er alle påstandene om undergrupperne i T bevist. Man kunne naturligvis også have vist dem enten ved geometriske betragtninger, eller ved at betragte de 144 værdier i gruppetavlen for A_4.

Den udvidede tetraedergruppe T_d indeholder også de uegentlige flytninger svarende til de ulige permutationer. Der er to typer, nemlig

type	cykler	orden	antal
c	$(\cdot\cdot)(\cdot)(\cdot)$	2	6
d	$(\cdot\cdot\cdot\cdot)$	4	6

ialt 12 = ord T_d - ord T

Type c er spejling i et af tetraedrets symmetriplaner , hvorved de to hjørner i symmetriplanen bliver liggende, og de to andre hjørner ombyttes, altså en transposition. Type d kan beskrives med glosen "drejespejling".

Vi skal ikke her foretage den fuldstændige bestemmelse af alle undergrupper i T_d (eller den dermed isomorfe S_4) - der er ialt 30 stk. af en halv snes forskellige arter - men vi vil nøjes med at bestemme de normale undergrupper.

Antag $N \lhd T_d$. Vi anvender sætningen s. 30, idet vi sætter H = T, og får et ord N går op i (24/12) ord $(N \cap T)$ = 2 ord $(N \cap T)$, og at $N \cap T$ må være en af de ovenfor fundne normale undergrupper i T. Altså er N enten en af de normale undergrupper i T eller vil fremgå af en sådan ved tilføjelse af lige så mange elementer fra $T_d \setminus T$. Lad os gennemgå mulighederne:

Hvis $N \cap T$ er lig T, så er enten N lig T, og den har vi tidligere (s. 27) noteret som normal i T_d, eller N er hele T_d, og den er normal i sig selv.

$N \cap T$ kan være firgruppen $\{e,b,b',b''\}$, og beviset s. 29 for at denne mængde er en homomorfikerne gælder uændret indenfor T_d, og firgruppen er altså normal undergruppe i T_d (faktorgruppen bliver af 6'orden og består altså af alle 6 permutationer af linierne X,Y og Z, medens indenfor T blev fak-

torgruppen kun af 3'orden,hvilket man også kan indse geometrisk). Hvis N bestod af firgruppen suppleret med 4 elementer fra $T_d \backslash T$, blev den af 8'orden, og faktorgruppen blev af 3'orden, men ifølge sætningen om ord $\varphi(x)$ skulle så de 16 elementer i $T_d \backslash N$ have en orden delelig med 3, og sådan 16 elementer findes jo ikke.

Hvis $N \cap T$ er lig $\{e\}$, så er enten $n = \{e\}$, som vi ved, er trivielt normal , eller også består N af to elementer, altså foruden e et af 2'orden, som må være af type c; vi kan nummerere således,at $c = (12)(3)(4)$ og antage $N = \{e,c\}$; en modstrid fremgår let ved at regne med permutationer, thi hvis N normal skulle $x^{-1}cx \in \{e,c\}$, hvilket svigter for næsten alle valg af x, f.eks. giver $x = (1234)$ at $x^{-1}cx = (14)(2)(3)$.

Ialt får vi

Normale undergrupper i T_d (eller i gruppen S_4) af 24'orden:

orden	elementer	antal	struktur
1	$\{e\}$	1	$\{e\}$
4	$\{e,b,b',b''\}$	1	firgr.
12	{lige perm.}	1	A_4
24	alle	1	S_4

Man ser altså. at af de ialt 30 undergrupper i S_4 er kun de 4 normale. Dette er i grel kontrast til situationen for abelske grupper, thi, som man umiddelbart ser af de tidligere fundne karakteriseringer af normal undergruppe: I en abelsk gruppe er enhver undergruppe normal.

Øvelser til Algebraens grundbegreber, § 1.

1. Gør rede for, at hver af følgende kompositioner

   a) $x * y = (x^2 + y^2)^{\frac{1}{2}}$, $x,y \in \dot{R}$,

   b) $x * y = (x^2 + y^2)^{\frac{1}{2}}$, $x,y \in \dot{R}_+ \cup \{0\}$,

   c) $x * y = (xy)^{\frac{1}{2}}$, $x,y \in \dot{R}_+$,

   d) $x * y$ = største fælles divisor for x og y, $x,y \in \dot{N}$,

   er en komposition inden for den nævnte mængde, og undersøg, om kompositionen er associativ, kommutativ, om der findes et neutralt element og i bekræftende fald, hvilke elementer der er invertible; undersøg endelig, hvilke elementer der kan bortforkortes.

2. I mængden $\hat{F}(E \to \dot{R})$ af reelle funktioner med en given mængde $E \neq \emptyset$ som definitionsmængde indføres kompositioner $+$ og $\cdot$, idet man for $f,g \in \hat{F}(E \to \dot{R})$ ved $f + g$, henholdsvis fg, forstår funktionerne

   $t \to f(t) + g(t)$, $t \in E$, og $t \to f(t)g(t)$, $t \in E$.

   Gør rede for, at $+$ er en kommutativ gruppekomposition inden for $\hat{F}(E \to \dot{R})$, medens $\cdot$ er en associativ og kommutativ komposition med neutralt element inden for $\hat{F}(E \to \dot{R})$. Bestem de ved $\cdot$ invertible elementer af $\hat{F}(E \to \dot{R})$.

3. Lad E være en ikke tom mængde og X_E mængden af alle funktioner fra E til $\{0,1\}$. Idet addition og multiplikation af reelle funktioner med E som definitionsmængde tænkes indført som i øvelse 2, sætter vi for $\chi_1, \chi_2 \in X_E$

   $$\chi_1 \dot{+} \chi_2 = \chi_1 + \chi_2 - \chi_1\chi_2.$$

   Vis, at $\cdot$ og $\dot{+}$ er kompositioner inden for X_E, og vis, at den enentydige korrespondance mellem mængden $\dot{D}(E)$ af delmængder

af E og X_E, hvor $A \in \dot{D}(E) \leftrightarrow \chi \in X_E$ betyder

$$\chi(x) = \begin{cases} 1 \text{ for } x \in A \\ 0 \text{ for } x \in CA, \end{cases}$$

er en isomorfi såvel mellem $(\dot{D}(E), \cap)$ og $(X_E, \cdot)$ som mellem $(\dot{D}(E), \cup)$ og $(X_E, \dot{+})$.

4. Idet n er et givet naturligt tal, skal man vise, at den ved $x \to x^n$ bestemte funktion med definitionsmængde $\dot{Q}$, henholdsvis $\dot{R}$, er en homomorf afbildning af $(\dot{Q}, \cdot)$, henholdsvis $(\dot{R}, \cdot)$ ind i sig selv. Undersøg i hvert af de to tilfælde, for hvilke værdier af n afbildningen er isomorf.

5. Gør rede for, at

a) $$z \to \bar{z}, \quad z \in \dot{C},$$

er en endomorf afbildning såvel af $(\dot{C}, +)$ som af $(\dot{C}, \cdot)$,

b) $$z \to (z + \bar{z})/2, \quad z \in \dot{C},$$

er en homomorf afbildning af $(\dot{C}, +)$ ind i $(\dot{R}, +)$,

c) $$z \to |z|, \quad z \in \dot{C},$$

er en homomorf afbildning af $(\dot{C}, \cdot)$ ind i $(\dot{R}, \cdot)$,

d) $$z \to z/|z|, \quad z \in \dot{C} \setminus \{0\},$$

er en endomorf afbildning af $\{\dot{C} \setminus \{0\}, \cdot\}$.

I hvilke tilfælde er afbildningen isomorf ?

6. Idet c er et givet positivt reelt tal, sættes

$$v_1 * v_2 = \frac{v_1 + v_2}{1 + v_1 v_2 / c^2} \quad \text{for } v_1, v_2 \in]-c, c[.$$

(Einsteins lov for sammensætning af parallelle hastigheder.)

Vis, at $*$ er en komposition inden for intervallet $]-c, c[$, og at $(]-c, c[, *)$ er en gruppe.

* Vis, at $(]-c,c[,*)$ er isomorf med $(\grave{R},+)$. (Dette går ud på at finde en bijektiv funktion $f: \grave{R} \to]-c,c[$, således at

$$\forall_{\grave{R}} x,y: f(x + y) = f(x) * f(y).$$)

7. Er $(\grave{R},+)$ isomorf med $(\grave{R},\cdot)$? med $(\grave{R} \setminus \{0\},\cdot)$?

8. Bestem samtlige automorfe afbildninger af $(\grave{N},\cdot)$. (Undersøg, hvad et primtal kan føres over i ved en sådan afbildning.)

9. Vis, at enhver endomorf afbildning f af $(\grave{Z},+)$, d.v.s. en funktion $f: \grave{Z} \to \grave{Z}$, der tilfredsstiller "funktionalligningen"

$$\forall_{\grave{Z}} x,y: f(x + y) = f(x) + f(y),$$

er af formen $x \to ax$, $x \in \grave{Z}$, altså at $\exists_{\grave{Z}} a \; \forall_{\grave{Z}} x: f(x) = ax$.

Vis samme påstand, idet $\grave{Z}$ overalt erstattes med $\grave{Q}$.

Vis, at enhver endomorf afbildning f af $(\grave{R},+)$, som tillige er voksende, d.v.s.

$$\forall_{\grave{R}} x,y: x < y \Rightarrow f(x) \leqq f(y),$$

er af formen $x \to ax$, $x \in \grave{R}$, hvor $a \geqq 0$. (Man kan f.eks. benytte, at hvert irrationalt tal er grænseværdi såvel for en voksende som for en aftagende følge af rationale tal.)

10. Benyt det sidste resultat i øvelse 9 til at vise:

a) Enhver homomorf afbildning f af $(\grave{R},+)$ ind i $(\grave{R}_+,\cdot)$, d.v.s. en funktion $f: \grave{R} \to \grave{R}_+$, der tilfredsstiller funktionalligningen

$$\forall_{\grave{R}} x,y: f(x + y) = f(x)f(y),$$

er, hvis den tillige er voksende, af formen $x \to a^x$, $x \in \grave{R}$, hvor $a \geqq 1$. (Sammensæt f med en passende isomorf afbildning.)

b) Enhver homomorf afbildning f af $(\grave{R}_+,\cdot)$ ind i $(\grave{R},+)$, d.v.s. en funktion $f: \grave{R}_+ \to \grave{R}$, der tilfredsstiller funktionalligningen

$$\forall_{\grave{R}_+} x,y: f(xy) = f(x) + f(y),$$

er, hvis den tillige er voksende, enten af formen $x \to \log_a x$, $x \in \dot{R}$, hvor $a > 1$, eller den er identisk 0.

c) Enhver endomorf afbildning f af $(\dot{R}_+,\cdot)$, d.v.s. en funktion $f: \dot{R}_+ \to \dot{R}_+$, der tilfredsstiller funktionalligningen

$$\forall_{\dot{R}_+} x,y: f(xy) = f(x)f(y),$$

er, hvis den tillige er voksende, af formen $x \to x^a$, $x \in \dot{R}_+$, hvor $a \geq 0$.

Angiv endelig alle aftagende, homomorfe afbildninger af $(\dot{R},+)$ og $(\dot{R}_+,\cdot)$ ind i $(\dot{R},+)$ og $(\dot{R}_+,\cdot)$.

11. Opskriv kompositionstavler for $(\dot{Z}_m,+)$ og $(\dot{Z}_m,\cdot)$ for $m = 2, 3, 4$ og 5 og undersøg i hvert af de 4 tilfælde, om multiplikation modulo m er en komposition, evt. en gruppekomposition inden for $\dot{Z}_m \setminus (0)_m$.

12. For $x_1, x_2 \in \dot{R}_+$ sættes $x_1 \sim x_2$, hvis de to tal kan skrives som evt. uendelige decimalbrøker med samme cifre i samme rækkefølge, altså afvigende højst ved kommaets placering. Gør rede for, at der herved er defineret en ækvivalensrelation i $\dot{R}_+$, som harmonerer med multiplikation. Mængden af ækvivalensklasser med multiplikation ved repræsentanter er da en gruppe; angiv en hermed isomorf gruppe.

13. I $\dot{N}^2$ defineres en komposition + ved

$$(p,q) + (r,s) = (p+r,q+s)$$

og en relation $\sim$ ved

$$(p_1,q_1) \sim (p_2,q_2) \Leftrightarrow p_1 + q_2 = p_2 + q_1.$$

Vis, at $\sim$ er en ækvivalensrelation i $\dot{N}^2$, som harmonerer med +. Vis, at mængden af ækvivalensklasser med addition ved repræsentanter er en gruppe, isomorf med $(\dot{Z},+)$.

14. Om en associativ og kommutativ komposition $*$ inden for en mængde M forudsættes, at hvert element af M kan bortforkortes. I M^2 defineres en komposition, som vi også vil betegne med $*$, ved

$$(p,q) * (r,s) = (p*r, q*s)$$

og en relation $\sim$ ved

$$(p_1,q_1) \sim (p_2,q_2) \Leftrightarrow p_1 * q_2 = p_2 * q_1 .$$

Vis, at $\sim$ er en ækvivalensrelation i M^2, som harmonerer med $*$. Vis, at mængden af ækvivalensklasser organiseret ved regning med repræsentanter er en kommutativ gruppe.

Gør rede for, at "konstruktionen" for $(M,*) = (\mathbb{N},\cdot)$ fører til en med $(\mathbb{Q}_+,\cdot)$ isomorf gruppe.

Øvelser til Algebraens grundbegreber, § 2.

1. Lad $\cdot$ være en associativ komposition inden for en mængde G. Det forudsættes, at hver af ligningerne

$$ax = b \quad \text{og} \quad ya = b$$

for vilkårligt opgivne $a,b \in G$ har mindst en løsning. Vis, at $(G,\cdot)$ er en gruppe. (Begynd f.eks. med at vise, at en løsning til en ligning af formen $ya = a$ må være neutralt element.)

2. Lad $\cdot$ være en associativ komposition inden for en endelig mængde G. Det forudsættes, at forkortningsreglerne

$$ax = ay \Rightarrow x = y \quad \text{og} \quad xa = ya \Rightarrow x = y$$

gælder for $a,x,y \in G$. Vis, at $(G,\cdot)$ er en gruppe. (Resultatet fra øv.1 kan benyttes.)
Vis ved et modeksempel, at tilsvarende ikke gælder for uendelige mængder.

3.* Lad $\cdot$ være en associativ komposition inden for en mængde G, og lad e være et element af G. Vis, at det er tilstrækkeligt for, at $(G,\cdot)$ er en gruppe med e som neutralt element, at

$$\forall_G x\colon ex = x \quad \text{og} \quad \forall_G x\, \exists_G y\colon yx = e,$$

altså at e er "venstre neutralt", og at hvert element af G har et "venstre inverst".

4. For hvilke grupper $(G,\cdot)$ er afbildningen $x \to x^{-1}$, $x \in G$, automorf ?

5. Lad $(G,\cdot)$ være en gruppe og $H \neq \emptyset$ en endelig delmængde af G, hvor

$$\forall_H x,y\colon xy \in H.$$

Vis, at H er en undergruppe af $(G,\cdot)$.
Vis ved et modeksempel, at tilsvarende ikke gælder for H uendelig.

6. Lad H og K være undergrupper af en gruppe $(G,\cdot)$. Vis, at $H \cup K$ ikke er en undergruppe af $(G,\cdot)$, medmindre $H \subsetneq K$ eller $K \subsetneq H$.

7. Beskriv den mindste undergruppe af $(\dot{Q}_+,\cdot)$, der indeholder en given mængde P af primtal.
Vis, at mængden af undergrupper af $(\dot{Q}_+,\cdot)$ ikke er numerabel.

8. Idet H er en undergruppe og g et element af gruppen $(G,\cdot)$, skal man vise, at $(gHg^{-1},\cdot)$, hvor

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\},$$

er en med $(H,\cdot)$ isomorf undergruppe af $(G,\cdot)$. (Den kaldes en til $(H,\cdot)$ konjugeret undergruppe af G.)

Lad specielt $(G,\circ)$ være en transformationsgruppe for en mængde E, og lad H_α betegne undergruppen bestående af de transformationer tilhørende G, der lader elementet $\alpha \in E$ gå over i sig selv. Idet $g \in G$, skal man da vise, at

$$g \circ H_\alpha \circ g^{-1} = H_{g(\alpha)}.$$

9. Vis, at de isometrier af en plan, ved hvilke et givet kvadrat i denne afbildes på sig selv, danner en gruppe $(D_4,\circ)$

af orden 8 (som er isomorf med gruppen af de flytninger af rummet, ved hvilke kvadratet afbildes på sig selv). Undersøg, om gruppen er kommutativ.

De til D_4 hørende flytninger af planen udgør en undergruppe C_4 af orden 4. De til D_4 hørende isometrier, ved hvilke hver af kvadratets diagonaler afbildes på sig selv, danner en anden undergruppe V af orden 4 (som er isomorf med gruppen af flytninger af rummet, ved hvilke hver af tre parvis givne, vinkelrette linier afbildes på sig selv). Vis, at de to undergrupper ikke er isomorfe.

10. Opstil gruppetavler for de to i øv.9 omtalte grupper af orden 4, og angiv undergrupper af $(S_4, \circ)$, som de er isomorfe med.

11. Idet $M = \dot{R} \setminus \{0,1\}$, betragtes de for $t \in M$ definerede funktioner

$$f_1(t) = t \quad , \quad f_2(t) = 1/t \quad , \quad f_3(t) = 1-t \quad ,$$

$$f_4(t) = t/(t-1), \quad f_5(t) = 1/(1-t), \quad f_6(t) = (t-1)/t,$$

Vis, at $(\{f_1,f_2,f_3,f_4,f_5,f_6\}, \circ)$ er en med den symmetriske gruppe $(S_3, \circ)$ isomorf transformationsgruppe for M. (Giv intervallerne $]-\infty,0[$, $]0,1[$ og $]1,\infty[$, hvis foreningsmængde er M, numrene 1, 2 og 3, og undersøg, hvorledes de afbildes ved funktionerne f_i.)

12. Lad der være givet et tal $c \in \dot{R}_+$. For et vilkårligt $\alpha \in \dot{R}$ betragtes afbildningen $f_\alpha: \dot{R}^2 \to \dot{R}^2$, hvorved til hvert $(x,t) \in \dot{R}^2$ svarer talparret (x',t') bestemt ved

$$x' = x \cosh \alpha - ct \sinh \alpha$$

$$ct' = -x \sinh \alpha + ct \cosh \alpha \ .$$

Vis, at $f_\alpha: \grave{R}^2 \to \grave{R}^2$ er bijektiv. Idet (x,t) og (x',t') fortolkes som sædvanlige retvinklede koordinater for punkter i planen, skal man tillige vise, at hver af linierne $x = ct$ og $x = -ct$ og ligeledes for vilkårligt $r \in \grave{R}_+$ hver gren af hyperblen med ligningen

$$x^2 - ct^2 = r^2$$

afbildes på sig selv. (Parameterfremstillingerne

$$\begin{aligned} x &= r \cosh u \\ ct &= r \sinh u, \end{aligned} \quad u \in \grave{R}, \qquad \begin{aligned} x &= -r \cosh u \\ ct &= r \sinh u, \end{aligned} \quad u \in \grave{R},$$

for hyperblens grene kan benyttes med fordel.)

Vis, at der for $\alpha,\beta \in \grave{R}$ gælder $f_\alpha \circ f_\beta = f_{\alpha+\beta}$, og begrund herved, at $(\{f_\alpha | \alpha \in \grave{R}\}, \circ)$ er en med $(\grave{R},+)$ isomorf transformationsgruppe. (Gruppen af specielle Lorentz transformationer. Fortolk c som lysets hastighed, t som tiden og $v = c \operatorname{tgh} \alpha$ som den konstante hastighed af x'-koordinatsystemet i forhold til x-koordinatsystemet på en linie.)

13. Hvilke funktioner $f: R_+ \to R_+$ svarer til translationer $x \to x + c$, $x \in \grave{R}$, og homotetier $x \to cx$, $x \in \grave{R}$, af $\grave{R}$ ved den enentydige korrespondance $e^x = y$ mellem $\grave{R}$ og $\grave{R}_+$?

14. a) Idet f er en drejning af planen om et punkt A og s spejlingen af planen i en linie l, skal man gøre rede for, at $s \circ f \circ s$ er en drejning om spejlbilledet s(A) af punktet A med hensyn til linien l. Er planen orienteret, og φ et vinkeltal for drejningen f, vil $-\varphi$ være et vinkeltal for drejningen $s \circ f \circ s$.

b) Idet f er en drejning af rummet om en linie l og s spejlingen af rummet i en plan π, skal man gøre rede for,

at $s \circ f \circ s$ er en drejning om spejlbilledet $s(l)$ af linien l med hensyn til planen π. Tænkes linien l orienteret, hvilket giver anledning til en orientering også af spejlbilledet $s(l)$ gælder der endvidere, idet omløbsretningen om en orienteret linie modsat urvisernes, set fra liniens positive ende, regnes positiv: er φ et vinkeltal for drejningen f, vil $-\varphi$ være et vinkeltal for drejningen $s \circ f \circ s$.

c) Lad g og h være drejninger af rummet om to hinanden skærende linier m og n. Idet spejlingen i den ved m og n bestemte plan betegnes med t, skal man påvise, at $t \circ g^{-1} \circ t = g$, og at

$$g \circ h = t \circ (h \circ g)^{-1} \circ t,$$

samt ud fra det sidste resultat beskrive sammenhængen mellem $g \circ h$ og $h \circ g$ geometrisk.

15. Planen tænkes delt i kongruente kvadrater ved et netværk af rette linier. Vis, at enhver flytning af planen, hvorved netværket går over i sig selv, kan sammensættes af en drejning om midtpunktet i et givet af kvadraterne og en translation. Vis, at gruppen af flytninger af planen, hvorved netværket går over i sig selv, kan karakteriseres som den mindste transformationsgruppe indeholdende to passende flytninger, nemlig dels en drejning og en translation, dels to drejninger.

16. Planen tænkes delt i kongruente regulære sekskanter (som en bikage) ved et netværk af rette liniestykker. Vis, at gruppen af flytninger af planen, hvorved netværket går over i sig selv, kan karakteriseres som den mindste transformationsgruppe

indeholdende to passende flytninger, nemlig dels en drejning og en translation, dels to drejninger. Vis, at gruppen også kan opfattes som bestående af de flytninger af planen, hvorved et netværk, der deler planen i kongruente ligesidede trekanter, går over i sig selv.

17. Idet a og b er hele tal, som ikke begge er 0, skal man vise, at $H = \{ax + by \mid x,y \in \mathbb{Z}\}$ er en undergruppe af $(\mathbb{Z},+)$ og følgelig kan skrives på formen $H = \{zd \mid z \in \mathbb{Z}\}$, hvor $d \in \mathbb{N}_+$. Vis videre, at d er største fælles divisor for a og b.

Idet også c er et helt tal, skal man angive en nødvendig og tilstrækkelig betingelse for, at den "diofantiske ligning"

$$ax + by = c$$

har en løsning (x,y) bestående af hele tal. (En ligning med ubekendte, for hvilke der søges heltallige værdier, kaldes en diofantisk ligning efter den græske matematiker Diofantos, ca. +250, der har behandlet sådanne opgaver.)

18. Lad a, b og c være hele tal, a og b ikke begge 0.
Gør rede for, at mængden af heltallige løsninger (x,y) til ligningen

$$ax + by = 0$$

kan skrives på formen $\{(pt,qt) \mid t \in \mathbb{Z}\}$. Under forudsætning af, at ligningen

$$ax + by = c$$

har en heltallig løsning (x_0,y_0), skal man dernæst angive alle dens heltallige løsninger.

Eksempler: $3x - 4y = 1$, $6x - 8y = 4$.

19. Vis, at enhver undergruppe $(H,\cdot)$ af en cyklisk gruppe $(G,\cdot)$ ligeledes er cyklisk. (Lad c være en frembringer for $(G,\cdot)$ og betragt mængden $\{n \in \grave{Z} \mid c^n \in H\}$.)

20. Idet c er frembringer for en cyklisk gruppe med m elementer, skal man vise, at elementet c^k har ordenen m/d, hvor d er største fælles divisor for m og k.

Eksempel: Angiv samtlige frembringere i $(\grave{Z}_{10},+)$.

21. Hvilke elementer af $(\grave{R}_1,+)$ har endelig orden ?

22. Gør rede for, at mængden $\{z \in \grave{C} \mid \exists_{\grave{N}} n: z^n = 1\}$ af samtlige komplekse enhedsrødder med multiplikation som komposition er en uendelig kommutativ gruppe, hvor hvert element har endelig orden.

* Giv et eksempel på en uendelig kommutativ gruppe, hvor hver ægte undergruppe er endelig. (Søg en passende undergruppe af ovennævnte.)

23. Vis, at hvis alle fra det neutrale element forskellige elementer af en gruppe har orden 2, vil gruppen være kommutativ.

Angiv en gruppe med førstnævnte egenskab bestående af 4 isometrier af planen, henholdsvis 8 isometrier af rummet.

24. Vis, at antallet af elementer af orden 2 i en endelig gruppe af lige orden er ulige, i en endelig gruppe af ulige orden er lige.

Vis, at i en endelig kommutativ gruppe er kompositionen af alle elementer, hvis orden er større end 2, lig med det neutrale element.

25. Angiv såvel de venstre som de højre sideklasser til den af permutationen $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ frembragte cykliske undergruppe H af den symmetriske gruppe $(S_3,\circ)$ af alle permutationer af mængden $\{1,2,3\}$.

26. Beskriv inddelingen af gruppen af flytninger af planen i venstre (højre) sideklasser til undergruppen af translationer. (Benyt, at enhver flytning af planen er en translation eller en drejning.)

27.

	a_1	a_2	a_3	a_4	a_5	a_6
a_1					a_5	
a_2						
a_3						
a_4		a_1	a_2			a_3
a_5		a_4	a_1			
a_6						

Ovenstående er en delvis udfyldt gruppetavle for en kommutativ gruppe $(G,\cdot)$ med elementerne a_1,a_2,a_3,a_4,a_5,a_6. Opskriv den fuldstændige gruppetavle for $(G,\cdot)$. Undersøg, om den ved a_5 bestemte venstre translation $x \to a_5x$, $x \in G$, er en lige eller ulige permutation af G. Find samtlige undergrupper af $(G,\cdot)$.

28. Vis, at der pånær isomorfi findes netop to grupper af orden 4. (Analysen af en ikke cyklisk gruppe med 4 elementer knyttes med fordel til en kompositionstavle.)

29. En transformationsgruppe $(G,\circ)$ for en mængde E siges at være transitiv, hvis

$$\forall_E x,y\ \exists_G f\colon f(x) = y.$$

Vis, at ordenen af en transitiv gruppe $(G,\circ)$ af permutationer af en mængde E med n elementer er delelig med n. (Søg en undergruppe med index n.) Vis endvidere, idet n forudsættes ≥ 2, at G må indeholde en permutation, hvorved intet element af E går over i sig selv. (Foreningen af n undergrupper med index n kan ikke være hele G.)

30. Vis, at de inverse til elementerne i en venstre sideklasse til en undergruppe H af en gruppe $(G,\cdot)$ udgør en højre sideklasse til H. Vis, at mængden af venstre og mængden af højre sideklasser til H i $(G,\cdot)$ er ækvipotente.

31. I gruppen $(G,\cdot)$ siges et element $x \in G$ at være konjugeret med et element $y \in G$, hvis

$$\exists_G g\colon gx = yg.$$

Vis, at der herved defineres en ækvivalensrelation i G. Ækvivalensklasserne kaldes klasser af konjugerede elementer.

Vis, at en undergruppe af $(G,\cdot)$ er normal, hvis og kun hvis den er forening af klasser af konjugerede elementer.

32. Beskriv inddelingen af gruppen af flytninger af planen i klasser af konjugerede. Afgør herved, om undergruppen af translationer, henholdsvis af drejninger om et givet punkt, er normal. (Se øv.31.)

33. Idet $*$ er en komposition med definitionsmængde $L \times M$ og $N \subseteq L$, $P \subseteq M$, sættes

$$N * P = \{n * p \mid n \in N,\ p \in P\}.$$

Vis, at

$$N * P = \bigcup\{n * P \mid n \in N\} = \bigcup\{N * p \mid p \in P\}.$$

(Som det er sædvane, er her skrevet $h * K$ i stedet for $\{h\} * K$ og analogt.)

Lad nu H og K være undergrupper af en gruppe $(G,\cdot)$. Vis, at HK er en undergruppe af $(G,\cdot)$, hvis og kun hvis $HK = KH$. Vis, at HK er en undergruppe, hvis H eller K er en normal undergruppe af $(G,\cdot)$, og at HK er en normal undergruppe af $(G,\cdot)$, hvis H og K begge er det.

Vis, at hvis undergrupperne H og K er endelige, vil HK bestå af qr/s elementer, hvor q, r og s er antallet af elementer i H, K og $H \cap K$.

34. Vis, at mængden $\{a \in G \mid \forall_G x: ax = xa\}$ af elementer af en gruppe $(G,\cdot)$, som hvert er ombytteligt med alle elementer af G, er en normal undergruppe af $(G,\cdot)$. Den kaldes gruppens centrum.

Vis, at hvis gruppen har netop ét element af orden 2, må dette tilhøre centret.

35. Idet $a \neq 0$ og b er reelle tal, betegnes med $f_{a,b}$ afbildningen

$$x \to ax + b, \quad x \in \dot{R}.$$

Gør rede for, at $f_{a,b}$ er en homoteti eller translation af tallinien.

Vis, at afbildningerne $f_{a,b}$, $a \in \dot{R} \setminus \{0\}$, $b \in \dot{R}$, udgør en

transformationsgruppe, og at der ved $f_{a,b} \to a$ defineres en homomorf afbildning af denne på $(\dot{\mathbb{R}} \setminus \{0\}, \cdot)$; angiv kernen og beskriv den tilsvarende inddeling af transformationsgruppen i sideklasser.

36. Lad $(G,\cdot)$ være en gruppe, og lad der i G være givet en ækvivalensrelation $\sim$, som harmonerer med kompositionen. Idet gruppens neutrale element betegnes med e, skal man vise, at

$$H = \{x \in G \mid x \sim e\}$$

er en normal undergruppe af $(G,\cdot)$. Vis endvidere, at den givne ækvivalensrelation svarer til klasseinddelingen af G bestående af sideklasserne til H.

Hvilke ækvivalensrelationer harmonerer med kompositionen i en gruppe med 13 elementer?

37. Idet H er en normal undergruppe med endelig index n i en gruppe $(G,\cdot)$, skal man vise, at x^n tilhører H for hvert $x \in G$.

Slut heraf, at ingen af grupperne $(\dot{\mathbb{Q}},+)$ og $(\dot{\mathbb{R}},+)$ har ægte undergrupper med endelig index.

38. Gruppen af flytninger af rummet, ved hvilke et givet regulært oktaeder afbildes på sig selv, kaldes <u>oktaedergruppen</u> og betegnes med O. (Den er identisk med gruppen af flytninger, ved hvilke terningen, hvis hjørner er midtpunkterne af oktaedrets sideflader, afbildes på sig selv, og kunne derfor også kaldes for hexaedergruppen.)

Find de cykliske undergrupper af $(O,\circ)$ og bestem gruppens orden. Vis, at $(O,\circ)$ er isomorf med den symmetriske gruppe $(S_4,\circ)$.

Giv et geometrisk bevis for, at tetraedergruppen $(T,\circ)$ er en undergruppe af $(O,\circ)$.

Vis, at der findes en homomorf afbildning af $(0,\circ)$ på $(S_3,\circ)$. Bestem denne homomorfis kerne og undersøg, om der findes andre fra $\{e\}$ og 0 forskellige normale undergrupper af $(0,\circ)$.

39.* Gruppen af flytninger af rummet, ved hvilke et givet regulært ikosaeder afbildes på sig selv, kaldes ikosaedergruppen og betegnes med I. (Den er identisk med "dodekaedergruppen", idet midtpunkterne af ikosaedrets sideflader er et regulært dodekaeders hjørner.)

Find de cykliske undergrupper af $(I,\circ)$ og bestem gruppens orden. Vis, at $(I,\circ)$ er isomorf med den alternerende gruppe $(A_5,\circ)$.

Vis, at $(I,\circ)$ ikke har andre normale undergrupper end $\{e\}$ og I selv (at $(I,\circ)$ er en "simpel gruppe").

40.* Bevis, at hvis en gruppe af isometrier (af planen eller rummet) er endelig, vil alle dens isometrier have et fælles fixpunkt. (Benyt f.eks. følgende sætning: Til endelig mange givne punkter findes der blandt rummets punkter et og kun et, for hvilket kvadratsummen af dets afstande fra de givne punkter antager den mindst mulige værdi. Dette kan sluttes af den for vilkårlige vektorer $\underline{v},\underline{v}_1,\ldots,\underline{v}_n$ gyldige ligning

$$\sum_{\nu=1}^{n}(\underline{v}-\underline{v}_\nu)^2 = \sum_{\nu=1}^{n}(\underline{v}^*-\underline{v}_\nu)^2 + n(\underline{v}-\underline{v}^*)^2,$$

hvor

$$\underline{v}^* = \frac{1}{n}\sum_{\nu=1}^{n}\underline{v}_\nu \quad \cdot)$$

41. Vis, at hver fra $\{e\}$ forskellig endelig gruppe af flytninger af planen er cyklisk og består af drejningerne, ved

hvilke en regulær polygon (i tilfældet af ordenen 2, et liniestykke) afbildes på sig selv. (Benyt sætningen i øv.40, og betragt den drejning i gruppen, der har den mindste positive drejningsvinkel.)

42.* I rummet findes der følgende fra {e} forskellige endelige grupper af flytninger:

1) De cykliske grupper C_n, $n = 2,3,\ldots$. Gruppen C_n er af orden n og består af drejningerne, ved hvilke en regulær n-sidet pyramide (for n = 2 en ligebenet, men ikke ligesidet trekant) afbildes på sig selv. (For n = 3 må pyramiden ikke være et regulært tetraeder.)

2) Diedergrupperne D_n, $n = 2,3,\ldots$. Gruppen D_n er af orden 2n og består af drejningerne, ved hvilke et regulært n-sidet prisme (for n = 2 en rektangulær, men ikke kvadratisk skive) afbildes på sig selv. (For n = 4 må prismet ikke være en terning. For n > 2 kan prismet erstattes med en regulær n-kant, der kan opfattes som et regulært "polyeder" med to sideflader, et "dieder".)

3) Tetraedergruppen T, oktaedergruppen O, ikosaedergruppen I.

Gennemfør det nedenfor skitserede bevis for, at der ikke findes andre endelige grupper af flytninger af rummet.

Lad N være en sådan gruppes orden. De fra e forskellige N - 1 elementer er da drejninger om akser gennem et fast punkt F(se øv.40) og afbilder derfor en vilkårlig valgt kugleflade med centrum F på sig selv. Skæringspunkterne mellem kuglefladen og gruppens drejningsakser kan fordeles på klasser ved fastsættelsen, at to af dem skal høre til samme klasse, hvis der findes en drejning i gruppen, der fører det ene over i det andet. Lad $K_1,\ldots,K_m$ betegne disse klasser og n_μ

antallet af punkter i klassen K_μ. Hvert punkt i K_μ er fixpunkt for en cyklisk undergruppe, og dennes orden ν_μ er den samme for alle punkter i klassen, idet de pågældende undergrupper er indbyrdes konjugerede (øv.8). Heraf kan man slutte, at $n_\mu \nu_\mu = N$ og

$$2(N - 1) = \sum_{\mu=1}^{m} n_\mu(\nu_\mu - 1),$$

hvilket giver

$$2(1 - \frac{1}{N}) = \sum_{\mu=1}^{m}(1 - \frac{1}{\nu_\mu}).$$

Da $N \in \dot{\mathbb{N}}$ og $\nu_\mu \in \dot{\mathbb{N}}$, kommer kun værdierne $m = 2$ og $m = 3$ i betragtning. For hvert $N > 1$ kan talsættene (ν_1,ν_2) eller (ν_1,ν_2,ν_3), som tilfredsstiller ligningen, bestemmes, og det kan vises, at de kun kan forekomme hos de ovenfor nævnte grupper.

43.* Lad $(G,\circ)$ være en endelig gruppe af isometrier af rummet, og lad H være undergruppen bestående af flytningerne i G. Alle isometrier tilhørende G har et fælles fixpunkt F(se øv.40). Med s betegnes spejlingen i punktet F. Nu skelnes mellem to tilfælde: $s \in G$ og $s \notin G$. I det første tilfælde kan den fra H forskellige sideklasse skrives $s\circ H$, og man har $G = H \cup (s\circ H)$, hvor H er en af de i øvelse 42 bestemte flytningsgruppeр. I det andet tilfælde kan sideklassen skrives $u\circ H = H\circ u$, hvor u er en uegentlig isometri i G. Da s er ombyttelig med hver isometri med fixpunkt F (vis dette), vil mængden $G' = H \cup (s\circ u\circ H)$ af flytninger være en gruppe, altså en af de i øvelse 42 bestemte. Den forelagte gruppe G kan altså fås ved i en af disse grupper med en undergruppe H af

index 2 at erstatte den fra H forskellige sideklasse g∘H med s∘g∘H. Disse resultater tillader at bestemme samtlige endelige grupper af isometrier af rummet.

Øvelser til Algebraens grundbegreber, § 3.

1. Om to kompositioner + og · inden for samme mængde M er givet, at + er associativ, at hvert element af M kan bortforkortes ved +, at der findes et neutralt element e ved · , og at · er distributiv med hensyn til +. Vis, at + er kommutativ.

2. Lad $(M,+,\cdot)$ være en ring. Vis, at der for $a,b \in M$, $m,n \in \check{Z}$ gælder

$$(na)b = n(ab) = a(nb) \quad \text{og} \quad (ma)(nb) = (mn)(ab),$$

hvor potenser i gruppen $(M,+)$ er betegnet som anført side II,2,14.

3. Lad $(M,+,\cdot)$ være en ring, hvor nulreglen gælder. Det forudsættes, at M har mindst to elementer. Vis, at der for $a,b \in M \setminus \{o\}$, $n \in \check{Z}$ gælder

$$na = o \iff nb = o,$$

og begrund herved, at alle fra o forskellige elementer af M har samme orden i gruppen $(M,+)$. Den fælles orden kaldes ringens karakteristik. Vis, at hvis karakteristikken er endelig, må den være et primtal. (Benyt øv. 2.)

4. Lad $(M,+,\cdot)$ være et kommutativt legeme. For $a,b \in M$, $b \neq o$, betegnes med a/b løsningen til de ensbetydende ligninger $bx = a$ og $xb = a$. Idet også $c,d \in M$, $d \neq o$, skal man vise:

$$a/b = c/d \iff ad = bc,$$

$$a/b \pm c/d = (ad \pm bc)/(bd);$$

$$(a/b)(c/d) = (ac)/(bd),$$

samt for $c \neq o$

$$(a/b)/(c/d) = (ad)/(bc).$$

5. Lad $(G,+)$ være en kommutativ gruppe. Mængden af homomorfe afbildninger af $(G,+)$ ind i sig selv betegnes med $\mathrm{Hom}(G,G)$, og for $f,g \in \mathrm{Hom}(G,G)$ forstås ved $f + g$ afbildningen

$$t \to f(t) + g(t), \quad t \in G.$$

Vis, at $(\mathrm{Hom}(G,G),+,\circ)$ er en ring. (Den kaldes <u>ringen af endomorfier</u> af $(G,+)$.)

6. Vis, at mængden af reelle, henholdsvis komplekse polynomier med sædvanlig addition og multiplikation er en integritetsring, mængden af rationale funktioner et legeme. (En rationalfunktion er en kvotient mellem to polynomier; den er defineret overalt pånær i højst endelig mange punkter. Punkter, hvor kontinuitet kan opnås (ved "plombering"), medtages i definitionsmængden for en rational funktion såvel som for en sum og et produkt af sådanne.)

7. a) Hvor mange gruppekompositioner med o som neutralt element findes der inden for en mængde med 3 elementer o, p og q ? Opskriv kompositionstavle(r).

b) Gør rede for, at der pånær isomorfi højst findes ét legeme med 3 elementer. (Eksistens fremgår af et resultat side II,3,17.)

8. Vis, at ringen af endomorfier af $(\grave{Z},+)$ er isomorf med $(\grave{Z},+,\cdot)$. (Se øv.5 og II,1,øv.9.) Vis samme påstand, idet $\grave{Z}$ erstattes med $\grave{Q}$.

9. Gør rede for, at mængden $\grave{C}^2$ af par af komplekse tal med kompositionerne

$$(x_1,x_2) + (y_1,y_2) = (x_1+y_1, x_2+y_2),$$
$$(x_1,x_2)(y_1,y_2) = (x_1y_1-x_2y_2, x_1y_2+x_2y_1)$$

er en kommutativ ring med etelement. Bestem de elementer, der ikke er invertible ved multiplikationen. Gælder nulreglen ?

10. Bevis, at der findes en og pånær isomorfi kun en kommutativ ring $(M,+,\cdot)$, som indeholder et eksemplar $(\grave{R},+,\cdot)$ af de reelle tals legeme samt et element ε med $\varepsilon^2 = 0$, således at ethvert $x \in M$ har en og kun en fremstilling af formen

$$x = x_1 + \varepsilon x_2, \quad x_1,x_2 \in \grave{R}.$$

(Betragt passende kompositioner + og $\cdot$ inden for $\grave{R}^2$.)

Elementerne af en ring med de nævnte egenskaber kaldes <u>duale tal</u>.

11. Ved undersøgelser vedrørende reelle tal kan man tænke på et eksemplar $(\grave{R},+,\cdot)$, som på den i øv.10 beskrevne måde indgår i de duale tals ring. For et polynomium P med reelle koefficienter har da P(x) mening for ethvert dualt tal x. Vis, at

$$P(x_1 + \varepsilon x_2) = P(x_1) + \varepsilon x_2 DP(x_1),$$

hvor $x_1,x_2 \in \grave{R}$ og DP betegner den afledede af P.

12. Inden for mængden $\grave{D}(E)$ af delmængder af en mængde E defineres en komposition + ved

$$A + B = (A \cup B) \setminus (A \cap B).$$

a) Vis, at $(\grave{D}(E),+,\cap)$ er en kommutativ ring med etelement. (Benyt figurer.)

b) Hvilken egenskab ved en afbildning $f: E_1 \to E_2$ er nødvendig og tilstrækkelig for, at den tilsvarende mængdeafbildning er en homomorf afbildning af $(\grave{D}(E_1),+)$ ind i $(\grave{D}(E_2),+)$? af $(\grave{D}(E_1),\cap)$ ind i $(\grave{D}(E_2),\cap)$?

13. Vis, at der ikke findes andre endomorfe afbildninger af $(\grave{Z},+,\cdot)$ end nulfunktionen $z \to 0$, $z \in \grave{Z}$, og identiteten $z \to z$, $z \in \grave{Z}$.
Vis det tilsvarende for $(\grave{Q},+,\cdot)$, henholdsvis $(\grave{R},+,\cdot)$. (Slut i sidste tilfælde, at en endomorf afbildning må være voksende, ved at benytte, at hvert positivt tal er kvadrat på et reelt.)

14. Hvilke ækvivalensrelationer harmonerer både med additionen og med multiplikationen i et legeme ?

15. For et vilkårligt primtal p er multiplikation modulo p en gruppekomposition inden for mængden af de $p - 1$ fra $(0)_p$ forskellige restklasser modulo p. (Hvorfor ?)

Vis ved hjælp heraf Fermats "lille" sætning: For hvert helt tal a og hvert primtal p er

$$a^p \equiv a \pmod{p}.$$

16. Anvend det sidste resultat i II,2,øv. 24 på gruppen $(\dot{Z}_p \setminus \{(0)_p\}, \cdot)$, hvor p betegner et primtal, og bevis derved Wilsons sætning: For hvert primtal p er

$$(p - 1)! \equiv -1 \pmod{p}.$$

17. Vis, at restklassen $(a)_m$, hvor $m \in \dot{N}$ og $a \in \dot{Z}$, er invertibel ved multiplikationen modulo m, hvis og kun hvis a er primisk med m. (Man kan betragte den diofantiske ligning $ax + my = 1$, se II,2, øv. 17.)

18. Inden for mængden $\dot{D}(E)$ af delmængder af en mængde E defineres en komposition + ved

$$A + B = (A \cup B) \setminus (A \cap B).$$

Vis, at $(\dot{D}(E),+,\cap)$ er isomorf med ringen $(\hat{F}(E \to \dot{Z}_2),+,\cdot)$ af funktioner fra E til restklasselegemet $(\dot{Z}_2,+,\cdot)$. Beskriv mængden $A_1 + A_2 + \ldots + A_n$, hvor $A_1, A_2, \ldots, A_n$ er delmængder af E.

19. Vis, at $A = \{m + n\sqrt{3} \mid m,n \in \dot{Z}\}$ er en delring af de reelle tals legeme $(\dot{R},+,\cdot)$.

I A defineres en ækvivalensrelation ~ ved

$m + n\sqrt{3} \sim m' + n'\sqrt{3} \iff m \equiv m' \pmod 2 \ \wedge \ n \equiv n' \pmod 2$.

Vis, at ~ harmonerer med kompositionerne i ringen $(A,+,\cdot)$. Mængden $\tilde{A}$ af ækvivalensklasser organiseres da som en ring $(\tilde{A},\tilde{+},\tilde{\cdot})$ ved regning med repræsentanter.

Angiv antallet af ækvivalensklasser samt en mængde bestående af én repræsentant for hver klasse. Opskriv kompositionstavle for $(\tilde{A},\tilde{\cdot})$. Er $(\tilde{A},\tilde{+},\tilde{\cdot})$ en integritetsring ?

20. Idet m og k er naturlige tal og A en restklasse modulo m, skal man vise, at mængden $\{ka \mid a \in A\}$ er en restklasse modulo km.

Idet nu m er et givet naturligt tal, skal man undersøge, for hvilke $k \in \mathbb{N}$ afbildningen $f: \dot{Z}_m \to \dot{Z}_{km}$ bestemt ved

$$(x)_m \to (kx)_{km}, \quad x \in \dot{Z},$$

er en homomorf afbildning af restklasseringen $(\dot{Z}_m,+,\cdot)$ ind i restklasseringen $(\dot{Z}_{km},+,\cdot)$.

Vis som en anvendelse, at restklasseringen $(\dot{Z}_{12},+,\cdot)$ har et med $(\dot{Z}_3,+,\cdot)$ isomorft dellegeme.

21. Find den mindste delring L_1 af de rationale tals legeme $(\dot{Q},+,\cdot)$, som indeholder tallet $\frac{1}{10}$. Angiv endvidere de invertible elementer ved multiplikationen inden for L_1.

Find den mindste delring L_2 af $(\dot{Q},+,\cdot)$, som indeholder begge tallene $\frac{1}{5}$ og $\frac{1}{6}$. Angiv de invertible elementer ved multiplikationen inden for L_2.

Er ringene $(L_1,+,\cdot)$ og $(L_2,+,\cdot)$ isomorfe ? Er grupperne $(L_1,+)$ og $(L_2,+)$ isomorfe ?

22. Lad $(M,+,\cdot)$ være en ring med etelement e. Beskriv den mindste delring, som indeholder e, og vis, at den er isomorf med $(\dot{Z},+,\cdot)$ eller med en restklassering $(\dot{Z}_n,+,\cdot)$, $n \in \mathbb{N}$.

Det forudsættes nu, at $(M,+,\cdot)$ er en integritetsring. Vis, at en delring da og kun da er en integritetsring, når den indeholder e, og begrund derved, at $(M,+,\cdot)$ har en mindste delintegritetsring, isomorf med $(\dot{Z},+,\cdot)$ eller med restklasselegemet $(\dot{Z}_p,+,\cdot)$ modulo et primtal p.

Endelig forudsættes, at $(M,+,\cdot)$ er et kommutativt legeme.

Vis, at det mindste dellegeme er isomorft med $(\grave{Q},+,\cdot)$ eller med restklasselegemet $(\grave{Z}_p,+,\cdot)$ modulo et primtal p.

23. Gør rede for, at der pånær isomorfi kun findes én ring med etelement, hvor antallet af elementer i ringen er et givet primtal p.

24. En integritetsring, der ikke har nogen ægte delintegritetsring, kaldes en primintegritetsring. Et kommutativt legeme, der ikke har noget ægte dellegeme, kaldes et primlegeme.
Gør rede for, at der blandt delringene i en vilkårlig integritetsring er netop én primintegritetsring, blandt dellegemerne i et vilkårligt kommutativt legeme netop ét primlegeme.
Vis, at enhver primintegritetsring er isomorf med $(\grave{Z},+,\cdot)$ eller med restklasselegemet $(\grave{Z}_p,+,\cdot)$ modulo et primtal p.
Vis, at ethvert primlegeme er isomorft med $(\grave{Q},+,\cdot)$ eller med restklasselegemet $(\grave{Z}_p,+,\cdot)$ modulo et primtal p. (Benyt øv.22.)

25. Lad $L \subsetneq \grave{C}$ være et tallegeme og $s \in \grave{C}$ et tal, hvor $s \notin L$, men $s^2 \in L$. Det mindste tallegeme indeholdende L og s betegnes L(s). Vis, at

$$L(s) = \{x + ys \mid x,y \in L\},$$

og at afbildningen $(x,y) \to x + ys$, $x,y \in L$, er en bijektiv afbildning af L^2 på L(s). Vis videre, at der ved

$$x + ys \to x - ys, \quad x,y \in L,$$

defineres en automorf afbildning af $(L(s),+,\cdot)$.

Eksempler: $\grave{R}(i) = \grave{C}$, $\grave{Q}(\sqrt{2})$.

Findes der et $s \notin \dot{Q}$ med $s^2 \in \dot{Q}$, så $\dot{Q}(s) = \dot{R}$? Findes der en følge af tallegemer $L_1, L_2, \ldots$ og en følge af tal $s_1, s_2, \ldots$, hvor $s_n \notin L_n$, $s_n^2 \in L_n$ og $L_n(s_n) = L_{n+1}$, $n = 1,2,\ldots$, således at $L_1 = \dot{Q}$ og $\bigcup_{n=1}^{\infty} L_n = \dot{R}$?

26. Vis, at tallegemer $(\dot{Q}(s),+,\cdot)$ og $(\dot{Q}(t),+,\cdot)$, hvor $s,t \notin \dot{Q}$, men $s^2, t^2 \in \dot{Q}$, kun er isomorfe hvis $\frac{s}{t} \in \dot{Q}$, - i hvilket tilfælde jo $\dot{Q}(s) = \dot{Q}(t)$. (Se øv.25.)

§ 1. De naturlige tal.

Mængden af de naturlige tal kan efter R. Dedekind (Was sind und was sollen die Zahlen?, 1887) og G. Peano (Arithmetices principia nova methodo exposita, 1889) karakteriseres ved nogle få egenskaber. De grundbegreber, ved hjælp af hvilke disse egenskaber formuleres, er "mængde", "element af en mængde", "delmængde af en mængde" og "afbildning". Idet en afbildning er en speciel relation og en sådan defineres ved hjælp af begreberne "mængdeprodukt" og "delmængde", kan man i listen af grundbegreber erstatte "afbildning" med "mængdeprodukt". Dedekinds og Peanos aksiomer for de naturlige tal gengiver i eksakt formulering disses mest primitive egenskaber som ordenstal, nemlig at der efter hvert naturligt tal følger et bestemt andet, og at man kan komme til hvert naturligt tal ved at begynde med tallet 1, tage det derpå følgende, dernæst det på dette følgende o.s.v. Med de i disse noter brugte logiske tegn kan Peanos aksiomer i det væsentlige gengives således:

Forklaringer.

N betegner mængden af naturlige tal.

1 betegner enheden.

a+1 betegner efterfølgeren af a eller a plus 1.

$=$ betegner lighed.

Aksiomer.

1. $1 \in N$.
2. $\forall a \in N : a = a$.
3. $\forall a,b \in N : a = b \iff b = a$.
4. $\forall a,b,c \in N : (a = b \wedge b = c) \Rightarrow a = c$.
5. $\forall b \in N : a = b \Rightarrow a \in N$.

6. $\forall a \in N : a+1 \in N$.

7. $\forall a,b \in N : a = b \iff a+1 = b+1$.

8. $\forall a \in N : a+1 \neq 1$.

9. Hvis k betegner en mængde:

$\{1 \in k \wedge \forall x [x \in N \wedge x \in k \Rightarrow x+1 \in k]\} \Rightarrow N \subseteq k$.

"Forklaringerne" må ikke opfattes som definitioner. De tjener udelukkende til at fremkalde de rette associationer. De pågældende begreber "defineres implicit" ved, at de skal opfylde de i aksiomerne formulerede krav. Aksiomerne 2-5 fastlægger brugen af lighedstegnet. Med benyttelse af afbildningsbegrebet kan de resterende fem aksiomer erstattes af de nedenfor formulerede, som er ensbetydende med Dedekinds aksiomer, og som vil danne grundlaget for det følgende.

Om et par bestående af en ikke tom mængde N og en afbildning $\varepsilon : N \to N$ forudsættes:

I. Der findes et element $1 \in N$, således at $1 \notin \varepsilon(N)$.

II. Afbildningen ε er injektiv (enentydig).

III. Hvis det for en mængde $M \subseteq N$ gælder, at $1 \in M$ og $\varepsilon(M) \subseteq M$, så er $M = N$.

Billedelementet $\varepsilon(x)$ af et element $x \in N$ kaldes efterfølgeren af x og betegnes også med x'.

Det skal vises, at hvis disse krav er opfyldt, kan der i N defineres en kompositionsforskrift +, som har additionens velkendte egenskaber, og således at $\varepsilon(x) = x+1$. Det vil endvidere blive vist, at to par (N,ε) og (N^*,ε^*), som begge opfylder I-III, er isomorfe i den forstand, at der findes en enentydig korrespondance mellem N og N^*, således at $x \longleftrightarrow x^*$, $x \in N$, $x^* \in N^*$ medfører, at $\varepsilon(x) \longleftrightarrow \varepsilon^*(x^*)$. Spørgsmålet om eksistensen af et sådant par og det dermed sammenhængende om aksiomsystemets modsigelsesfrihed, kan ikke diskuteres på det valgte grundlag.

Man må nøjes med at konstatere, at man jo tilskriver mængden af naturlige tal de i aksiomerne udtrykte egenskaber.

Sætning 1. $\varepsilon(N) = N \setminus \{1\}$.

Bevis: Sæt $M = \varepsilon(N) \cup \{1\} \subseteq N$. Da gælder $1 \in M$, og hvis $x \in M$, så $\varepsilon(x) \in \varepsilon(N) \subseteq M$, altså $\varepsilon(M) \subseteq M$. Af III sluttes, at $M = N$, og heraf påstanden.

Sætning 2. $\forall x \in N : \varepsilon(x) \neq x$.

Bevis: Sæt $M = \{x \in N \mid \varepsilon(x) \neq x\}$. Da gælder $1 \in M$, idet $\varepsilon(1) \neq 1$ ifølge I. Hvis $x \in M$, altså $\varepsilon(x) \neq x$, fås af II, at $\varepsilon(\varepsilon(x)) \neq \varepsilon(x)$, altså $\varepsilon(x) \in M$. Dette viser, at $\varepsilon(M) \subseteq M$. Af III sluttes, at $M = N$.

Sætning 3. For hvert $a \in N$ eksisterer der en og kun een afbildning $\alpha_a : N \to N$, således at

(1) $$\alpha_a(1) = \varepsilon(a),$$

(2) $$\alpha_a \circ \varepsilon = \varepsilon \circ \alpha_a.$$

For disse afbildninger gælder

(3) $$\alpha_1 = \varepsilon,$$

(4) $$\alpha_{\varepsilon(a)} = \varepsilon \circ \alpha_a.$$

Bevis: Antag, at afbildningerne α_a og α_a^* for et givet $a \in N$ opfylder (1) og (2). Sæt

$$M = \{x \in N \mid \alpha_a(x) = \alpha_a^*(x)\}.$$

Da gælder $1 \in M$; thi ifølge (1) er $\alpha_a(1) = \alpha_a^*(1) = \varepsilon(a)$. Hvis $x \in M$, altså $\alpha_a(x) = \alpha_a^*(x)$, fås ved hjælp af (2) anvendt på α_a og α_a^*, at

$$\alpha_a(\varepsilon(x)) = \varepsilon(\alpha_a(x)) = \varepsilon(\alpha_a^*(x)) = \alpha_a^*(\varepsilon(x)),$$

altså $\varepsilon(x) \in M$. Dette viser, at $\varepsilon(M) \subseteq M$. Af III sluttes, at $M = N$. Dermed er bevist, at der højst kan findes een afbildning af den forlangte art.

Lad L betegne mængden af de elementer $a \in N$, for hvilke

Findes der et $s \notin \dot{Q}$ med $s^2 \in \dot{Q}$, så $\dot{Q}(s) = \dot{R}$? Findes der en følge af tallegemer $L_1, L_2, \ldots$ og en følge af tal $s_1, s_2, \ldots$, hvor $s_n \notin L_n$, $s_n^2 \in L_n$ og $L_n(s_n) = L_{n+1}$, $n = 1,2,\ldots$, således at $L_1 = \dot{Q}$ og $\bigcup_{n=1}^{\infty} L_n = \dot{R}$?

26. Vis, at tallegemer $(\dot{Q}(s),+,\cdot)$ og $(\dot{Q}(t),+,\cdot)$, hvor $s,t \notin \dot{Q}$, men $s^2, t^2 \in \dot{Q}$, kun er isomorfe hvis $\frac{s}{t} \in \dot{Q}$, - i hvilket tilfælde jo $\dot{Q}(s) = \dot{Q}(t)$. (Se øv.25.)

der eksisterer en afbildning $\alpha_a: N \to N$, som tilfredsstiller (1) og (2). Da gælder $1 \in M$; thi for den ved $\alpha_1 = \varepsilon$ (altså (3)) definerede afbildning er (1) og (2) øjensynlig opfyldt. Hvis $a \in L$, hvis der altså findes en afbildning α_a, for hvilken (1) og (2) gælder, vil den ved

$$\alpha_{\varepsilon(a)} = \varepsilon \circ \alpha_a$$

(altså ved (4)) definerede afbildning ligeledes opfylde (1) og (2); thi

$$\alpha_{\varepsilon(a)}(1) = \varepsilon(\alpha_a(1)) = \varepsilon(\varepsilon(a)),$$

$$\alpha_{\varepsilon(a)} \circ \varepsilon = (\varepsilon \circ \alpha_a) \circ \varepsilon = \varepsilon \circ (\alpha_a \circ \varepsilon) = \varepsilon \circ (\varepsilon \circ \alpha_a) = \varepsilon \circ \alpha_{\varepsilon(a)}.$$

Dette viser, at $\varepsilon(L) \subseteq L$. Af III sluttes, at $L = N$. Dermed er sætning 3 bevist, idet (3) og (4) gælder ifølge de opstillede definitioner.

Definition. I N defineres en kompositionsforskrift, betegnet som addition, ved

$$x+a = \alpha_a(x).$$

Man har da specielt ifølge (3)

(5) $\quad \forall a \in N : \alpha_1(a) = \varepsilon(a) = a+1,$

og (1), (2) og (4) kan skrives

(6) $\quad \forall a \in N : 1+a = a+1,$

(7) $\quad \forall a,x \in N : (x+1)+a = (x+a)+1.$

(8) $\quad \forall a,x \in N : x+(a+1) = (x+a)+1.$

Sætning 4. $\forall a,x \in N : x+a = a+x.$

Bevis: For et fast $a \in N$ sættes

$$M = \{x \in N \mid x+a = a+x\}.$$

Da gælder $1 \in M$ på grund af (6), og hvis $x \in M$, altså $x+a = a+x$, fås ved hjælp af (7) og (8)

$$(x+1)+a = (x+a)+1 = (a+x)+1 = a+(x+1),$$

altså $x+1 = \varepsilon(x) \in M$. Følgelig er $\varepsilon(M) \subseteq M$, altså $M = N$ ifølge III.

Sætning 5. $\forall a,b,x \in N : x+(a+b) = (x+a)+b$.

Bevis: For faste $a,x \in N$ sættes

$$M = \{b \in N \mid x+(a+b) = (x+a)+b\}.$$

Da gælder $1 \in M$ ifølge (8). Hvis $b \in M$, fås ved hjælp af (8), (8), $b \in M$ og (8).

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

altså $b+1 = \varepsilon(b) \in M$. Dette viser, at $\varepsilon(M) \subseteq M$, hvoraf $M = N$ ifølge III.

Sætning 6. $\forall a,x,y \in N : x+a = y+a \Rightarrow x = y$.

For givne $a,b \in N$ har ligningen $x+a = b$ altså højst een løsning $x \in N$.

Bevis: Sæt

$$M = \{a \in N \mid \forall x,y \in N : x+a = y+a \Rightarrow x = y\}.$$

Da gælder $1 \in M$ ifølge (5) og II. Ved hjælp af sætning 5 sluttes af $x+(a+1) = y+(a+1)$, at $(x+a)+1 = (y+a)+1$, og heraf ved hjælp af II, at $x+a = y+a$. Hvis $a \in M$, kan heraf sluttes, at $x = y$, altså at da også $a+1 = \varepsilon(a) \in M$. Man har altså $\varepsilon(M) \subseteq M$ og derfor $M = N$ ifølge III.

Sætning 7. $\forall a,x \in N : x+a \neq x$.

Bevis: For et fast $a \in N$ sættes $M = \{x \in N \mid x+a = x\}$. Da gælder $1 \in M$ ifølge (5) og sætning 2. Hvis $x \in M$, fås ved hjælp af (7) og II, at

$$(x+1)+a = (x+a)+1 \neq x+1,$$

altså at $x+1 = \varepsilon(x) \in M$. Dette viser, at $\varepsilon(M) \subseteq M$, og dermed $M = N$ ifølge III.

Sætning 8. For givne $a,b \in N$, $a \neq b$, har en og kun een af ligningerne $x+a = b$ og $y+b = a$ en løsning henholdsvis $x \in N$ og $y \in N$.

Bevis: For fast $a \in N$ sættes

$M = \{b \in N \mid a = b \vee (\exists x \in N : x+a = b) \vee (\exists y \in N : y+b = a)\}$.

Da gælder $1 \in M$. Dette er klart, hvis $a = 1$, og hvis $a \neq 1$, findes der ifølge (5) og sætning 1 et $x \in N$, således at $x+1 = a$.

Det antages nu, at $b \in M$. Der foreligger da tre muligheder:

1° $a = b$. Da er $1+a = a+1 = b+1$, og ligningen $x+a = b+1$ har løsningen $x = 1$, altså $b+1 \in M$.

2° $\exists x \in N : x+a = b$. Da er $(x+1)+a = (x+a)+1 = b+1$, hvilket viser, at $b+1 \in M$.

3° $\exists y \in N : y+b = a$. Er $y = 1$, altså $a = b+1$, fås $b+1 \in M$. Er $y = 1$, finde der ifølge sætning 1 et $z \in N$, således at $\varepsilon(z) = z+1 = y$. Man har da

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

altså også i dette tilfælde $b+1 \in M$.

Dermed er vist, at $\varepsilon(M) \subseteq M$, hvoraf $M = N$ ifølge III. For $a \neq b$ har altså mindst een af de to ligninger en løsning.

At ikke såvel $x+a = b$ som $y+b = a$ kan have en løsning, følger af at

$$(y+\ )+a = y+(x+a) = y+b = a$$

ville stride mod sætning 7.

Tilsvarende sætninger vedrørende multiplikation anføres uden bevis.

Sætning 9. For hvert $a \in N$ eksisterer der en og kun een afbildning $\mu_a : N \to N$, således at

(9) $$\mu_a(1) = a,$$

(10) $$\forall x \in N : \mu_a(x+1) = \mu_a(x) + a.$$

For disse afbildninger gælder

(11) $$\forall x \in N : \mu_1(x) = x,$$

(12) $$\forall x \in N : \mu_{a+1}(x) = \mu_a(x) + x.$$

Definition. I N defineres en kompositionsforskrift, betegnet som multiplikation, ved

$$xa = \mu_a(x).$$

Ligningerne (9)-(12) kan da skrives

(13) $1a = a$

(14) $(x+1)a = xa+a,$

(15) $x1 = x,$

(16) $x(a+1) = xa+x.$

Sætning 10. $\forall a,x,y \in N : (x+y)a = xa+ya.$

Sætning 11. $\forall a,x \in N : xa = ax.$

Sætning 12. $\forall a,b,x \in N : x(ab) = (xa)b.$

Sætning 13. $\forall a,x,y \in N : xa = ya \Rightarrow x = y.$

Definition. I N defineres en relation, betegnet med $<$, ved

$$a < b \iff \exists x \in N : x+a = b.$$

Sætning 14. Relationen $<$ er en ikke-refleksiv, total ordningsrelation.

Bevis: At $a \nless a$, følger af sætning 7. Af $a < b$ og $b < c$, altså af eksistensen af $x,y \in N$, således at $x+a = b$ og $y+b = c$, følger

$$(y+x)+a = y+(x+a) = y+b = c,$$

altså $a < c$. Sætning 8 viser, at der for $a \neq b$ enten gælder $a < b$ eller $b < a$.

Den til $<$ inverse relation $>$, som ligeledes er en ikke-refleksiv, total ordningsrelation, defineres ved

$$a > b \iff b < a,$$

og de tilhørende refleksive ordningsrelationer er bestemt ved

$$a \leqq b \iff (a < b \vee a = b) \iff a \ngtr b,$$

$$a \geqq b \iff (a > b \vee a = b) \iff a \nless b.$$

Sætning 15. $\forall\, a,b \in N : a < a+b$,

Bevis: $b+a = a+b$.

Sætning 16. $\forall\, a,b,c \in N : a < b \iff a+c < b+c$.

Bevis: $\Rightarrow$ Af $x+a = b$ følger

$$x+(a+c) = (x+a)+c = b+c.$$

$\Leftarrow$ Af $b \leqq a$ ville man ifølge det allerede viste kunne slutte, at $b+c \leqq a+c$, hvilket strider mod det givne.

Sætning 17. $\forall\, a,b,c \in N : a < b \iff ac < bc$.

Bevis: $\Rightarrow$ Af $x+a = b$ følger

$$xc + ac = (x+a)c = bc.$$

$\Leftarrow$ Af $b \leqq a$ ville man ifølge det allerede viste kunne slutte, at $bc \leqq ac$, hvilket strider mod det givne.

Den indførte ordningsrelation i N har foruden de nævnte egenskaber (som f.eks. den sædvanlige ordning i mængden af positive rationale tal også har) visse særlige, for de naturlige tals ordning karakteristiske egenskaber. For nemt at kunne formulere disse, anføres nogle definitioner og sætninger vedrørende ordnede mængder.

Lad $(M,\leqq)$ være en mængde, hvori der er defineret en refleksiv, ikke nødvendigvis total ordningsrelation. Et element a i en ordnet mængde M siges at være dens første element, hvis $a \leqq x$ for alle $x \in M$. Det er klart, at hvis der overhovedet findes et sådant element, er det entydig bestemt, idet $a \leqq a'$ og $a' \leqq a$ medfører $a = a'$. Tilsvarende defineres sidste element. Idet ordningsrelationens restriktion til en delmængde er en ordningsrelation i denne, overføres disse definitioner umiddelbart til delmængder af $(M,\leqq)$.

En delmængde M' af en ordnet mængde M siges at være nedad (opad) begrænset, hvis den har en minorant (majorant), hvormed

menes et element $m \in M$, for hvilket $m \preceq x$ $(x \preceq m)$ for alle $x \in M'$.

En mængde M siges at være velordnet ved en ordningsrelation $\preceq$, hvis hver ikke tom delmængde, ordnet ved relationens restriktion til den, har et første element. (Dette medfører, at ordningsrelationen er total; thi da delmængden $\{x,y\}$ bestående af to forskellige elementer har et første, må der gælde $x \prec y$ eller $y \prec x$.)

Det er klart, at hver delmængde af en velordnet mængde er velordnet ved ordningsrelationens restriktion til den.

Sætning a. I en velordnet mængde $(M,\preceq)$ findes der til hvert element x, som ikke er sidste element, et (og selvfølgelig kun eet) umiddelbart følgende, d.v.s. et element x', således at $x \prec x'$ og at $x \prec y$ medfører $x' \preceq y$.

Bevis: Da $x \in M$ ikke er sidste element, er mængden $\{y \in M \mid x \prec y\}$ ikke tom. Den har altså et første element x', og dette opfylder de stillede krav.

Sætning b (Transfinit induktion). Hvis det for en delmængde $(M', \preceq)$ af en velordnet mængde $(M, \preceq)$ gælder, at

$$\forall a \in M : M_a \subseteq M' \Rightarrow a \in M',$$

hvor $M_a = \{x \in M \mid x \prec a\}$ er det ved a bestemte "afsnit" af M, så er $M' = M$.

Bevis: Hvis delmængden $M \setminus M'$ af M ikke var tom, ville den have et første element a, og for dette havde man $x \in M'$ for $x \prec a$, altså $M_a \subseteq M'$. Ifølge forudsætningen ville dette medføre $a \in M'$ i strid med $a \in M \setminus M'$.

(Bemærk, at den indirekte slutning også er gyldig, hvis $M \setminus M'$ indeholdt det første element af M, som så ville være det betragtede element a. Man havde da $M_a = \emptyset$. Men da $\emptyset \subseteq M'$, ville forudsætningen også i dette tilfælde medføre $a \in M'$.)

Nu betragtes igen parret (N,ε) bestående af en mængde N og en afbildning $\varepsilon: N \to N$, som opfylder aksiomerne I-III.

Sætning 18. $\forall x \in N : 1 \leqq x$,

d.v.s., N har 1 som første element.

Bevis: Ifølge sætning 1 findes der for hvert $x \neq 1$ et $z \in N$, således at $\varepsilon(z) = z+1 = x$. Dette viser, at $1 < x$.

Sætning 19. $\forall x,y \in N : x < y \Rightarrow x+1 \leqq y$,

d.v.s., hvert element $x \in N$ har et umiddelbart følgende, nemlig $x+1$.

Bevis: Idet $x < y$, findes der et $z \in N$, således at $z+x = y$. Ifølge sætning 18 er $1 \leqq z$, altså $x+1 = 1+x \leqq z+x = y$ ifølge sætning 16.

Sætning 20. Mængden N er velordnet ved relationen $\leqq$.

Bevis: Lad M være en ikke tom delmængde af N, og lad L være mængden af alle minoranter for M, altså

$$L = \{y \in N \mid \forall x \in M \mid y \leqq x\}.$$

Da er $1 \in L$, altså $L \neq \emptyset$ ifølge sætning 18. Mængden $N \setminus L$ er heller ikke tom; thi for et element $x \in M$ vil $x+1 \notin L$, da $x < x+1$. Der findes derfor et element $a \in L$, for hvilket $a+1 \notin L$, da ellers $L = N$ ifølge aksiom III. Dette element a påstås at være første element i M. Idet a som element af L er en minorant for M, er det tilstrækkeligt at vise, at $a \in M$. Var $a \notin M$, ville man ifølge definition af L, have at $a < x$ for alle $x \in M$. Ifølge sætning 19 ville dette imidlertid medføre, at $a+1 \leqq x$ for alle $x \in M$, altså at $a+1 \in L$, i strid med bestemmelsen af a. Dermed er vist, at hver delmængde af M har et første element.

Herefter ses af sætning b, at følgende fra III forskellige induktionsslutning er gyldig i N:

Sætning 21. Hvis det for en delmængde M af N gælder, at

$\varepsilon(x) \underline{\prec} y$, da $\varepsilon(x)$ følger umiddelbart efter x. Endvidere gælder $y \prec \varepsilon(y)$. Transitiviteten af $\prec$ giver da $\varepsilon(x) \prec \varepsilon(y)$. Afbildningen ε er altså ordenstro for den ikke-refleksive relation $\prec$, altså specielt injektiv. Dermed er gyldigheden af aksiom II bevist. For at bevise III betragtes en mængde $M \subseteq N$, for hvilken $1 \in M$ og $\varepsilon(M) \subseteq M$. Antag, at mængden $N \setminus M$ ikke er tom. Den har da et første element b. Mængden $N_b = \{x \in N \mid x \prec b\}$ er en opad begrænset delmængde af M. Den er ikke tom, da $1 \in M$, og har følgelig et sidste element a. Ifølge det om M forudsatte gælder $\varepsilon(a) \in M$. Da $a \prec b$ og $\varepsilon(a)$ følger umiddelbart efter a, har man $\varepsilon(a) \underline{\prec} b$. Da a er det sidste element før b, har man $b \underline{\prec} \varepsilon(a)$, altså $b = \varepsilon(a) \in M$. Men dette strider mod, at $b \in N \setminus M$. Dermed er også III bevist.

For endelig at vise, at den ved ε bestemte ordningsrelation $\leqq$ stemmer overens med den givne $\underline{\prec}$, behøver man blot at bemærke, at 1 er første element af N ved begge ordninger, og at $\varepsilon(x)$ er det umiddelbart efter x følgende element, ved $\prec$ ifølge definition af ε, ved $<$ ifølge sætning 19. For $a \in N$ betragtes de to mængder

$$N_{-<a} = \{x \in N \mid x \prec a\}, \qquad N_{<a} = \{x \in N \mid x < a\}.$$

Påstanden går ud på, at de stemmer overens for hvert a. Lad $M \subseteq N$ være mængden af de $a \in N$, for hvilke $N_{-<a} = N_{<a}$. For $a = 1$ er begge mængder tomme, altså $1 \in M$. Idet

$$N_{-<\varepsilon(a)} = N_{-<a} \cup \{a\}, \qquad N_{<\varepsilon(a)} = N_{<a} \cup \{a\},$$

kan man af $N_{-<a} = N_{<a}$ slutte, at $N_{-<\varepsilon(a)} = N_{<\varepsilon(a)}$. Dette viser, at $\varepsilon(M) \subseteq M$, og anvendelsen af III giver $M = N$, hvilket skulle vises.

$$\forall a \in N : N_a \subseteq M \Rightarrow a \in M,$$

hvor $N_a = \{x \in N \mid x < a\}$, så er $M = N$.

Sætning 22. Hver ikke tom opad begrænset delmængde L af N har et sidste element.

Bevis: Sæt $M = \{y \in N \mid \forall x \in L : x \leq y\}$. Da er $M \neq \emptyset$, idet L er opad begrænset. Lad b være det første element i M. Da b ifølge definition af M er en majorant til L, drejer det sig kun om at vise, at $b \in L$. Hvis $b = 1$, må L være $\{1\}$, da $L \neq \emptyset$, og påstanden er indlysende. Hvis $1 < b$, findes der ifølge sætning 8 (eller 1) et $c \in N$, således at $c+1 = b$. For dette gælder $c \notin M$, idet $c < b$. Der eksisterer altså et $d \in L$, således at $c < d$. Af sætning 19 kan da sluttes, at $c+1 = b \leq d$. Men $b < d$ er udelukket, da $b \in M$ og $d \in L$. Følgelig har man $b = d \in L$ som påstået.

Sætning 23. Nødvendige og tilstrækkelige betingelser for, at en ordnet mængde $(N, \prec)$ tillader en afbildning $\varepsilon: N \to N$, således at aksiomerne I-III er opfyldt og den ved ε bestemte ordning $\leq$ stemmer overens med $\prec$, er at $(N, \prec)$ er velordnet ved $\prec$ og ikke har noget sidste element, og at hver ikke tom, opad begrænset delmængde af N har et sidste element.

Bevis: At betingelserne er nødvendige, viser sætningerne 20,15,22.

Tilstrækkeligheden indses på følgende måde. Idet det forudsættes, at $(N, \prec)$ ikke har noget sidste element og er velordnet, sluttes af sætning a, at hvert element $x \in N$ har et umiddelbart følgende x'. Ved $\varepsilon(x) = x'$ defineres en afbildning $\varepsilon: N \to N$. Betegnes det første element i N med 1, har man $1 \prec \varepsilon(x)$. Aksiom I er altså opfyldt. Er x og y to forskellige elementer af N, vil der gælde $x \prec y$ eller $y \prec x$, da $\prec$ er total. Antag, at betegnelserne er valgt således, at $x \prec y$. Man har da

Man lægger mærke til, at forudsætningen om, at hver opad begrænset delmængde af N har et sidste element, i beviset for betingelsernes tilstrækkelighed kun blev anvendt på afsnittene $N_b = \{x \in N \mid x \prec b\}$, $b \neq 1$. At N_b har et sidste element, er ensbetydende med, at b har et umiddelbart forudgående element.

Sætning 23 viser, at Dedekinds aksiomer I-III kan erstattes med aksiomer, der vedrører en ordningsrelation i den betragtede mængde N (E. Schmidt, ca. 1920):

Om en ordnet mængde $(N,\leqq)$ forudsættes:

1. N er velordnet ved $\leqq$.
2. N har ikke noget sidste element.
3. Hvert element af N, som er forskelligt fra det første, har et umiddelbart forudgående.

Et af de grundlæggende spørgsmål, som endnu ikke er besvaret, er, om Dedekinds aksiomsystem er kategorisk, d.v.s. om det fastlægger parret (N,ε) på nær isomorfi. At dette er tilfældet, vil vise sig at være en konsekvens af nedenstående sætning 24.

Om parret (N,ε) forudsættes at aksiomerne I-III og dermed sætningerne 1-23 er opfyldt. Det element, der går umiddelbart forud for et element $a \neq 1$ af N, betegnes med a-1. Med N_a betegnes som hidtil det ved a bestemte afsnit $\{x \in N \mid x < a\}$.

Sætning 24. Lad der være givet en mængde Ω, et element $\alpha \in \Omega$ og en afbildning $\varphi : \Omega \to \Omega$.

For hvert $p \in N$ eksisterer da en og kun een afbildning $f_p : N_{p+1} \to \Omega$, således at

$$f_p(1) = \alpha, \quad f_p(i+1) = \varphi(f_p(i)) \qquad \text{for } i \in N_p.$$

Der eksisterer en og kun een afbildning $f : N \to \Omega$, således at

$$f(1) = \alpha, \quad f(i+1) = \varphi(f(i)) \qquad \text{for } i \in N.$$

Bevis: Først vises, at der for et givet $p \in N$ højst kan findes een afbildning med de forlangte egenskaber. Lad f_p og g_p have dem. Da er $f_p(1) = \alpha = g_p(1)$. Antag, at $f_p(i) = g_p(i)$ for $i \in N_a$, hvor $a \in N_{p+1}$. Da er

$$f_p(a) = \varphi(f_p(a-1)) = \varphi(g_p(a-1)) = g_p(a).$$

Sætning b kan altså anvendes på den velordnede mængde N_{p+1} som mængden M og med mængden $\{i \in N_{p+1} \mid f_p(i) = g_p(i)\}$ som delmængden M'.

Lad nu L betegne mængden af de elementer $p \in N$, for hvilke der eksisterer afbildninger f_p af den forlangte art. Det er klart, at $1 \in L$, idet $f_1(1) = \alpha$ opfylder det første krav, og det andet falder bort. Antag, at der eksisterer en afbildning $f_p: N_{p+1} \to \Omega$, således at $f_p(1) = \alpha$ og $f_p(i+1) = \varphi(f_p(i))$ for $i \in N_p$. Afbildningen $f_{p+1}: N_{(p+1)+1} \to \Omega$ bestemt ved

$$f_{p+1}(i) = f_p(i) \qquad \text{for } i \in N_{p+1},$$
$$f_{p+1}(p+1) = \varphi(f_p(p))$$

opfylder da øjensynlig kravene med p+1 i stedet for p. Påstanden følger altså af aksiom III.

For $p < q$ vil restriktionen af f_q til N_{p+1} opfylde de til f_p stillede krav. På grund af entydigheden af f_p har man altså $f_q(i) = f_p(i)$ for $i \in N_{p+1}$. Sættes $f(i) = f_i(i)$ for $i \in N$, fås en afbildning af N ind i Ω, for hvilken $f(1) = f_1(1) = \alpha$ og

$$f(i+1) = f_{i+1}(i+1) = \varphi(f_{i+1}(i)) = \varphi(f_i(i)) = \varphi(f(i)).$$

At der kun kan findes een afbildning $f: N \to \Omega$ med disse egenskaber, følger af, at dens restriktion til et afsnit N_{p+1} for hvert $p \in N$ opfylder de til f_p stillede krav og følgelig må stemme overens med f_p. Dermed er sætning 24 bevist.

Sætning 25. Lad (N,ε) og (N^*,ε^*) være to par, hvert bestående af en mængde og en afbildning af denne ind i sig selv,

således at begge par tilfredsstiller Dedekinds aksiomer I-III med henholdsvis $1 \in N$ og $1^* \in N^*$. Da er de to par isomorfe i den forstand, at der findes en (og kun een) bijektiv afbildning $f:N \to N^*$, således at $f(1) = 1^*$ og $f(\varepsilon(x)) = \varepsilon^*(f(x))$ for alle $x \in N$.

Bevis: Sætning 24 med N^* i stedet for Ω, 1^* i stedet for α og ε^* i stedet for φ giver eksistensen af en (og kun een) afbildning $f:N \to N^*$ med de sidstnævnte egenskaber. Det skal vises, at denne afbildning er bijektiv. Hertil benyttes, at der ifølge det sagte også findes en afbildning $f^*: N^* \to N$, for hvilken $f^*(1^*) = 1$ og $f^*(\varepsilon^*(x)) = \varepsilon(f^*(x^*))$. Den sammensatte afbildning $f^* \circ f$ er den identiske afbildning af N. Mængden

$$M = \{x \in N \mid f^*(f(x)) = x\} \subseteq N$$

opfylder nemlig forudsætningerne af III; thi $f^*(f(1)) = f^*(1^*) = 1$, og hvis $f^*(f(x)) = x$, har man

$$f^*(f(\varepsilon(x))) = f^*(\varepsilon^*(f(x))) = \varepsilon(f^*(f(x))) = \varepsilon(x).$$

Af $f^*(f(x)) = x$ for alle $x \in N$ følger, at f er injektiv; thi af $f(x) = f(y)$ følger

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

Endvidere ses, at f^* er surjektiv. Men da f og f^* kan bytte rolle, må f også være surjektiv. Dermed er sætningen bevist.

Herefter er der mening i følgende definition:

Ved mængden $\mathbb{N}$ af naturlige tal forstås en mængde N organiseret ved en afbildning $\varepsilon:N \to N$, som opfylder Dedekinds aksiomer I-III.

Det følgende går ud på ud fra det valgte grundlag at gøre rede for de naturlige tals brugbarhed som kardinaltal for endelige mængder.

Sætning 26. Hvis der for to naturlige tal a og b eksisterer en injektiv afbildning f af afsnittet $\mathbb{N}_{a+1}$ ind i afsnittet $\mathbb{N}_{b+1}$, så er $a \leqq b$.

Bevis: Lad M betegne mængden af de $a \in \mathbb{N}$, for hvilke påstanden er rigtig for alle $b \in \mathbb{N}$. Det er klart, at $1 \in M$, idet $1 \leqq b$ for alle b. Antag, at $a \in M$, og lad f være en injektiv afbildning af $\mathbb{N}_{(a+1)+1}$ ind i et afsnit $\mathbb{N}_{b+1}$. Det skal vises, at $a+1 \leqq b$. Der skelnes mellem tre tilfælde:

1° $\quad b \notin f(\mathbb{N}_{(a+1)+1})$,

2° $\quad b = f(a+1)$,

3° $\quad b = f(c), \quad c \neq a+1$.

I tilfældene 1° og 2° vil restriktionen af f til $\mathbb{N}_{a+1}$ være en injektiv afbildning af $\mathbb{N}_{a+1}$ ind i $\mathbb{N}_b$. På grund af antagelsen $a \in M$ følger heraf, at $a \leqq b-1$, altså $a+1 \leqq b$. I tilfældet 3° defineres en afbildning $f' : \mathbb{N}_{(a+1)+1} \to \mathbb{N}_{b+1}$ ved

$$f'(x) = f(x) \quad \text{for } x \in \mathbb{N}_{(a+1)+1} \setminus \{c, a+1\},$$
$$f'(c) = f(a+1),$$
$$f'(a+1) = f(c) = b.$$

Denne afbildning er injektiv og falder under 2°.
Følgelig har man $a+1 \leqq b$ også i dette tilfælde. Dermed er vist, at $a+1 \in M$. Ifølge aksiom III er altså $M = \mathbb{N}$, hvilket skulle vises.

Sætning 27. Hvis en mængde A er ækvipotent såvel med afsnittet $\mathbb{N}_{a+1}$ som med afsnittet $\mathbb{N}_{b+1}$ af $\mathbb{N}$, så er $a = b$.

Bevis: Lad $\varphi : A \to \mathbb{N}_{a+1}$ og $\psi : A \to \mathbb{N}_{b+1}$ være bijektive afbildninger. Da er $f = \psi \circ \varphi^{-1}$ en bijektiv afbildning af $\mathbb{N}_{a+1}$ på $\mathbb{N}_{b+1}$

og f^{-1} en bijektiv afbildning af $\grave{N}_{b+1}$ på $\grave{N}_{a+1}$. Sætning 26 anvendt på disse to afbildninger giver $a \leqq b$ og $b \leqq a$.

Definition. En mængde A siges at være en endelig mængde, hvis den er tom eller ækvipotent med et afsnit $\grave{N}_{a+1}$ af mængden $\grave{N}$ af naturlige tal. I det sidstnævnte tilfælde er det naturlige tal a entydig bestemt (ifølge sætning 27) og kaldes antallet af elementer i A eller kardinaltallet kt A for A.

Det er klart, at hvis en af to ækvipotente mængder er endelig, er den anden det også, og de to mængder har samme kardinaltal.

Ikke endelige mængder kaldes uendelige mængder.

Sætning 28. Hver ægte delmængde B af en endelig mængde A er endelig, og hvis $B \neq \emptyset$, gælder kt B < kt A.

Bevis: Idet A er ækvipotent med et afsnit $\grave{N}_{a+1}$, hvor a = kt A, vil B være ækvipotent med en delmængde af $\grave{N}_{a+1}$. Det drejer sig altså om at vise, at hver ægte og ikke tom delmængde af $\grave{N}_{a+1}$ er ækvipotent med et afsnit $\grave{N}_{b+1}$, hvor b < a. Lad M betegne mængden af de $a \in \grave{N}$, for hvilke det gælder, at hver ægte og ikke tom delmængde af $\grave{N}_{a+1}$ er ækvipotent med et afsnit N_{b+1} med b < a. At $1 \in M$, følger af, at $\grave{N}_{1+1} = \{1\}$ ikke har sådanne delmængder. Antag, at $a \in M$, og lad $P \neq \emptyset$ være en ægte delmængde af $\grave{N}_{(a+1)+1}$. Idet mængden P har (a+1)+1 som majorant, har den et sidste element p. Hvis $P = \{p\}$, er P ækvipotent med $\grave{N}_{1+1} = \{1\}$, og kt P = 1 < a+1. Er $P\backslash\{p\}$ ikke tom, vil denne mængde ikke indeholde a+1. Altså er $P\backslash\{p\} \subsetneqq \grave{N}_{a+1}$. Her er lighed imidlertid umulig, da denne ville medføre p = a+1 og følgelig $P = \grave{N}_{(a+1)+1}$ i strid med forudsætningen om P. Ifølge induktionsantagelsen findes der en bijektiv afbildning af $P\backslash\{p\}$ på et afsnit $\grave{N}_{b+1}$ med b < a. Lader man til p svare b+1,

får man i alt en bijektiv afbildning af P på $\dot{N}_{(b+1)+1}$, og man har $b+1 < a+1$. Dermed er vist, at $a+1 \in M$. Af aksiom III sluttes, at $M = \dot{N}$. Hermed er sætningen bevist.

Sætning 29. Er A og B disjunkte endelige mængder, vil $A \cup B$ være endelig og $kt(A \cup B) = kt\ A + kt\ B$.

Bevis: Med M betegnes mængden af de $a \in \dot{N}$, for hvilke det gælder, at $\dot{N}_{b+1}$ for hvert $b \in \dot{N}$ er ækvipotent med $\dot{N}_{(a+b)+1} \setminus \dot{N}_{a+1}$. Idet der ved $x \to x+1$ defineres en bijektiv afbildning af $\dot{N}_{b+1}$ på $\dot{N}_{(b+1)+1} \setminus \dot{N}_{1+1}$, haves $1 \in M$. Antag, at $a \in M$, altså at der for hvert $b \in \dot{N}$ eksisterer en bijektiv afbildning

$$f_b : \dot{N}_{b+1} \to \dot{N}_{(a+b)+1} \setminus \dot{N}_{a+1}.$$

Ved til $x \in \dot{N}_{b+1}$ at lade svare $f_b(x)+1$, fås en bijektiv afbildning af $\dot{N}_{b+1}$ på $\dot{N}_{((a+1)+b)+1} \setminus \dot{N}_{(a+1)+1}$. Dette viser, at $a+1 \in M$. Af aksiom III kan altså sluttes, at $M = \dot{N}$. Er nu A og B disjunkte endelige mængder med kardinaltallene a og b, vil der findes en bijektiv afbildning $\varphi : A \to \dot{N}_{a+1}$ og en bijektiv afbildning $\psi : B \to \dot{N}_{b+1}$. Den sidstnævnte sammensat med afbildningen f_b, altså $f_b \circ \psi$ er da en bijektiv afbildning af B på $\dot{N}_{(a+b)+1} \setminus \dot{N}_{a+1}$. Ved til $\gamma \in A \cup B$ at lade svare $\varphi(\gamma)$, når $\gamma \in A$, og $f_b(\psi(\gamma))$, når $\gamma \in B$, fås en bijektiv afbildning af $A \cup B$ på $\dot{N}_{(a+b)+1}$. Dermed er sætningen bevist.

Uden bevis nævnes:

Sætning 30. Er A og B endelige mængder, vil $A \times B$ være endelig og $kt(A \times B) = kt\ A \cdot kt\ B$.

Øvelser til kap.II,§1.

1. Bevis, at Dedekinds aksiomer I,II,III er indbyrdes uafhængige, ved at angive mængder N og afbildninger $\varepsilon: N \to N$, således at hvilkesomhelst to af aksiomerne er opfyldte, medens det tredie ikke er det. (I det tilfælde, hvor I kræves at være falsk, skal III forstås således, at der findes et element $1 \in N$, for hvilket det i III forlangte er opfyldt.)

2. Giv beviser for sætningerne 9-13.

3. For $a < b$ betegnes løsningen x til ligningen $x+a = b$ med $b-a$. Vis, at hvis de venstre sider i de følgende relationer eksisterer, vil også de højre sider eksistere og relationerne være gyldige:

$$(b-a) + (d-c) = (b+d) - (a+c),$$

$$(b-a)c = bc-ac,$$

$$(b-a)(d-c) = (bd+ac)-(ad+bc).$$

Vis endvidere, at hvis $b-a$ og $d-c$ eksisterer, vil $b-a < d-c$ være ensbetydende med $b+c < a+d$.

4. Der er givet et element $a \in N$. Om en mængde $M \subseteq N$ forudsættes, at $a \in M$, og for hvert $x \in N$, at hvis $x \geq a$ og $x \in M$, så er $x+1 \in M$. Vis, at $M = N$.

5. Er mængderne

$$\{p + 1/q \mid p,q \in \mathbb{N}\}, \quad \{p - 1/q \mid p,q \in \mathbb{N}\}$$

af rationale tal velordnede ved den sædvanlige relation $<$? Ved $>$?

6. Lad M være velordnet ved relationen $-<$. Vis, at der for hver ordenstro afbildning $f: M \to M$ gælder $x \leqq f(x)$ for alle

$x \in M$.

Slut heraf, at den eneste surjektive ordenstro afbildning $f : M \to M$ er den identiske, og at der ikke findes nogen surjektiv ordenstro afbildning af et afsnit $M_a = \{x \in M \mid x -< a\}$ af M på M.

7. Find fejlslutningen i følgende induktions"bevis" for "sætningen": Hvilkesomhelst endelig mange indbyrdes forskellige linier i planen har et punkt fælles.

Påstanden er indlysende for 1 linie. Lad der være givet n indbyrdes forskellige linier $l_1,\ldots,l_n$. Hvis påstanden er rigtig for n-1 linier, vil såvel linierne $l_1,\ldots,l_{n-1}$ som linierne $l_1,\ldots,l_{n-2},l_n$ have et punkt fælles. Disse to punkter må falde sammen, da begge ligger på l_1 og l_2. Antagelsen medfører altså, at $l_1,\ldots,l_n$ har et punkt fælles, så at aksiom III kan anvendes.

8. Find fejlslutningen i følgende induktions"bevis" for "sætningen": For alle naturlige tal n er $|\sin n\pi/3| \leqq \frac{1}{2}$ og $|\cos n\pi/3| \leqq \frac{1}{2}$.

Lad n være et naturligt tal, og antag, at påstanden er rigtig for alle naturlige tal mindre end n. Da er

$$|\sin n\pi/3| = |\sin \pi/3 \cos(n-1)\pi/3 + \cos \pi/3 \sin(n-1)\pi/3|$$
$$\leqq \tfrac{1}{2}\cdot\tfrac{1}{2} + \tfrac{1}{2}\cdot\tfrac{1}{2} = \tfrac{1}{2},$$

og tilsvarende sluttes, at $|\cos n\pi/3| \leqq \frac{1}{2}$. Følgelig kan sætning 21 anvendes.

9. For naturlige tal p og n sættes $s_p(n) = \sum_{\nu=1}^{n} \nu^p$. Find (ved at anvende binomialformlen på $(\nu+1)^{p+1}$) $s_p(n)$ udtrykt ved $s_1(n),\ldots,s_{p-1}(n)$. Vis, at der for hvert $p \in \mathbb{N}$ eksisterer et polynomium P_{p+1} af graden p+1 og med rationale koefficienter, således at $s_p(n) = P_{p+1}(n)$.

10. Bevis sætning 30.

11.* Vis, at en mængde er endelig, hvis og kun hvis den ikke er ækvipotent med nogen af sine ægte delmængder. [Ved beviset for betingelsens tilstrækkelighed kan man begynde med at vise, at hvis en mængde er uendelig, kan hvert afsnit af $\grave{N}$ og også $\grave{N}$ selv afbildes injektivt i den. (Hver uendelig mængde har en numerabel delmængde.)]

12.* Vis, at en ikke tom mængde er endelig, hvis og kun hvis der findes en afbildning af den ind i sig selv, ved hvilken ingen ægte og ikke tom delmængde afbildes ind i sig selv. (Benyt sætning 24.)

13. Der er givet en mængde Ω med en kompositionsforskrift \$. Bevis følgende: Til hver afbildning $\alpha : \grave{N}_{p+1} \to \Omega$ findes der en og kun een afbildning $\sigma : \grave{N}_{p+1} \to \Omega$, således at $\sigma(1) = \alpha(1)$ og

$$\sigma(j+1) = \sigma(j) \,\$\, \alpha(j+1) \quad \text{for } j \in \grave{N}_p.$$

Når kompositionsforskriften er betegnet som addition eller multiplikation, skrives henholdsvis

$$\sigma(j) = \sum_{i=1}^{j} \alpha(i), \qquad \sigma(j) = \prod_{i=1}^{j} \alpha(i),$$

og ellers

$$\sigma(j) = \left(\!\!\int_{i=1}^{j}\right) \alpha(i).$$

Vis, at hvis kompositionsforskriften \$ er associativ, gælder for hvert $q \in \grave{N}_p$

$$\left(\!\!\int_{i=1}^{p}\right) \alpha(i) = \left(\!\!\int_{i=1}^{q}\right) \alpha(i) \,\$\, \left(\!\!\int_{i=1}^{p-q}\right) \alpha(q+1).$$

Man skriver da også

$$\$_{i=1}^{p} \alpha(i) = \alpha(1) \$ \ldots \$ \alpha(p).$$

* Vis, at hvis kompositionsforskriften $ desuden er kommutativ, gælder for hver permutation f af $\mathbb{N}_{p+1}$

$$\$_{i=1}^{p} \alpha(f(i)) = \$_{i=1}^{p} \alpha(i).$$

§ 2. Brøklegeme; ordnet Legeme.

Definition: Ved en halvgruppe $(H,\cdot)$ forstås en mængde H med en associativ kompositionsforskrift $\cdot$, for hvilken forkortningsreglerne gælder.

Eksempler: Enhver gruppe er en halvgruppe. I en ring $(M,+,\cdot)$ vil $(M\setminus\{0\},\cdot)$ være en halvgruppe hvis og kuh hvis multiplikationen er en komposition i denne mængde (for dette betyder, at nulreglen og dermed forkortningsreglerne gælder). Mængden af 2×2 -matricer $\underline{\underline{A}}$ med det $\underline{\underline{A}} \geq 1$ udgør med matrixmultiplikation en ikke-kommutativ halvgruppe. Mængden af vektorer i planen beliggende indenfor et givet vinkelrum udfra $\underline{0}$ af størrelse $\leq \pi$ udgør med vektoraddition en halvgruppe.

(Det bør bemærkes, at ovenstående er én blandt flere indbyrdes afvigende i den matematiske litteratur forekommende definitioner af "semigrupper" og "demigrupper").

Dersom en halvgruppe $(H,\cdot)$ er indeholdt i en gruppe $(G,\cdot)$ (d.v.s. at $(H,\cdot)$ er "underhalvgruppe" i $(G,\cdot)$), findes der i gruppen en mindste undergruppe G_o, som indeholder halvgruppen. Thi man ser, at fællesmængden af de undergrupper i $(G,\cdot)$ som indeholder halvgruppen har den nævnte egenskab, og denne fællesmængde er ikke tom, da G selv er en sådan undergruppe.

Hvis $(H,\cdot)$ er kommutativ, bliver $(G_o,\cdot)$ også kommutativ, og G_o vil netop bestå af alle elementer af formen ab^{-1}, hvor $a,b \in H$; vi vil sige, at $(G_o,\cdot)$ er den af $(H,\cdot)$ frembragte brøkgruppe indenfor $(G,\cdot)$. Thi dels er det klart, at G_o i hvert fald må indeholde alle disse elementer. Og dels kan man se, at disse elementer udgør en kommutativ gruppe; dertil bemærker vi først,

at formlen $b(ab^{-1})b = ba = ab = b(b^{-1}a)b$ viser, at $ab^{-1} = b^{-1}a$; ved gentagen anvendelse af dette resultat ser man, at både $(ab^{-1})(cd^{-1})$ og $(cd^{-1})(ab^{-1})$ bliver lig $(ac)(bd)^{-1}$, så at $\cdot$ er en kommutativ komposition indenfor den nævnte elementmængde, og da endvidere $(ab^{-1})^{-1} = ba^{-1}$ udgør de virkelig en kommutativ gruppe.

Man ser, at $(G_o, \cdot)$ fremgår af $H \times H$ ved den afbildning φ, der til parret (a,b) lader svare elementet ab^{-1}, og af den anførte formel for produktet af to elementer ses, at hvis man i $H \times H$ indfører kompositionen $*$ ved $(a,b) * (c,d) = (ac,bd)$, så er $(G_o, \cdot)$ netop homomorft billede ved φ af $(H \times H, *)$.

Da vi her og senere talrige gange skal benytte forbindelsen mellem en homomorfi og den tilsvarende ækvivalensrelation, skal vi minde om resultatet fra AG II, specielt §1,15-19 og §3,12, idet vi formulerer dette resultat som følgende almindelige homomorfisætning:

<u>En homomorf afbildning f af en mængde med kompositionsforskrifter (0 eller 1 eller flere) giver anledning til en ækvivalensrelation ~ på mængden, harmonerende med kompositionerne, og således at x ~ y netop når f(x) = f(y). Hvis man omvendt har en mængde med kompositioner og en på mængden defineret ækvivalensrelation ~, som harmonerer med kompositionerne, så eksisterer der homomorfe afbildninger af mængden med kompositionerne, således at f(x) = f(y) netop når x ~ y, og billedet ved en sådan homomorfi f er bestemt entydigt pånær isomorfi</u> (idet det er isomorft med strukturen af mængden af ækvivalensklasser organiseret ved de kompositioner der fås ved at regne med repræsentanter fra klasserne).

Ved den omtalte homomorfi φ som afbilder $(H \times H, *)$ på $(G_o, \cdot)$ består den tilsvarende ækvivalens i at $(a,b) \sim (c,d)$ netop når $ab^{-1} = cd^{-1}$, hvilket også kan udtrykkes $ad = bc$. Ækvivalensrelationen er dermed fastlagt alene ved strukturen af $(H, \cdot)$, hvormed man får sætningen:

Lad der være givet en kommutativ halvgruppe; i enhver gruppe som indeholder den vil halvgruppen frembringe en kommutativ brøkgruppe, og dennes struktur er bestemt entydigt pånær isomorfi.

Vi skal også vise: Enhver kommutativ halvgruppe kan udvides til en kommutativ gruppe, som er brøkgruppe for den.

Beviset er nærliggende efter det foregående. Lad halvgruppen hedde $(H, \cdot)$. Vi betragter $H \times H$, og indfører herpå en relation $\sim$ ved

$$(a,b) \sim (a_1,b_1) \iff ab_1 = a_1b \ ;$$

denne relation er åbenbart reflexiv og symmetrisk, og den er også transitiv, da $ab_1 = a_1b \wedge bc_1 = b_1c$ medfører $ab_1bc_1 = a_1bb_1c$, hvoraf ved forkortningsreglen fås $ac_1 = a_1c$. Det er altså en ækvivalensrelation. Endvidere indfører vi på $H \times H$ en komposition $*$ ved

$$(a,b) * (c,d) = (ac,bd);$$

denne komposition er åbenbart kommutativ og associativ, og $\sim$ harmonerer med $*$, thi betragter man

$$(a,b) * (c,d) = (ac,bd)$$

$$(a_1,b_1) * (c_1,d_1) = (a_1c_1,b_1d_1) \ ,$$

og antager at faktorerne på venstre side er ækvivalente, altså

at $ab_1 = a_1b$ og $cd_1 = c_1d$, får man $(ac)(b_1d_1) = (a_1c_1)(bd)$, som viser, at højresiderne også er ækvivalente.

Ifølge den almindelige homomorfisætning findes der så en homomorf afbildning φ af $(H \times H, *)$ over på en mængde G_o med komposition $\circ$, således at elementer fra $H \times H$ får samme billede hvis og kun hvis de er ækvivalente. Billedet $(G_o, \circ)$ bliver en kommutativ gruppe, thi da $*$ er kommutativ og associativ får $\circ$ de samme egenskaber, og endvidere indeholder G_o et neutralt element, nemlig $\varphi(a,a)$, fordi $\varphi(a,a) \circ \varphi(c,d) = \varphi(ac,ad) = \varphi(c,d)$ (det sidste lighedstegn fordi $(ac,ad) \sim (c,d)$; da der højst kan findes et neutralt element ses, at $\varphi(a,a)$ er uafhængig af $a \in H$), og endelig vil ethvert element have et inverst, fordi $\varphi(a,b) \circ \varphi(b,a) = \varphi(ab,ba) =$ det neutrale element. Dermed er vist, at $(G_o, \circ)$ er en kommutativ gruppe.

Vi skal nu vise, at $(G_o, \circ)$ har en delmængde som er isomorf med $(H, \cdot)$, for hvis det er tilfældet kan vi erstatte denne delmængdes elementer med elementerne fra H, og når vi efter denne erstatning benytter betegnelsen $(G, \cdot)$ i st.f. $(G_o, \circ)$ så er $(G, \cdot)$ virkelig en udvidelse af $(H, \cdot)$. Dertil vælger vi et $c \in H$, og til et vilkårligt $a \in H$ lader vi nu svare $\varphi(ac,c) \in G_o$; da $\varphi(ac,c) = \varphi(bc,c) \iff a = b$ bliver denne afbildning injektiv, og da $\varphi(ac,c) \circ \varphi(bc,c) = \varphi(abc^2, c^2) = \varphi(abc,c)$ bliver det en homomorf afbildning af $(H, \cdot)$. Dermed har vi skabt gruppen $(G, \cdot)$ som en kommutativ udvidelse af halvgruppen $(H, \cdot)$.

Sluttelig ser vi, at $(G, \cdot)$ er brøkgruppe for $(H, \cdot)$, thi et vilkårligt element $\varphi(a,b) \in G_o$ ses indenfor G_o at opfylde ligningen $\varphi(a,b) \circ \varphi(bc,c) = \varphi(ac,c)$, hvilket med betegnelserne fra $(G, \cdot)$ betyder at $\varphi(a,b) \cdot b = a$ eller $\varphi(a,b) = ab^{-1}$. Sætningens bevis er dermed fuldført.

Ved en ordnet halvgruppe $(H,\cdot,<)$ forstår vi en halvgruppe $(H,\cdot)$, for hvis elementer der er indført en irreflexiv total ordningsrelation $<$, som opfylder betingelsen

$$a < b \Rightarrow ac < bc \wedge ca < cb.$$

I det sidste udsagn kan $\Rightarrow$ erstattes med $\Leftrightarrow$ uden at ændre indholdet, hvilket let bevises indirekte, idet $a \geq b \Rightarrow ac \geq bc \wedge ca \geq cb$.

Ved en ordnet gruppe $(G,\cdot,<)$ forstår vi en gruppe $(G,\cdot)$, der betragtet som halvgruppe er en ordnet halvgruppe.

Den foranstående udvidelsessætning for halvgrupper kan nu kompletteres med følgende: Enhver kommutativ ordnet halvgruppe kan udvides til en kommutativ ordnet gruppe, som er brøkgruppe for den, og dennes struktur er bestemt entydigt pånær isomorfi. NB: Glosen isomorfi anvendes overalt i disse forelæsninger som referende til både kompositioner og relationer, og dækker altså f.eks. hvad der i Mat.1 kaldes "ordenstro isomorfi" o.l.

Bevis: Lad den ordnede halvgruppe hedde $(H,\cdot,<)$ og den (uordnede) brøkgruppe hedde $(G,\cdot)$; små bogstaver betegner elementer fra H. Til et vilkårligt endeligt sæt elementer fra G kan man bestemme et n, så elementerne kan skrives på formen $an^{-1}, bn^{-1}, \ldots$ (det er muligt at skaffe en "fællesnævner" n, nemlig produktet af de enkelte elementers "nævnere"). Med hensyn til entydigheden mangler vi blot at godtgøre, at brøkgruppens ordningsrelation $<$ er bestemt entydigt udfra sin restriktion til halvgruppen, og det er klart, fordi $an^{-1} < bn^{-1} \Leftrightarrow a < b$ (betingelsen for ordnet gruppe). Med hensyn til muligheden af brøkgruppens ønskede ordning ved en relation $\prec$ er metoden nærliggende: for

to elementer an^{-1} og bn^{-1} fra G defineres

$$an^{-1} \prec bn^{-1} \iff a < b;$$

Dette er virkelig brugbart som definition, thi hvis de samme elementer havde en anden fremstilling $a_1n_1^{-1}$ hhv. $b_1n_1^{-1}$, så gælder $an_1 = a_1n \wedge bn_1 = b_1n$, og man får $a < b \iff an_1 < bn_1 \iff a_1n < b_1n \iff a_1 < b_1$. Ordningen af G er en udvidelse af ordningen af H, for hvis $a,b \in H$, så kan de skrives som $(an)n^{-1}$ hhv. $(bn)n^{-1}$ og man får $a \prec b \iff an < bn \iff a < b$. Og endelig opfylder $(G,\cdot,\prec)$ betingelsen for at være en ordnet gruppe, idet $an^{-1} \prec bn^{-1} \iff a < b \iff ac < bc \iff (an^{-1})(cd^{-1}) \prec (bn^{-1})(cd^{-1})$. Beviset er dermed fuldført.

Kommutative grupper og halvgrupper skrives hyppigt med kompositionstegnet + . Betingelsen for at en halvgruppe er ordnet bliver i så fald skrevet på den mere tilvante form $a < b \Rightarrow a + c < b + c$.

Som eksempel til sætningen kan betragtes halvgruppen af komplexe tal $z = x + iy$ beliggende i første kvadrant ($0 \leqq x,y$) med addition som komposition og en ordning givet ved $z_1 < z_2 \iff 0 \leqq \arg(z_1 - z_2) < \pi$. Den tilsvarende brøkgruppe (eller "differensgruppe") bliver $(\check{C},+)$ med den samme ordning. Dersom man med samme komposition og ordning betragter komplexe tal $z = x + ix$, $3 \leqq x$, bliver differensgruppen de komplexe tal på linien $z = x + ix$, ordnet efter voksende x. Eksemplet skal blot være anskueliggørende, sætningens formål fremgår senere.

Ved en <u>ordnet ring</u> $(M,+,\cdot,<)$ forstås en ring $(M,+,\cdot)$, hvor der på mængden M er indført en total irreflexiv ordningsrelation $<$, således at $(M,+,<)$ er en ordnet gruppe (kommutativ), og

således at $0 \leqq x \wedge 0 \leqq y \Rightarrow 0 \leqq xy$, idet 0 er ringens nulelement.

Eksempel: Som $(M,+,<)$ tager man en vilkårlig ordnet gruppe, og idet ethvert produkt sættes lig nul = gruppens neutrale element, kommer der en ordnet ring.

For ringe hvori nulreglen gælder kan den sidste betingelse i definitionen erstattes af $0 < x \wedge 0 < y \Rightarrow 0 < xy$, men det kan ikke gøres i almindelighed, hvilket fremgår af det nævnte eksempel (interessantere eksempler eksisterer).

Ved et ordnet legeme $(L,+,\cdot,<)$ forstår man en ordnet ring $(L,+,\cdot,<)$, hvor $(L,+,\cdot)$ er et legeme.

I en ordnet gruppe (skrevet additivt) og à fortiori i en ordnet ring og et ordnet legeme gælder, at

$$a < b \wedge c < d \Rightarrow a + c < b + d,$$

d.v.s. at "uligheder kan adderes"; det ses, idet man får $a+c < b+c < b+d$. Såfremt $x > o$ vil vi sige, at x er positiv, og såfremt $x < o$ vil vi sige, at x er negativ. Da et legeme er en ring hvori nulreglen gælder, har vi ifølge det tidligere nævnte , at produktet af to positive elementer er igen positivt. Heraf slutter vi nu, at

$$a < b \wedge o < c \Rightarrow ac < bc \wedge ca < cb,$$

("en ulighed kan multipliceres med et positivt element"); det ses, idet man får $o < b-a \wedge o < c$, som ved multiplikation giver $o < bc-ac \wedge o < cb-ca$.

Mængden af de positive elementer i en ordnet ring $(M,+,\cdot,<)$ vil vi kalde M_+ og mængden af de negative vil vi kaldes M_- .

Så viser reglerne ovenfor, at <u>både + og · er kompositioner indenfor</u> M_+, og endvidere, at + også er en komposition i M_-. Vi har

$$M = M_+ \cup \{o\} \cup M_- ,$$

hvor de tre komponenter på højre side er indbyrdes disjunkte. Da $a \neq o \iff -a \neq o$ ser vi, at for <u>$a \neq o$ vil af elementerne a og -a det ene ligge i M_+ og det andet ligge i M_-,</u> thi hvis de lå i samme komponent ville deres sum o også ligge i den. Ved på passende måde at erstatte a med -a ser man, at <u>produktet af et positivt og et negativt element bliver negativt</u>, og at <u>produktet af to negative elementer bliver positivt.</u> Man bemærker også, at i et ordnet legeme $(L,+,\cdot,<)$ er $(L_+,+,<)$ en ordnet halvgruppe og $(L_+,\cdot,<)$ er en ordnet gruppe. Endelig fremgår, at i en ordnet ring (og endda i enhver ordnet gruppe $(M,+,<)$) vil afbildningen $a \to -a$ være en involutorisk automorfi af $(M,+)$, hvorved $M_+ \to M_-$ og omvendt, og $<$ erstattes af $>$.

For senere anvendelser vil følgende bemærkning være nyttig: <u>Hvis der i mængden L af elementer i et legeme $(L,+,\cdot)$ findes en delmængde L_+, så $o \notin L_+$ og så for $a \neq o$ mindst et af elementerne a og -a tilhører L_+, og således at + og · er kompositioner indenfor L_+, så kan der på L defineres en relation $<$, således at $(L,+,\cdot,<)$ bliver et ordnet legeme og L_+ netop bliver mængden af positive elementer i L.</u>

Bevis: Først bemærker vi, at af a og -a vil netop ét tilhøre L_+, for hvis de begge gjorde det ville også $a+(-a) = o \in L_+$. Vi definerer nu relationen $<$ ved

$$a < b \iff b - a \in L_+ .$$

Ved at sætte a = o ses, at {positive} = L_+ . Relationen er irreflexiv, da a-a = o $\notin L_+$, og den er total og asymmetrisk, da for a $\neq$ b netop ét af elementerne b-a og a-b tilhører L_+, og endelig er den transitiv, da b-a, c-b $\in L_+$ medfører at deres sum c-a $\in L_+$; det er altså en total irreflexiv ordningsrelation på L. At (L,+,<) er en ordnet gruppe følger, da a < b $\Rightarrow$ b-a = (b+c) -(a+c) $\in L_+ \Rightarrow$ a+c < b+c. Og sluttelig er det jo direkte givet, at o < x $\wedge$ o < y $\Rightarrow$ o < xy.

Vi skal nu betragte problemer vedrørende indlejring af en ring i et legeme, altså situationen: (M,+,·) er en delring af (L,+,·), hvor (L,+,·) er et legeme.

Lad os først bemærke den almene sætning: Fællesmængden for (endelig eller uendelig mange) dellegemer af et legeme (L,+,·) er igen et dellegeme af (L,+,·). Lad dellegemerne hedde (L_j,+,·); beviset følger så, idet når alle (L_j,+) er undergrupper i (L,+), så er ($\cap L_j$,+) også undergruppe, og når alle ($L_j \setminus \{o\}$,·) er undergrupper i (L$\setminus${o},·), så er ($\cap L_j \setminus \{o\}$,·) også undergrupper; de øvrige krav til kompositionerne på $\cap L_j$ er klart opfyldt, da de er restriktion af kompositionerne på L. Endvidere: Fællesmængden for (endelig eller uendelig mange) delringe af en ring (M,+,·) er igen en delring af (M,+,·). Beviset fås på analog måde, idet for additionen bliver ($\cap M_j$,+) en undergruppe i (M,+), og vedrørende multiplikationen ses, at når · er en komposition i ethvert M_j, altså x,y $\in M_j \Rightarrow$ xy $\in M_j$, så følger x,y $\in \cap M_j \Rightarrow$ xy $\in \cap M_j$.

Hvis (M,+,·) er en delring af et legeme (L,+,·), så findes der et mindste dellegeme (L_o,+,·) af legemet som indeholder (M,+,·), nemlig fællesmængden af samtlige dellegemer der indeholder (M,+,·), for denne fællesmængde er et legeme, og den er

ikke tom, da L selv i hvert fald er et dellegeme af den nævnte art.

Hvis $(M,+,\cdot)$ er en kommutativ delring af et legeme $(L,+,\cdot)$, så findes der et mindste dellegeme $(L_o,+,\cdot)$ af $(L,+,\cdot)$ som indeholder $(M,+,\cdot)$. Dette dellegeme er kommutativt, og det betegnes som brøklegemet for $(M,+,\cdot)$ indenfor $(L,+,\cdot)$. Det er bestemt ved at $(L_o\setminus\{o\},\cdot)$ er brøkgruppen for $(M\setminus\{o\},\cdot)$ indenfor $(L\setminus\{o\},\cdot)$. Dersom den samme ring $(M,+,\cdot)$ er indeholdt i forskellige legemer $(L,+,\cdot)$, så vil de af den frembragte brøklegemer være indbyrdes isomorfe.

Bevis: Når M er indeholdt i et legeme vil nulreglen gælde, og $(M\setminus\{o\},\cdot)$ er derfor en kommutativ halvundergruppe i $(L\setminus\{o\},\cdot)$, og brøkgruppen eksisterer altså; og når L_o skal være et legeme der indeholder M er det klart, at det i hvert fald må indeholde alle elementer fra brøkgruppen. Brøkgruppens elementer suppleret med o er netop samtlige elementer som kan skrives på formen an^{-1}, hvor $a,n \in L \wedge n \neq o$, og de vil med + udgøre en gruppe fordi $an^{-1} - bn^{-1} = (a-b)n^{-1}$ (idet vi som tidligere omtalt altid kan skaffe "fællesnævner"). Betingelserne for dellegeme er dermed opfyldt. At det er kommutativt er klart, da dels brøkgruppen er kommutativ, og dels produkter hvori o indgår som faktor evident er kommutative. Da brøkgruppen er bestemt entydigt pånær isomorfi, vil $(L_o,\cdot)$ være bestemt entydigt pånær isomorfi, og endelig viser formlen $an^{-1} + bn^{-1} = (a+b)n^{-1}$, at der - da jo additionen på M er givet - højst er én måde på hvilken denne isomorfi kan udvides til kompositionen +.

Men selv om der ikke på forhånd er givet et legeme som indeholder ringen, så kan vi konstruere det, idet der gælder:

Enhver kommutativ ring hvori nulreglen gælder kan udvides til et kommutativt legeme som er brøklegeme for ringen, og dette er bestemt entydigt pånær isomorfi.

Entydigheden fremgår af sætningen ovenfor, og resten af beviset er nærliggende; den givne ring skal hedde $(M,+,\cdot)$, og små bogstaver betegner elementer fra den. Vi har da at $(M\setminus\{o\},\cdot)$ er en kommutativ halvgruppe, og ifølge tidligere sætning kan den udvides til en brøkgruppe, hvis elementer alle er af formen an^{-1}, $a,n \in M\setminus\{o\}$; endelig mange elementer af den kan altid skrives med et fælles n. I brøkgruppen er multiplikation givet ved formlen $(am^{-1})(bn^{-1}) = (ab)(mn)^{-1}$. Vi udvider brøkgruppen med et element Ω til en mængde L, og definerer, at et produkt hvori Ω er faktor skal være lig Ω ; hvis vi skriver Ω som on^{-1}, hvor n er vilkårlig $\neq o$, gælder der alment multiplikationsformlen $(am^{-1})(bn^{-1}) = (ab)(mn)^{-1}$. Denne multiplikation er kommutativ og associativ, og ethvert fra Ω forskelligt element an^{-1} har et inverst na^{-1}, så med multiplikation vil de fra Ω forskellige elementer udgøre en gruppe. Vi definerer på L en addition $\oplus$, idet $an^{-1} \oplus bn^{-1}$ sættes lig $(a+b)n^{-1}$. Denne addition er åbenbart kommutativ og associativ, har Ω som neutralt element, og et vilkårligt element an^{-1} har et modsat $(-a)n^{-1}$, så L er med den definerede addition en kommutativ gruppe. Desuden er $\oplus$ en udvidelse af kompositionen + på M, idet $a = (an)n^{-1}$ og $b = (bn)n^{-1}$ som $\oplus$ -sum får $(an+bn)n^{-1} = a+b$. Og den distributive lov gælder, fordi både $(cd^{-1})(an^{-1} \oplus bn^{-1})$ og $(cd^{-1})(an^{-1}) \oplus (cd^{-1})(bn^{-1})$ ved udregning ses at give $c(a + b)(dn)^{-1}$. Sætningen er dermed fuldt bevist.

Sætningen kan kompletteres med en tilsvarende sætning om ordnet ring og legeme: Enhver ordnet kommutativ ring hvori nulreglen gælder kan udvides til et ordnet kommutativt legeme, som

er brøklegeme for ringen, og dette er bestemt entydigt pånær isomorfi.

Vi bemærker først, at ved fremstillingen an^{-1} af elementerne fra Legemet (ovenfor) kan vi, da $n \neq o$, uden indskrænkning af almindeligheden antage, at n er positiv, for ellers erstatter vi blot an^{-1} med $(an)(n^2)^{-1}$. Med hensyn til entydigheden mangler vi blot at vise, at relationen $<$ på L er bestemt entydigt ved sin restriktion til M, og det er klart, thi når vi er i et ordnet legeme og n er positiv, så er $an^{-1} < bn^{-1} \iff a < b$ (små bogstaver betyder stadig elementer fra M). Med hensyn til muligheden af at udvide den ordnede ring $(M,+,\cdot,<)$ til et brøklegeme $(L,+,\cdot)$ som er ordnet, mangler vi blot at vise, at vi kan gøre $(L,+,\cdot)$ til et ordnet legeme ved en ordning $\prec$, som er en udvidelse af $<$: vi vil gøre det ved at benytte en tidligere sætning (s.8). Elementerne i L kan alle skrives på formen an^{-1}, hvor $n > o$ (i M), og vi definerer nu $L_+ = \{an^{-1} \mid a > o \wedge n > o\}$. Vi har $o \notin L_+$, og for $a \neq o$ vil af elementerne $\pm(an^{-1}) = (\pm a)n^{-1}$ netop ét tilhøre L_+, idet netop ét af elementerne $\pm a$ er positiv i M. Endvidere + og $\cdot$ kompositioner i L_+, fordi $an^{-1} + bn^{-1} = (a+b)n^{-1}$ og $(an^{-1})(bn^{-1}) = (ab)(n^2)^{-1}$, og $a,b > o \Rightarrow a+b > o \wedge ab > o$. Ifølge den nævnte sætning er $(L,+,\cdot,\prec)$ altså virkelig et ordnet legeme. Endelig er $\prec$ en udvidelse af $<$, fordi $a \prec b \iff (an)n^{-1} \prec (bn)n^{-1} \iff ((b-a)n)n^{-1} \in L_+ \iff b-a > o \iff a < b$.

I en ordnet kommutativ gruppe $(M,+,<)$ og dermed også i en ordnet ring og et ordnet legeme vil vi definere den <u>absolutte værdi</u> af et element a ved

$$|a| = \max\{a,-a\},$$

altså $|a| = a$ for $o \leqq a$ og $|a| = -a$ for $a \leqq o$. Der gælder øjensynlig $o \leqq |a|$, hvor $=$ er gyldigt hvis og kun hvis $a = o$, og endvidere $|-a| = |a|$, samt

$$-|a| \leqq \left\{\begin{matrix} a \\ -a \end{matrix}\right\} \leqq |a|.$$

Ved at anvende det sidste på a og b og addere fås

$$-(|a| + |b|) \leqq \left\{\begin{matrix} a + b \\ -(a + b) \end{matrix}\right\} \leqq |a| + |b|,$$

altså

$$|a + b| \leqq |a| + |b|.$$

Erstattes heri b med b-a fås $|b| - |a| \leqq |b-a|$, og hvis man dernæst ombytter a og b vil venstresiden skifte fortegn, og tilsammen fås

$$||b| - |a|| \leqq |b-a|.$$

Det kan endvidere være nyttigt at bemærke, at man ved en umiddelbar regning finder

$$c < \left\{\begin{matrix} a \\ b \end{matrix}\right\} < d \Rightarrow |a-b| < d-c.$$

For en ordnet ring, og specielt et ordnet legeme, får man ved blandt $|ab| = |(-a)b| = |a(-b)| = |(-a)(-b)|$ at tage en fremstilling i hvilken begge faktorer er ikke-negativ, at

$$|ab| = |a|\cdot|b|;$$

man bør bemærke, at dette gælder uanset om nulreglen gælder i rin-

gen, og uanset om den er kommutativ. I en ordnet ring (med mere end et element) gælder for et eventuelt etelement e, at

$$|e| = e > o,$$

thi $e \neq o$, og antages e negativ fremkommer en modstrid fordi $e = (-e)(-e)$ ifølge definitionen af ordnet ring skal være $\geq o$. Heraf ses for et element a i et ordnet legeme, og almindeligt for ethvert invertibelt element i en ring, at

$$|a^{-1}| = |a|^{-1}.$$

En mængde M siges at være tæt ordnet ved en total irreflexiv ordningsrelation $\prec$, hvis der til hvilkesomhelst elementer $a,b \in M$ for hvilke $a \prec b$, findes et element $c \in M$, således at $a \prec c \prec b$.

Ethvert ordnet legeme $(L,+,\cdot,<)$ er tæt ordnet ved $<$, thi for $a < b$ får man $a+a < a+b < b+b$, hvoraf ved division med det positive element $e+e$ fås $a < \frac{e}{2}(a+b) < b$.

Lad mængden M være ordnet ved en total irreflexiv ordningsrelation $\prec$: man siger, at en delmængde K af M ligger overalt tæt i M , (ofte siges blot "tæt i M"), hvis der til hvilkesomhelst elementer $a,b \in M$, for hvilke $a \prec b$, findes et element $k \in K$, således at $a \prec k \prec b$.

Lad $(L,+,\cdot,<)$ være et ordnet legeme; hvis der findes et kommutativt dellegeme K, som ligger overalt tæt i L, så er $(L,+,\cdot)$ selv et kommutativt legeme.

Først vil vi vise, at $k \in K \wedge a \in L$ medfører at $ak = ka$ (altså at K's elementer kommuterer med hele L); ved beviset kan vi gerne antage, at $k > o$. Det føres indirekte: hvis $ak \neq ka$ kan man mellem dem bestemme først $k_1 \in K$ og dernæst $k_1+k_2 \in K$, hvor $k_2 > o$ (herved er to gange brugt at K er tæt i L); så gælder $|ak-ka| > k_2$. Dernæst kan man mellem $a- k_2k^{-1}$ og a bestemme $k_3 \in K$, og man ser,

at

$$k_3 < a < k_3 + k_2k^{-1}.$$

Uligheden multipliceres med k fra højre og venstre (siden er dog ligegyldig for elementerne fra K), og man finder

$$kk_3 < \begin{Bmatrix} ak \\ ka \end{Bmatrix} < kk_3 + k_2,$$

hvoraf ses $|ak-ka| < k_2$, hvilket giver en modstrid.

Så gentages metoden for at vise, at ab = ba; vi antager $b > 0$. Hvis $ab \neq ba$ kan man mellem dem bestemme to elementer fra K, og dermed et k_2 så $|ab-ba| > k_2$. Dernæst kan man mellem $a - k_2b^{-1}$ og a bestemme $k_3 \in K$, hvoraf

$$k_3 < a < k_3 + k_2b^{-1}.$$

Vi multiplicerer med b både fra højre og venstre (og kan herved efter behag erstatte k_2b^{-1} med $b^{-1}k_2$), og finder

$$bk_3 < \begin{Bmatrix} ab \\ ba \end{Bmatrix} < bk_3 + k_2,$$

hvoraf ses $|ab-ba| < k_2$, hvilket giver en modstrid.

De foranstående resultater kan umiddelbart anvendes på det i § 1 opbyggede system af naturlige tal. Sætningsnumrene i det følgende henviser til denne paragraf.

I sætningerne 4,5 og 6 blev det vist, at $(\acute{N},+)$ udgør en kommutativ halvgruppe. På denne defineredes en relation $<$ ved at $a < b$ hvis og kun hvis der findes et naturligt tal x således at $b = a+x$, og sætningerne 14 og 16 udsiger, at der derved er dannet en ordnet halvgruppe $(\acute{N},+,<)$. Ifølge nærværende § kan halvgruppen udvides til den ordnede gruppe $(\acute{Z},+,<)$ af de hele tal.

Nulelementet betegnes 0 ("nul"), og ifølge sætn. 7 tilhører det ikke de naturlige tal. Idet ethvert $c \in \acute{Z}$ kan skrives på for-

men c = b-a, hvor a,b ∈ Ń ser man af sætn. 8, at hvis c er et fra 0 forskelligt helt tal, så vil netop ét af tallene +c og -c være et naturligt tal. Af definitionen på ordningsrelationen < ser man , idet man erindrer at (Ź,+,<) er en ordnet gruppe, at mængden af positive hele tal $Ź_+$ netop bliver Ń. Afbildningen a → -a vil være en involutorisk automorfi af (Ź,+) ved hvilken de positive tal afbildes på de negative og omvendt, medens < erstattes af >.

Sætn. 18 viser, at det mindste positive tal er 1 (lig den neutrale multiplikator indenfor de naturlige tal), hvorefter gruppeegenskaben for de hele tal (Ź,+) viser, at der for ethvert tal x findes et umiddelbart efterfølgende, som netop er x+1. Af den nævnte involutoriske automorfi ses, at det største negative hele tal er -1, og at der til ethvert helt tal x findes et umiddelbart foregående, nemlig x-1. Og sætningerne 20-22 viser (sammen med gruppeegenskaben og den involutoriske automorfi), at enhver nedad begrænset delmængde af de hele tal har et mindste element, og at enhver opad begrænset delmængde af de hele tal har et største element.

Med hensyn til multiplikation blev en sådan defineret som en komposition indenfor de naturlige tal, og i sætningerne 10,11,12 og 13 blev det omtalt, at den er distributiv m.h.t. additionen, kommutativ, associativ og at forkortningsreglen gælder, altsammen på Ń; specielt er altså (Ń,·) en kommutativ halvgruppe. Endvidere var den defineret sådan at tallet 1 er neutralt element.

Man kan nu definere en multiplikation som en komposition indenfor Ź på følgende måde: Hvis en af faktorerne i produktet ab er 0, sættes produktet lig 0; hvis både a og b er ≠ 0 sættes produktet ab til ± |a|·|b|, idet |a|·|b| er det ved multiplikationen indenfor Ń bestemte element af Ń, og hvor man skal vælge fortegn

net + hvis begge faktorer er positive eller begge faktorer er negative, medens man skal vælge fortegnet - hvis den ene faktor er positiv og den anden faktor er negativ. Man ser umiddelbart, at den derved definerede multiplikation er en udvidelse af multiplikationen på $\acute{N} = \acute{Z}_+$. Endvidere er den åbenbart kommutativ. Endvidere er det klart, at nulreglen gælder. Tallet 1 er neutral faktor, hvilket er klart hvis den anden faktor er positiv eller 0 og let ses hvis den er negativ, idet så $a = -|a|$. Den er associativ, idet et produkt abc er uafhængigt af hvorledes man sætter parenteser i det, hvilket er klart hvis en af faktorerne er 0, for så er produktet 0, og iøvrigt ses ved at gennemgå de forskellige fortegnsmuligheder og benytte, at multiplikationen på $\acute{N}$ var associativ. Endelig er den distributiv, idet der gælder $a(b+c) = ab+ac$; det er klart, hvis et af bogstaverne har værdien 0, og i de andre tilfælde kan det ses ved at benytte at multiplikationen på $\acute{N}$ var distributiv idet man gennemgår samtlige forskellige fortegnsmuligheder for a,b,c og b + c. Dermed er det bl.a. vist, at $(\acute{Z},+,\cdot)$ er en ring.

Endvidere er det en ordnet ring fordi $0 \leqq a \wedge 0 \leqq b \Rightarrow 0 \leqq ab$. Af multiplikationens egenskaber kombineret med noget af det tidligere får vi ialt: Systemet af hele tal $(\acute{Z},+,\cdot,<)$ er en kommutativ ordnet ring med et etelement og i hvilken nulreglen gælder, altså en integritetsring.

På systemet $(\acute{Z},+,\cdot,<)$ kan vi nu anvende sætningen fra s.11-12 foran, om udvidelse af en ordnet kommutativ ring med nulregel til et ordnet kommutativt legeme som er brøklegeme for ringen, og derved fremkommer de rationale tals legeme $(\acute{Q},+,\cdot,<)$. Ved de rationale tals legeme $(\acute{Q},+,\cdot,<)$ forstås det pånær isomorfi entydigt bestemte ordnede kommutative legeme som er brøklegeme for den ordnede ring $(\acute{Z},+,\cdot,<)$. Det er tæt ordnet, for det er ethvert legeme.

Man bemærker, at i den foregående systematiske opbygning af matematikken i kursus AG (Mat.1), kapitlerne I og II, og i nærværende kapitel AT er der ikke på noget sted bygget på kendskab til ringen $(\mathbb{Z},+,\cdot,<)$ af hele tal eller legemet $(\mathbb{Q},+,\cdot,<)$ af rationale tal. De er kun på grund af deres tilvante karakter benyttet i (ganske vist talrige) illustrerende eksempler og øvelser. Ligeledes har systemet af naturlige tal heller ikke været nogen forudsætning. En enkelt undtagelse er dog gjort af praktiske - men ikke af logiske - grunde med omtalen i AG II,2 af potensreglerne og de dertil knyttede gruppeteoretiske betragtninger, men uden skade for logikken kunne det have været udsat til den nærværende paragraf. Ligeledes er begrebet primtal, som anvendes lige nedenfor, af praktiske - men ikke logiske - grunde taget noget på forskud. Lignende bemærkninger kunne knyttes til de følgende paragraffers indførelse af reelle og komplekse tal.

Lad $(L,+,\cdot)$ være et legeme med mindst to elementer. Ved primlegemet i L forstår man det mindste ikke-trivielle dellegeme af L (idet det vil fremgå, at et sådant eksisterer). Når L har mere end ét element findes der et etelement e forskelligt fra nulelementet, og e er indeholdt i ethvert ikke-trivielt dellegeme, og fællesmængden af alle ikke-trivielle dellegemer bliver netop primlegemet.

Primlegemet indeholder i hvert fald e og hele den cykliske undergruppe af $(L,+)$ som frembringes af e, altså alle elementer af form he, hvor $h \in \mathbb{N}$. Men disse elementer udgør i sig en delring af $(L,+,\cdot)$, fordi der gælder formlerne

$$he + ke = (h+k)e; \qquad (he) \cdot (ke) = (hk)e;$$

(NB prikken betyder legemsmultiplikation, medens størrelser som

he betyder elementer i den cykliske gruppe frembragt af e ved +; formlernes begrundelse ligger i de i AG II, 2 omtalte potensregler). Af formlernes udseende ser man endda, at delringen fremgår af ringen $(\dot{Z},+,\cdot)$ ved homomorfien $h \to he$. Homomorfe afbildninger af $(\dot{Z},+,\cdot)$ er fuldstændigt undersøgt i AG II,3 hvor det vistes, at de enten er isomorfier eller billedet er isomorft med en ring $(\dot{Z}_m,+,\cdot)$ af restklasser af de hele tal modulo et naturligt tal m. I den foreliggende situation er muligheden m = 1 udelukket, da det ville medføre e = nulelementet, og da endvidere nulreglen gælder i billedet (som jo er indeholdt i et legeme) må m være et primtal p, men så er billedet også et legeme (AG II,3,17).

I det sidste tilfælde er altså primlegemet isomorft med legemet af restklasser modulo et primtal p, og vi siger, at legemet $(L,+,\cdot)$ har karakteristik p. Der gælder pe = o, og derfor for ethvert $a \in L$ at pa = o (hvor pa er et element af formen a+a+...+a, p addender).

I det første tilfælde er delringen isomorf med $(\dot{Z},+,\cdot)$, og vi kan umiddelbart anvende en sætning foran (side 10), ifølge hvilken der må eksistere et primlegeme som er isomorft med brøklegemet for $(\dot{Z},+,\cdot)$; altså er primlegemet isomorft med $(\dot{Q},+,\cdot)$. Vi siger, at legemet $(L,+,\cdot)$ har karakteristik 0.

Man bemærker, at i begge tilfælde er den nødvendige og tilstrækkelige betingelse for at he = o at h er et multiplum af karakteristikken.

Et endeligt legeme må have et endeligt primlegeme, så at karakteristikken for et endeligt legeme er et primtal p. Karakteristikken for et uendeligt legeme kan man derimod ikke sige noget om.

Det er foran vist, at i et ordnet legeme er etelementet positivt, hvoraf ses, at afbildningen $he \to h$ er en isomorf afbild-

ning af den ordnede mængde $(\{he\},<)$ på $(\dot{Z} = \{h\},<)$; deraf ses, at for $h > 0$ er alle $he > o$, så at et ordnet legeme har karakteristik 0. Endvidere: primlegemet for et ordnet legeme er isomorft med det ordnede legeme $(\dot{Q},+,\cdot,<)$, og ordningen på primlegemet er bestemt entydigt; det følger umiddelbart af den tidligere sætning om det entydigt bestemte ordnede brøklegeme for en ordnet ring.

Et ordnet legeme $(L,+,\cdot,<)$ i hvilket primlegemet ligger overalt tæt kaldes ofte arkimedisk ordnet. Af en sætning side 14 ses umiddelbart, at ethvert arkimedisk ordnet legeme er kommutativt.

Nødvendigt og tilstrækkeligt for at et ordnet legeme $(L,+,\cdot,<)$ er arkimedisk ordnet er, at der til ethvert positivt $a \in L$ findes et $n \in \dot{N}$, så $n^{-1} = e/n < a$ (d.v.s. at "følgen $\ldots,1/n,\ldots$ konvergerer mod nul"). Vi viser først nødvendigheden: Hvis legemet er arkimedisk vil der mellem o og a findes et element mn^{-1} fra primlegemet, og hvis m vælges positiv bliver n også positiv, og så er $o < n^{-1} \leq mn^{-1} < a$. Dernæst tilstrækkeligheden: Vi antager $c < d$, og skal vise, at der mellem dem findes et rationalt element mn^{-1}. Hvis $c < o < d$ er det klart opfyldt, og vi kan derfor (med eventuelt fortegnsskifte) gerne antage, at $o < c < d$. Vi vælger først n så $n^{-1} < d-c$, og dernæst m som det mindste naturlige tal (eksisterende !) for hvilket $m^{-1} < (nc)^{-1}$. Så bliver $(m-1)n^{-1} \leq c < mn^{-1}$ (ses let at være gyldigt, også selv om $m = 1$), og ved at addere $n^{-1} < d-c$ til venstresiden fås den ønskede dobbeltulighed $c < mn^{-1} < d$. Beviset har benyttet, at det rationale primlegeme er kommutativt, men for selve legemet er ikke forudsat kommutativitet. Man ser, at den nævnte betingelse for arkimedisk ordning også kan udtrykkes: Til ethvert $a \in L$ skal findes et $n \in N$, så $a < n$.

Øvelser til § 2.

1) Definer kompositioner + og .i en mængde af 4 elementer, således at der opstår et legeme.

2) Vis, at en endelig halvgruppe er en gruppe.
Vis, at en endelig ring hvori nulreglen gælder (f.eks. en integritetsring) er et legeme.

3) Vis, at mængden af n × n-matricer over en ring med matrixaddition og matrixmultiplikation udgør en ring.
Vis, at mængden af n × n-matricer over $\dot{R}$, og som har lutter 0 under diagonalen med matrixaddition og matrixmultiplikation udgør en ring. Angiv for denne ring samtlige nilpotente elementer (et nilpotent element er et element a, for hvilket der findes et $n \in \dot{N}$, så a^n = nulelementet).

4) Vis, at i en vilkårlig ring vil dens centrum være en delring; ved centrum for ringen $(M,+,\cdot)$ forstås mængden af elementer x, for hvilke $x \cdot y = y \cdot x$ for alle $y \in M$.
Vis, at i et vilkårligt legeme er centrum et dellegeme.

5) På mængden $\dot{N}$ af naturlige tal defineres en komposition ved

$$a * b = a + b + ab.$$

Vis, at $(\dot{N},*)$ er en kommutativ halvgruppe, som er isomorf med $(\dot{N}\setminus\{1\},\cdot)$. Bevis, at dens brøkgruppe er isomorf med $(\dot{Q}_+,\cdot)$.

6) Vis, at såfremt $(M,+,\cdot)$ er et endeligt kommutativt legeme, hvis etelement betegnes e, så har produktet af alle de fra nul forskellige elementer altid værdien -e (for visse specielle legemer er en særbetragtning eventuelt nødvendig).

7) Lad M være mængden af kontinuerte funktioner x(t), som afbilder $\dot{R}$ ind i $\dot{R}$ og som kun er forskellige fra 0 på et endeligt interval. Vis, at M kan organiseres som en ring $(M,+,*)$, idet vi som ringadditionen benytter sædvanlig addition, og som ringmultiplikationen benytter "foldningen"

$$x * y(t) = \int_{-\infty}^{\infty} x(t - s)\, y(s)\, ds.$$

Vis, at mængden af lige funktioner indenfor M udgør en delring.

Eftervis, at ringen $(M,+,*)$ ikke har noget etelement e(t) (man kan f.eks. vise, at hvis man definerer $k(t) = 1$ på $[-1,1]$ og $k(t) = 0$ udenfor dette interval ($k(t) \notin M$), så skulle

$$e * k(t) = \int_{-1}^{1} e(t - s)\, ds$$

være lig k(t), og heraf udlede en modstrid).

8) Lad $(M,+,\cdot)$ være en vilkårlig ring. På $(\dot{Z} \times M)$ defineres kompositioner $\oplus$ og $\odot$ ved

$$(m,x) \oplus (n,y) = (m+n, x+y)$$

$$(m,x) \odot (n,y) = (mn,\ my + nx + x \cdot y).$$

Vis, at $(\dot{Z} \times M, \oplus, \odot)$ er en ring med etelement, og at den har en med $(M,+,\cdot)$ isomorf delring.

9) Lad $(M,+,\cdot)$ være en vilkårlig ring. For dennes elementer defineres en ny komposition \$ ved $a \$ b = a + b - ab$. Vis, at kompositionen \$ er associativ, og at der findes et ved kompositionen neutralt element. Vis, at ethvert nilpotent element i ringen har et med hensyn til \$ inverst element; nilpotent er defineret i øv. 3.

10) Vis, at $M = \{r + s\sqrt{2} \mid r,s \in \grave{Z}\}$ udgør en delring af $(\grave{R},+,\cdot)$, og at dens brøklegeme er $\{r + s\sqrt{2} \mid r,s \in \grave{Q}\}$.
Vis, at $r + s\sqrt{2} \to r^2 - 2s^2$ afbilder $(M,\cdot)$ homomorft ind i $(\grave{Z},\cdot)$, og godtgør herved, at mængden af de naturlige tal der kan skrives som $r^2 - 2s^2$, $r,s \in \grave{Z}$, med multiplikation udgør en halvgruppe. Er denne halvgruppe en ægte del af $\grave{N}$?

11) Lad der på en ret linie i planen være givet to punkter P_o og P_1, og lad M være mængden af reelle tal r, som er således at $r \cdot \vec{P_oP_1} = \vec{P_oP_r}$, hvor P_r kan konstrueres med passer og lineal udfra P_o og P_1. Vis, at $(M,+,\cdot)$ er et legeme.

12) Lad $(M,+,\cdot)$ være en (ikke-kommutativ) ring. Lad e være et venstre-etelement, hvormed menes, at $e\cdot a = a$ for alle $a \in M$. Bevis, at dersom nulreglen gælder i ringen, da er e også et højre-etelement, d.v.s. at $b\cdot e = b$ for alle $b \in M$. Gør rede for, at dersom der findes netop eet venstre-etelement e, da kan man ikke deraf slutte, at nulreglen gælder, men man kan ikke destomindre slutte, at e også er højre-etelement.

13) Lad $(M,+,\cdot)$ være en (ikke-kommutativ) ring med et et-element e. Lad x være et venstre-inverst element til a, d.v.s. at $x\cdot a = e$. Vis, at dersom nulreglen gælder, eller dersom det blot er givet, at x er det eneste venstre-inverse til a, så er x også højre-invers til a, d.v.s. at $a\cdot x = e$.

14) Halvgruppen $(\dot{N},\cdot)$ har brøkgruppen $(\dot{Q}_+,\cdot)$. Vis på grundlag af de naturlige tals egenskaber (men uden at benytte ringen $(\dot{Z},+,\cdot)$), at halvgruppen $(\dot{N},+)$ kan udvides til en kommutativ halvgruppe $(\dot{Q}_+,+)$, således at multiplikationen i $\dot{Q}_+$ bliver distributiv med hensyn til +.

15) Lad $(M,\prec)$ være en totalt ordnet mængde, som hverken har et første eller et sidste element, men hvori enhver nedad begrænset delmængde har et første og enhver opad begrænset delmængde har et sidste element. Bevis, at $(M,\prec)$ er isomorf med $(\dot{Z},<)$

16) Godtgør, at de komplexe tals legeme $(\dot{C},+,\cdot)$ ikke kan ordnes til et ordnet legeme.

17) Vis, at i et legeme med karakteristik p gælder formlen $(a+b)^p = a^p + b^p$.

18) I mængden $D = \dot{Q}\times\dot{Q}$ af par af rationale tal defineres kompositionerne + og · ved

$$(a_1,a_2) + (b_1,b_2) = (a_1+b_1,a_2+b_2),$$

$$(a_1,a_2) \cdot (b_1,b_2) = (a_1b_1,a_1b_2+a_2b_1).$$

Vis, at der herved fremkommer en kommutativ ring $(D,+,\cdot)$ med etelement og som har et med $(\dot{Q},+,\cdot)$ isomorft dellegeme. Identificeres dette med $\dot{Q}$, kan ethvert element i D skrives

$$(a_1,a_2) = a_1 + a_2\rho, \qquad a_1,a_2 \in \dot{Q},$$

hvor $\rho = (0,1)$, $\rho^2 = 0$. ($(D,+,\cdot)$ kaldes ringen af duale tal). Vis, at der ved

$$a_1 + a_2\rho < b_1 + b_2\rho \iff a_1 < b_1 \vee (a_1 = b_1 \wedge a_2 < b_2)$$

defineres en relation < på D, således at $(D,+,\cdot,<)$ er en ord-

net ring.

Vis, at $(D,+,\cdot,<)$ ikke er arkimedisk ordnet.

19) Vis, at matricerne (med komplexe elementer)

$$= \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix} \qquad a,b,c,d \in \dot{Q}$$

med matrixaddition og matrixmultiplikation udgør en ikke-kommutativ ring med etelement e, og i hvilken ethvert element forskelligt fra nulelementet har et inverst, altså et ikke-kommutativt legeme.

Angiv legemets primlegeme og dets centrum (se def. i øv.4).

Angiv 3 forskellige elementer, hvis kvadrat er -e; kan legemet ordnes?

Idet K kan angives ved talsættet $(a,b,c,d) \in \dot{Q}^4$, viser øvelsen, at $\dot{Q}^4$ på en ikke triviel måde kan organiseres som en ikke-kommutativt ring, og endda som et legeme (legemet af "kvaternioner"; i st.f. $\dot{Q}$ kunne også være benyttet $\dot{R}$).

20) Lad $(G,\$)$ være en vilkårlig kommutativ gruppe, og lad M være mængden af homomorfier af $(G,\$)$ ind i sig selv ("endomorfier" af $(G,\$)$). Til $f,g \in M$ defineres en afbildning $f + g$ af G ind på sig selv ved $(f + g)(x) = f(x) \$ g(x)$, $x \in G$; vis, at der herved er defineret en komposition indenfor M. Til $f,g \in M$ defineres endvidere en afbildning $f \cdot g$ af G indpå sig selv ved $(f \cdot g)(x) = f(g(x))$, $x \in G$; vis, at der også herved er defineret en komposition indenfor M. Vis, at $(M,+,\cdot)$ er en ring, kaldet "endomorfiringen" for $(G,\$)$. Vis, at endomorfiringen for gruppen $(\dot{Z},+)$ er isomorf med $(\dot{Z},+,\cdot)$. Lad $(G,\$)$ være en transformationsgruppe af 4. orden, bestående af de fire afbildninger af planen E_2 på sig selv

$$g_1: \quad (x,y) \to (x,y),$$

$$g_2: \quad (x,y) \to (-x,y).$$

$$g_3: \ (x,y) \to (-x,-y),$$

$$g_4: \ (x,y) \to (x,-y);$$

find antallet af elementer i endomorfiringen for $(G,\$)$, og vis, at ringen ikke er kommutativ og at nulreglen ikke gælder.

21. Lad $(A,+,\cdot,<)$ være en ordnet ring, og lad B være en delring af den. Vi siger, at $x \in A$ er uendelig stor relativt til B, hvis det for alle $y \in B$ gælder, at $|y| < |x|$. Vis, at mængden af de $x \in A$ som ikke er uendelig store relativt til B udgør en Delring C af $(A,+,\cdot,<)$, og at $B \subsetneq C$.
Vis, at i en kommutativ ring $(A,+,\cdot,<)$ vil de nilpotente elementer udgøre en delring B, og at $x \in A \backslash B$ medfører at x er uendelig stor relativt til B (nilpotent defineret i øv.3).

22. Vis ved den almindelige homomorfisætning, at hvis f og g er to forskellige homomorfe afbildninger af en mængde med kompositionsforskrifter, og $f(x) = f(y) \Rightarrow g(x) = g(y)$, så kan g skrives på formen $g \doteqdot \varphi \circ f$, hvor φ er en homomorfi, hvis definitionsmængde og værdimængde ønskes angivet.

Trykfejl og rettelser til AT § 2.

Side 1 linie 7-8 f.n. "og denne... tom, da" udgår.

\- 6 - 7 f.o. tilføj "Af definitionen ses let, at relationen $\prec$ er irreflexiv, total, asymmetrisk og transitiv; lad os f.eks. bevise det første: $an^{-1} = bn^{-1} \Rightarrow a = b$, så at hverken $a < b$ eller $a > b$, og derfor hverken $an^{-1} \prec bn^{-1}$ eller $an^{-1} \succ bn^{-1}$. Den er derfor brugbar som ordningsrelation.

\- 6 - 5 f.n. for "voksende" læs "aftagende".

\- 7 - 6 f.o. - "kommer" - "fremkommer".

\- 8 - 3 f.o. - "M_+ " - "$M_+ \cup \{0\}$".

\- 8 - 3 f.o. - "M_- " - "$M_- \cup \{0\}$".

\- 8 - 10 f.o. - "negativt" - "ikke-positivt".

\- 8 - 10 f.o. - "positivt" - "ikke-negativt".

\- 9-10 "og den..tom, da" "i hvert fald" udgår.

\- 11 - 11 f.n. tilføj "så at vi kan identificere Ω med 0".

\- 18 - 12 f.o. for "en" læs "uden".

\- 19 - 14 f.o. - "I det sidste" - "I dette".

\- 19 - 19 f.o. - "I det første tilfælde" - "I isomorfitilfældet".

\- 20 - 10 f.o. tilføj "Da karakteristikken af et ordnet legeme er 0, er primlegemet isomorft med $(\mathbb{Q},+,\cdot,<)$".

Øvelse 17 tilføj "kommutativt".

\- 19 tilføj " $\underline{\underline{K}}$ " til venstre udfor matricen.

§ 3. Idealer.

Lad $(M,*,\ldots)$ være en mængde med kompositioner, mindst én, og således at $(M,*)$ er en gruppe. Ved en homomorf afbildning φ bliver $(M,*,\ldots)$ overført i et billede $(L,\circ,\ldots)$ med ligeså mange kompositioner, og således at $(L,\circ)$ er en gruppe.

Ifølge den almindelige homomorfisætning (§2,2) er φ bestemt entydigt pånær isomorfi i billedet ved den tilsvarende ækvivalensrelation $\sim$, som er således beskaffen, at $x \sim y$ er ensbetydende med at $\varphi(x) = \varphi(y)$. Men denne ækvivalensrelation er for givet $(M,*,\ldots)$ bestemt ved den delmængde I af M, som ved afbildningen føres over i det neutrale element e_L i gruppen $(L,\circ)$, altså ved $I = \varphi^{-1}(e_L)$. Thi vi får $x \sim y$ hvis og kun hvis $x * y^{-1} \in I$, da dette jo betyder, at $\varphi(x * y^{-1}) = e_L \Leftrightarrow \varphi(x) = \varphi(y)$.

Vi har altså sætningen : <u>For en given mængde med kompositioner $(M,*,\ldots)$, hvor M med den først noterede komposition $*$ udgør en gruppe, er en homomorf afbildning φ bestemt entydigt pånær isomorfi i billedet ved den delmængde I af M, som ved homomorfien overføres i det neutrale element i den gruppe, som er billede af $(M,*)$</u>. Denne delmængde I betegnes som homomorfiens <u>kerne</u>, og den pånær isomorfi entydigt bestemte billedstruktur $(L,\circ,\ldots)$ skrives $(M,*,\ldots)/I$, og betegnes som den <u>kvotientstruktur</u> eller <u>faktorstruktur</u> der fremgår af $(M,*,\ldots)$ ved en afbildning med I som kerne.

Hvis M har et endeligt elementantal m, så må I også have et endeligt elementantal i, og da $x \sim x_o$ hvis og kun hvis $x = x_o * z$, hvor z kan gennemløbe I, ser man, at enhver af ækvivalensklasserne i M indeholder i elementer, og antallet af ækvivalensklasser lig antallet af elementer i kvotientstrukturen bliver derfor lig m/i.

Heraf fremgår bl.a. at I ikke kan være en vilkårlig delmængde af M (idet i skal gå op i m), men man har jo også, at den nødvendige og tilstrækkelige betingelse for at en delmængde I af M kan være kerne for en homomorf afbildning af $(M,*,...)$ er, at den relation $\sim$, som defineres ved at $x \sim y \Leftrightarrow x * y^{-1} \in I$, skal være en ækvivalensrelation på M og harmonerende med samtlige forekommende kompositioner.

Lad os først betragte situationen hvis der kun er én komposition, d.v.s. hvis der blot er givet en gruppe $(M,\cdot)$, i hvilken vi nu benytter sædvanlig multiplikativ skrivemåde. For det første skal relationen $\sim$ være en ækvivalensrelation, d.v.s. den skal være

reflexiv, hvilket medfører xx^{-1} = etelementet $\in I$,

symmetrisk, ... $xy^{-1} \in I \Rightarrow yx^{-1} \in I$,

transitiv, ... $xy^{-1} \in I \wedge yz^{-1} \in I \Rightarrow xz^{-1} \in I$,

og man ser, at disse krav netop udtrykker, at I er en undergruppe i $(M,\cdot)$. For det andet skal den harmonere med multiplikationen, hvilket betyder, at

$$xy^{-1} \in I \wedge x_1y_1^{-1} \in I \quad \Rightarrow \quad (xx_1)(yy_1)^{-1} \in I;$$

vi sætter $x = iy$ og $x_1 = i_1y_1$, hvor $i,i_1 \in I$, og så fås ved indsættelse i betingelsens højreside, at $iyi_1y_1y_1^{-1}y^{-1} \in I$ skal gælde for alle valg af disse elementer, men det simplificeres jo umiddelbart til at $yi_1y^{-1} \in I$ altid skal gælde, og det er netop betingelsen for at I er en normal undergruppe i $(M,\cdot)$ (AG II,2,18). Vi har dermed repeteret beviset for de bekendte sætninger om at <u>i en gruppe $(M,\cdot)$ er de delmængder af M som kan være kerne ved en homomorfi af gruppen netop de normale undergrupper i $(M,\cdot)$</u>. Denne karakterisering kunne altså være benyttet som definition af "normal undergruppe".

Eksempel: I et sædvanligt 3-dimensionalt euklidisk rum udgør de ortogonale afbildninger af rummet på sig selv med fastholdt begyndelsespunkt (ortogonale m.h.t. afstandskvadratet, d.v.s. afstandsbevarende) en ikke-kommutativ gruppe. De egentlig ortogonale afbildninger ($\det \underline{\underline{S}} = +1$, de orienteringsbevarende) udgør en undergruppe hvis index er lig 2, og som er en normal undergruppe. Den er kerne ved en homomorfi, ved hvilken gruppen afbildes på en kvotientgruppe med 2 elementer, nemlig et neutralelement som er billede af ækvivalensklassen bestående af de orienteringsbevarende afbildninger, og et andet element som er billede af ækvivalensklassen af de orienteringsændrende afbildninger ($\det \underline{\underline{S}} = -1$).

Vi skal nu betragte situationen, hvor en ring $(M,+,\cdot)$ afbildes homomorft. De delmængder I af M som kan være kerne for en homomorf afbildning af ringen kaldes idealer i ringen.

Enhver ring indeholder to trivielle idealer. Det ene er M selv, som er kerne for en afbildning, ved hvilken ringen afbildes på en (udartet) ring bestående af ét element. Det andet er nulidealet $\{0\}$, som er kerne for en afbildning hvor enhver af de tilsvarende ækvivalensklasser består af ét element, altså en bijektiv homomorfi, d.v.s. en isomorfi.

Nødvendigt og tilstrækkeligt for at en delmængde I af en ring $(M,+,\cdot)$ er et ideal er, at følgende to betingelser er opfyldt:

Id 1: I er en undergruppe i ringens additive gruppe $(M,+)$.

Id 2: For $a \in I$ og $x \in M$ skal ax og xa begge tilhøre I.

Man bemærker, at for kommutative ringe er $ax = xa$, så at man for kommutative ringe kan nøjes med at nævne det ene af de to krav i Id2.

Først vises nødvendigheden: Id1 er nødvendig, fordi I specielt skal være kerne for en homomorf afbildning af gruppen $(M,+)$, og derfor skal være (normal) undergruppe i $(M,+)$. Idet homomorfien kaldes φ ses nødvendigheden af Id2 af at $\varphi(a) = 0 \Rightarrow \varphi(ax) = \varphi(a)\,\varphi(x) = 0 \wedge \varphi(xa) = \varphi(x)\,\varphi(a) = 0$.

For at vise tilstrækkeligheden kan vi betragte den relation $\sim$ som defineres ved $a \sim a_1 \iff a_1 - a \in I$. Når I er undergruppe i $(M,+)$, normal fordi $(M,+)$ er kommutativ, så er $\sim$ en ækvivalensrelation som harmonerer med gruppekompositionen +, hvilket blev vist i undersøgelsen ovenfor af homomorfi af en gruppe, og vi mangler blot at vise, at $\sim$ harmonerer med $\cdot$; vi skal altså vise, at $a \sim a_1 \wedge b \sim b_1 \Rightarrow ab \sim a_1 b_1$, men det er klart, thi når $a_1 - a \in I \wedge b_1 - b \in I$, så vil ifølge Id2 også $(a_1 - a)b_1$ og $a(b_1 - b)$ tilhøre I, og derfor også ifølge Id1 deres sum, som bliver $a_1 b_1 - ab$, tilhøre I. Dermed er eftervist, at Id1 og Id2 karaktiserer idealerne.

Af betingelserne ses umiddelbart, at <u>ethvert ideal er en delring</u> af $(M,+,\cdot)$. Det omvendte gælder ikke, f.eks. viser Id2 at et Ideal som indeholder etelementet e er lig hele M; men det gælder ikke almindeligt, at hvis en delring indeholder e, så er den lig hele M. F.eks. har $(\dot{Q},+,\cdot)$ den ægte delring $(\dot{Z},+,\cdot)$ som indeholder etelementet, og $(\dot{Z},+,\cdot)$ er altså ikke noget ideal i $(\dot{Q},+,\cdot)$.

Der gælder: <u>Fællesmængden for (endelig eller uendelig mange) idealer i en ring er et ideal i ringen</u>. Det kan vises ved at benytte Id1 og Id2; simplest ses det dog ved at bemærke, at hvis der på en mængde med kompositioner $(M,*,\ldots)$ er givet en samling ækvivalensrelationer harmonerende med kompositionerne, så vil den relation $\sim$ der defineres ved $x \sim y$ hvis og kun hvis x og y er ækvivalente ved alle de givne relationer, også være en ækvivalensrelation som harmonerer med alle kompositionerne; kernen svarende til $\sim$ er

netop fællesmængden af kernerne svarende til de givne relationer.

Ved en surjektiv homomorfi af en ring vil et ideal i ringen afbildes på et ideal i billedringen. Bevis: Lad φ være en homomorfi som afbilder ringen $(M,+,\cdot)$, og lad $I \subseteq M$ opfylde ID1 og Id2. Da vil $\varphi(I)$ indenfor $\varphi(M)$ opfylde Id1 (fordi en surjektiv homomorfi afbilder undergruppe på undergruppe), og den vil opfylde Id2 (fordi $b = \varphi(a)$, $a \in I$ og $y = \varphi(x)$, $x \in M$ giver $by = \varphi(a)\cdot\varphi(x) = \varphi(ax) \in \varphi(I)$, og analogt ses at $yb \in \varphi(I)$).

Eksempel på ideal: Mængden af kontinuerte reelle funktioner $x = x(t)$ på intervallet $[0,1]$ er med de sædvanlige kompositioner $x+y = x(t)+y(t)$ og $x\cdot y = x(t)\cdot y(t)$ en ring $(M,+,\cdot)$. Mængden $\{x \mid x(0) = 0\}$ er et ideal i ringen, thi det er kerne for afbildningen $x \to x(0)$, ved hvilken $(M,+,\cdot)$ afbildes homomorft på $(\dot{R},+,\cdot)$.

Eksempel på ideal: Ringen $(\dot{Z},+,\cdot)$ betragtes. I AG II,3 er det vist, at udover identiteten er samtlige homomorfe afbildninger af $(\dot{Z},+,\cdot)$ netop afbildningerne på restklasseringene $(\dot{Z}_m,+,\cdot)$. Den tilsvarende kerne er mængden af multipla af m. Bortset fra nulidealet $\{0\}$ er et ideal i $(\dot{Z},+,\cdot)$ altså netop mængden af multipla af et naturligt tal m. Fællesmængden for idealerne svarende til $m = 2$ og $m = 5$ er idealet svarende til $m = 10$. Ved en homomorf afbildning af $\dot{Z}$ på $\dot{Z}_6$ vil idealet bestående af alle multipla af 9 afbildes på restklasserne med repræsentanter 0 og 3, og disse to restklasser udgør et ideal i $\dot{Z}_6$, nemlig kerne for en afbildning ved hvilken $\dot{Z}_6$ afbildes på $\dot{Z}_3$.

Ved et primideal forstås et ideal I, som er således beskaffent, at $ab \in I \Rightarrow a \in I \vee b \in I$. I en ring $(M,+,\cdot)$ er et ideal I et primideal hvis og kun hvis nulreglen gælder i kvotientringen $(M,+,\cdot)/I$. Det er klart, for lad φ være en homomorfi som har I

som kerne, så udtrykker betingelsen jo blot at $\varphi(ab) = 0 \Rightarrow \varphi(a) = 0 \vee \varphi(b) = 0$. Eksempel: I $(\dot{Z},+,\cdot)$ er de ikke-trivielle primidealer - af formen I = {multipla af p} hvor p er et primtal, svarende til at nulreglen gælder i restklasseringene $(\dot{Z}_p,+,\cdot)$.

Ved et <u>maximalideal</u> forstås et ideal som ved inklusionsordningen er maximalt blandt de ægte delidealer. Anderledes beskrevet vil I være et maximalideal i ringen M hvis og kun hvis $I \subset M$ og der ikke findes noget ideal I_o så $I \subset I_o \subset M$.

Der gælder den vigtige sætning: <u>Når $(M,+,\cdot)$ er en kommutativ ring med et etelement, så vil en kvotientring $(M,+,\cdot)/I$ være et legeme hvis og kun hvis I er maximalideal i ringen</u>.

Bevis: Lad I være kerne for homomorfien φ. Når $(M,+,\cdot)$ er kommutativ og har et etelelement, så vil kvotientringen have de samme egenskaber. Hvis I er et maximalideal, så vil det for ethvert $a \in M \setminus I$ gælde, at $\{ma+i \mid m \in M \wedge i \in I\}$ er lig hele M, thi denne mængde ses at opfylde Id1 og Id2 og er derfor et ideal, og den indeholder I (nemlig for m = 0) og den indeholder mere (nemlig i hvert fald a, som fås for i = 0 og m = etelementet); dette betyder, at for et vilkårligt $\varphi(a) \neq 0$ og et vilkårligt $\varphi(b) \in \varphi(M)$ findes et m så b = ma+i, hvoraf fås $\varphi(b) = \varphi(ma+i) = \varphi(m)\varphi(a)$, så at for $\varphi(a) \neq 0$ er division med $\varphi(a)$ altid mulig indenfor $\varphi(M)$. I dette tilfælde er kvotientringen altså et legeme, da den har mere end ét element (fordi I er en ægte del af M). Hvis I er lig hele M består kvotientringen kun af ét element, og er altså ikke noget legeme. Hvis endelig I ikke er maximalideal fordi der findes et ideal I_o, hvor $I \subset I_o \subset M$, så kan vi vælge et $a \in I_o \setminus I$, og så bliver $\{ma+i \mid m \in M \wedge i \in I\}$ åbenbart et delideal af I_o; for $b \notin I_o$ gælder altså for alle m, at $b-ma \notin I$, så at

$\varphi(b-ma) = \varphi(b)-\varphi(m)\varphi(a) \neq 0$ for alle $\varphi(m)$, hvilket viser, at i dette tilfælde er division med $\varphi(a)$ ikke altid mulig, til trods for at $\varphi(a) \neq 0$; i dette tilfælde er $\varphi(M)$ altså ikke et legeme. Sætningen er dermed bevist.

Hvis $(M,+,\cdot)$ er en kommutativ ring med etelement vil det samme gælde for billedringen, og de foregående sætninger viser så, at kvotientringen $(M,+,\cdot)/I$ er en integritetsring netop når I er primideal, og den er et legeme netop når I er maximalideal. Da et kommutativt legeme er en integritetsring ses, at under de nævnte forudsætninger vil ethvert maximalideal være et primideal (men det omvendte gælder ikke). Som eksempel kan man betragte ringen $\dot{Z} \times \dot{Z}$ af talpar $a = (a_1,a_2)$ med kompositionerne $a+b = (a_1+b_1,a_2+b_2)$ og $ab = (a_1b_1,a_2b_2)$; den er kommutativ og har etelelementet $(1,1)$. Mængden af talpar hvori $a_1 = 0$ udgør et primideal i den, og den tilsvarende kvotientring er isomorf med integritetsringen $(\dot{Z},+,\cdot)$ (nemlig med ringen dannet af førstekomponenterne a_1). Det er ikke noget maximalideal da der findes større idealer, f.eks. vil for ethvert $m \in \dot{N}$ mængden af talpar hvori a_1 blot er delelig med m udgøre et ideal, og den tilsvarende kvotientring er isomorf med $(\dot{Z}_m,+,\cdot)$; hvis m er et primtal p findes der ikke noget større ægte delideal i $\dot{Z} \times \dot{Z}$, og så har vi et maximalideal (som også er primideal) og den tilsvarende kvotientring er isomorf med legemet $(\dot{Z}_p,+,\cdot)$.

I en kommutativ ring med etelement vil vi ved det af elementet a frembragte hovedideal (a) forstå mængden af multipla af a, altså mængden af elementer b som kan skrives b = ax med et x ∈ ringen; denne mængde ses at være et ideal idet den opfylder Id1 og Id2, og den er netop det mindste ideal som indeholder a. At b er et multiplum af a udtrykkes ved skrivemåde a|b (læs "a går op i b"; ved betegnelsens anvendelse bør man naturligvis undgå forvekslingsmuligheder med prædikatstregen i mængdeklammer), og så er altså (a) lig mængden af elementer b, hvor a|b. (Man kan i en vilkårlig ring definere et hovedideal (a) som det mindste ideal der indeholder a, men må så blot være opmærksom på, at hvis der ikke findes et etelement vil a ikke være et multiplum af sig selv, og manglende kommutativitet vil også give vanskeligheder.)

Ved en hovedidealring forstås en integritetsring, i hvilken ethvert ideal er et hovedideal. Et eksempel er $(\dot{Z},+,\cdot)$, se side 5; nulidealet $\{0\}$ er trivielt lig (0).

I en hovedidealring er altså afbildningen $\varphi : a \to (a)$ en surjektiv afbildning af M på mængden af idealerne i M. Da $a|b \wedge b|c \Rightarrow a|c$ (gå-op-relationen er transitiv) vil $a|b \Rightarrow (a) \supseteq (b)$, og omvendt giver $(a) \supseteq (b)$ at $b \in (a)$, altså at a|b. Vi har altså at a|b er ensbetydende med $(a) \supseteq (b)$.

I den resterende del af denne paragraf skal vi interessere os for den multiplikative struktur af en hovedidealring $(M,+,\cdot)$, altså strukturen $(M\setminus\{0\},\cdot)$, idet vi ser bort fra det i denne forbindelse interesseløse nulelement.

Afbildningen φ er ikke injektiv, idet vi får $(a) = (b)$ hvis og kun hvis $a|b \wedge b|a$, hvilket ses at være ensbetydende med at $a = br$, hvor r er et regulært element. Elementer a og b som er forbundet på denne måde kaldes associerede, og de frembringer

altså det samme hovedideal. Associeret-relationen er åbenbart en ækvivalensrelation. I AG II,2,2 er det vist, at mængden af regulære elementer udgør en gruppe, som ses at være den største undergruppe i halvgruppen $(M\setminus\{0\},\cdot)$, og ækvivalensklasserne af associerede ses netop at være sideklasserne til denne undergruppe. Associerede elementer har de samme multipla, da de frembringer samme hovedideal, og de har også de samme divisorer, for da de gensidigt går op i hinanden vil alt hvad der går op i det ene af dem også gå op i det andet; de forholder sig altså ens m.h.t. deleligheds egenskaber. Som eksempel er i $(\check{Z},+,\cdot)$ mængden af regulære elementer lig $\{1,-1\}$, og et par $\{a,-a\}$ udgør en klasse af associerede, og det, at man ved en undersøgelse af de hele tals multiplikative struktur betragter en sådan klasse under ét betyder, at man "ser bort fra fortegnet".

Idealet (a) er en ægte del af (b) hvis og kun hvis $a = bc$, hvor c er et ikke-regulært element, og specielt vil ethvert ægte delideal af M være frembragt af en klasse ikke-regulære elementer. Det følger umiddelbart af det foregående. Et ikke-regulært a kaldes <u>reducibelt</u> hvis det kan skrives som produkt $a = bc$ af to ikke-regulære elementer, og i modsat fald kaldes det <u>irreducibelt</u>, og af det foregående fremgår, at <u>a er irreducibel netop når (a) er et maximalideal</u>. Eksempel: Indenfor hovedidealringen $(\check{Z},+,\cdot)$ er de irreducible elementer netop $\pm p$, hvor p er <u>primtal</u>, og de reducible er $\pm m$, hvor m er et <u>sammensat</u> tal.

<u>Ethvert primideal i en hovedidealring er et maximalideal eller et af de trivielle idealer</u>. Bevis: Et ideal frembragt af et regulært element er hele M, som trivielt er primideal. Et ideal frembragt af 0 er nulidealet, som er primideal ifølge nulreglen. Et ideal frembragt af et irreducibelt element er maximalideal, og

derfor primideal (se side 7). Endelig er et ideal frembragt af et reducibelt element a = bc, hvor b og c er ikke-regulære, ikke maximalideal, men det er heller ikke primideal, thi det indeholder a uden at indeholde nogen af faktorerne b eller c.

Af sætningen følger umiddelbart, at hvis en hovedidealring afbildes homomorft, men ikke isomorft, ind i en integritetsring, og billedringen har mere end ét element, så er den et legeme. Thi da hovedidealringen er kommutativ og har etelement, gælder det samme for billedringen, og når billedet ligger i en integritetsring gælder nulreglen også; billedet er derfor selv en integritetsring. Men så er afbildningens kerne et primideal, og idet de to trivielle muligheder for dette er udelukket, må det være et maximalideal, og billedet er derfor et legeme. Trivielt eksempel: Hovedidealringen $(\dot{Z},+,\cdot)$ afbildes homomorft, og når de to trivielle muligheder udelukkes, bliver billedet en restklassering $(\dot{Z}_m,+,\cdot)$ hvor $m > 1$; hvis billedet skal ligge i en integritetsring må nulreglen gælde, og så må m være primtal, men så er billedet også et legeme $(\dot{Z}_p,+,\cdot)$.

En hovedidealring har to vigtige egenskaber: Den opstigende kædes egenskab og fællesmålsegenskaben.

Den opstigende kædes egenskab: En følge af idealer $I' \subsetneq I'' \subsetneq \cdots \subsetneq I^{(n)} \subsetneq \cdots$ er sluttelig stationær, d.v.s. at fra et vist trin er idealerne ens.

Bevis: Vi skal først vise, at $I = \bigcup I^{(j)}$ er et ideal, og det gøres let ved at eftervise Id1 og Id2: når $x,y \in I$ vil der tilstrækkelig langt fremme i kæden findes et $I^{(n)}$ som de begge tilhører, men så vil deres sum også tilhøre $I^{(n)}$ og dermed I; når $x \in I$ vil det tilhøre et $I^{(n)}$, og så vil alle multipla af x til-

høre $I^{(n)}$ og dermed I. Men når I er et ideal i en hovedidealring er det mængden af multipla af et frembringerelement a, og blandt disse forekommer a selv, og der findes altså et k, så $a \in I^{(k)}$, men så vil også $I = (a) \subseteq I^{(k)}$, og idealerne i kæden er altså ens fra og med $I^{(k)}$.

Oversættes idealinklusionen til gå-op-relationen udsiger egenskaben: Hvis man i en hovedidealring har en følge af elementer, hvor ethvert går op i det foregående, så er fra et vist trin alle elementerne associerede.

Lad os betragte et ikke-regulært element. Enten er det irreducibelt, eller også kan det skrives som produkt af to ikke-regulære; lad os betragte en af disse, enten er den irreducibel, eller også kan den skrives som produkt af to ikke-regulære; lad os betragte en af disse, o.s.v.. Ifølge kædeegenskaben må processen standse, hvilket kun kan ske ved at vi har mødt en irreducibel faktor, og ethvert ikke-regulært element er altså deleligt med en sådan. Lad os så gentage processen, men således at vi først uddrager den irreducible faktor, dernæst igen en irreducibel faktor o.s.v., og ifølge kædeegenskaben må processen igen standse. Dermed har vi vist, at i en hovedidealring kan ethvert element som ikke er 0 eller regulært skrives som et produkt (med 1 eller flere faktorer) af irreducible. Anvendt på $(\dot{Z},+,\cdot)$ viser det, at ethvert fra 0 forskelligt helt tal kan skrives som $\pm$ et produkt (med 0 eller 1 eller flere faktorer) af primtal.

Fællesmålsegenskaben: Til to elementer a og b findes altid et d (kaldet et "største fælles mål for a og b"), så for alle c gælder

$$c \mid a \wedge c \mid b \iff c \mid d,$$

og mængden af de d som opfylder betingelsen udgør en klasse af

associerede. Egenskaben udsiger altså, at mængden af fælles divisorer ("mål", et udtryk fra Euklid) for a og b netop er samtlige divisorer i et vist d (som selv er fælles divisor, og en "største" i en ved gå-op-relationen defineret partiel ordning).

Oversættes gå-op-relationen til idealinklusion udsiger egenskaben: Til to idealer (a) og (b) findes netop ét ideal (d), så $(c) \supseteq (a) \wedge (c) \supseteq (b) \iff (c) \supseteq (d)$. Så er beviset trivielt, idet vi som (d) blot benytter fællesmængden for de idealer (c) der indeholder både (a) og (b), thi ifølge en tidligere sætning (side 4) er denne fællesmængde selv et ideal.

Idealet (d) er det mindste ideal som indeholder idealerne (a) og (b), hvilket ses at være ensbetydende med, at det er det mindste ideal, som indeholder elementerne a og b, og i analogi med hovedidealbetegnelsen skriver man nu (d) = (a,b). Man tillader sig dog ofte også at lade betegnelsen (a,b) stå for et vilkårligt frembringerelement d for dette ideal, med andre ord: (a,b) kan stå for et - pånær associering entydig bestemt - største fælles mål for a og b. Indenfor $(\dot{Z},+,\cdot)$ skrives f.eks. (-6,9) = 3.

Multiplikation er distributiv m.h.t. (a,b)-dannelse, hvormed vi mener, at (ma,mb) = m(a,b). Lad os betegne (a,b) som d og (ma,mb) som D. Da d går op i a og b, vil md gå op i ma og mb, og er altså en fælles divisor for dem, og ifølge fællesmålsegenskaben vil md gå op i D, så at D kan skrives som mdx. Når mdx går op i ma vil dx gå op i a, og analogt ses, at dx går op i b, hvorefter fællesmålsegenskaben viser, at dx går op i d. Altså er x regulær, så at D og md er associerede, hvilket skulle vises.

Dersom $c \mid ab$, da kan c skrives på formen c = fg, hvor $f \mid a$ og $g \mid b$. Vi vælger f = (a,c), hvormed er opnået at $f \mid a$, og da $f \mid c$ kan c skrives på formen fg. Da c = fg er divisor i ab, og desuden er divisor i cb (trivielt), vil ifølge fællesmålsegenskaben

$fg \mid (ab,cb) = (a,c)b = fb$, hvoraf ses, at $g \mid b$, hvormed påstanden er vist. Dersom c går op i et produkt af t faktorer, da kan c skrives på formen $c_1 c_2 \cdots c_t$, hvor c_1 går op i den første af faktorerne, c_2 går op i den anden, o.s.v. Dersom $c_1 c_2 \cdots c_s = a_1 a_2 \cdots a_t$, er det muligt at foretage en videreopløsning af faktorerne på begge sider af lighedstegnet, indtil man opnår, at der står de samme faktorer på begge sider; det ses, idet man først opløser c_1 i t faktorer som hver går op i et a, så bortforkorter disse faktorer, dernæst behandler c_2 på samme måde, o.s.v. Specielt følger heraf, at hvis to produkter af irreducible elementer har den samme værdi, så må de - bortset fra associering - bestå af de samme faktorer.

Kombineres dette resultat med slutkonsekvensen af den opstigende kædes egenskab, får man hovedsætningen:

I en hovedidealring kan ethvert element, som ikke er 0 eller regulært, skrives som produkt (med 1 eller flere faktorer) af irreducible. Og denne produktfremstilling er entydig, bortset fra faktorernes rækkefølge, og bortset fra associering.

Hvis man betragter de positive elementer i hovedidealringen $(\dot{Z},+,\cdot)$ er de irreducible netop primtallene, og man får den såkaldte talteoriens hovedsætning: Ethvert naturligt tal kan, og bortset fra faktorernes rækkefølge kun på én måde, skrives som produkt (med 0 eller 1 eller flere faktorer) af primtal.

Hvis det samme irreducible element forekommer flere gange, eller blot nogle associerede, i en sådan produktfremstilling, kan det samles til en potens, evt. multipliceret med et regulært, og for et vilkårligt element a (ikke 0 eller regulært) får vi en fremstilling $a = r \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$, hvor r er regulær og $p_1, p_2, \ldots$ er irreducible og exponenterne α_j er naturlige tal. I denne fremstilling kan

man gerne formelt tilføje 0-te potenser af andre irreducible. Hvis man har to elementer a og c kan man på denne måde udtrykke dem ved potenser af de samme irreducible $p_1,\cdots,p_s$, og lad exponenterne hedde hhv. $\alpha_1,\cdots$ og $\gamma_1,\cdots$. En nødvendig og tilstrækkelig betingelse for at $c|a$ bliver så, at man for alle par af tilsvarende exponenter har $\gamma_j \leqq \alpha_j$.

Hvis man har to elementer a og b, og de er fremstillet på den nævnte måde med exponenterne hhv. $\alpha_1,\cdots$ og $\beta_1,\cdots$, så følger af det ovenstående, at et "største" fællesmål $d = (a,b)$ for dem er givet ved $d = p_1^{\delta_1}\cdots p_s^{\delta_s}$, hvor $\delta_j = \min\{\alpha_j,\beta_j\}$, og et "mindste" fælles multiplum af dem er givet ved $f = p_1^{\varphi_1}\cdots p_s^{\varphi_s}$, hvor $\varphi_j = \max\{\alpha_j,\beta_j\}$. Da $\min\{\alpha,\beta\} + \max\{\alpha,\beta\} = \alpha + \beta$, bliver $p_j^{\alpha_j}\cdot p_j^{\beta_j} = p_j^{\delta_j}\cdot p_j^{\varphi_j}$, hvoraf følger, at $ab = df$, altså at <u>produktet af to elementer er lig produktet af en "største" fælles divisor og et "mindste" fælles multiplum for dem</u>.

Som tidligere antydet refererer gloserne "største" og "mindste" til den partielle ordning som defineres ved gå-op-relationen; indenfor de naturlige tal vil $a|b$ imidlertid medføre $a \leqq b$, og i dette talområde bliver der derfor virkelig tale om største fælles divisor og mindste fælles multiplum ved den sædvanlige størrelsesordning. Eksistensen af et "største" fællesmål og et "mindste" fælles multiplum for to elementer (og dermed for et vilkårligt endeligt antal) betyder, at der for en mængde af to (eller blot endelig mange) elementer i en hovedidealring vil findes både en nedre grænse og en øvre grænse i den ved gå-op-relationen definerede partielle ordning. Noget sådant gælder ikke i almindelighed ved en partiel ordning (ΛG I,5,26-28).

Vi kan få karakteristiske eksempler ved at betragte et par delringe af de komplexe tals legeme $(\dot{C},+,\cdot)$:

Ved Gauss' ring (Gauss 1777-1855) forstås mængden $\dot{Z}[i] = \{a+ib \mid a,b \in \dot{Z}\}$. I det sædvanlige Wessel-diagram er det geometriske billede af $\dot{Z}[i]$ mængden $\dot{Z} \times \dot{Z}$ af gitterpunkter med heltallige koordinater. Hvis to elementer tilhører $\dot{Z}[i]$, vil både deres sum og deres produkt atter tilhøre $\dot{Z}[i]$, hvilket viser, at $\dot{Z}[i]$ er en delring af $(\dot{C},+,\cdot)$; da den indeholder tallet 1 er den en integritetsring. For de komplexe tal og deres numeriske værdi er som bekendt afbildningen $x \to |x|$ en homomorf afbildning af $(\dot{C},\cdot)$ ind i $(\dot{R},\cdot)$. Af Wessel-diagrammet er det klart, at de fra 0 forskellige elementer af $\dot{Z}[i]$ alle har en numerisk værdi som er større end eller lig 1, og den er kun lig 1 for elementerne $+1,-1,i,-i$; disse fire er regulære, og der kan ikke være andre regulære, da et produkt hvori et andet element indgår får en numerisk værdi, som er større end 1. Vi skal nu vise, at $\dot{Z}[i]$ er en hovedidealring: Lad I være et egentligt ideal i den, og lad $d \neq 0$ være et element fra I med minimal numerisk værdi; et sådant eksisterer åbenbart (Wessel-diagrammet !). Lad c være et vilkårligt element $\in$ I, så vil vi vise, at c er et multiplum af d, hvoraf følger, at I netop er hovedidealet (d). Vi har $cd^{-1} \in \dot{C}$, og antages, at $cd^{-1} \notin \dot{Z}[i]$ findes der et $f \in \dot{Z}[i]$, så $0 < |cd^{-1}-f| \leq 1/\sqrt{2} < 1$ (Wesseldiagrammet !), hvoraf følger, at $0 < |c-fd| < |d|$, hvilket strider mod at c-fd ifølge betingelserne Id1 og Id2 også tilhører I, samtidig med at d havde minimal numerisk værdi. Dermed er vist, at Gauss' ring er en hovedidealring. En klasse associerede i $\dot{Z}[i]$ består af fire elementer, f.eks. $\{\pm(3+i),\pm(1-3i)\}$. Elementet 3+i er reducibelt, da $3+i = (1+i)(2-i)$. Elementet 2-i er irredu-

cibelt, for dets numeriske værdi er $\sqrt{5}$, og hvis det var reducibelt skulle det være produkt af to elementer, hvis numeriske værdi lå mellem 1 og $\sqrt{5}$, og det er åbenbart umuligt.

Vi kan let angive en analog ring, som ikke er hovedidealring, nemlig $\dot{Z}[2i] = \{a+2ib \mid a,b \in \dot{Z}\}$ (tegn Wesseldiagrammet !). Det er åbenbart også en integritetsring. De eneste regulære elementer er +1 og -1. Elementerne ± 2 og $\pm 2i$ er irreducible (tænk på deres numeriske værdi og Wesseldiagrammet !), og de er ikke associerede. Da $-4 = (2i)^2 = -2 \cdot 2$ er fremstillingen som produkt af irreducible ikke entydig, og $\dot{Z}[2i]$ kan derfor ikke være en hovedidealring (men den geometriske betragtning, som ovenfor anførte til et tal mindre end 1, nemlig $1/\sqrt{2}$, vil jo også svigte).

At den entydige primopløsning i halvgruppen $(\dot{N},\cdot)$ langtfra er nogen trivialitet fremgår måske endnu mere slående af Hilbert's Eksempel (Hilbert 1862-1943): Sædvanlige hele positive tal af form $4h+1$ udgør med multiplikation en halvgruppe. I denne er $5,9,13,17,21,29,\ldots$ "irreducible", medens $25 = 5 \cdot 5$, $45 = 5 \cdot 9, \ldots$ er "reducible". Der gælder ikke entydig primopløsning, idet f.eks. $21 \cdot 21 = 9 \cdot 49$, og fællesmålsegenskaben gælder ikke, idet f.eks. de fælles divisorer for 189 og 441 er 1,9,21. (Men eksemplet er svagere end det foregående, da der jo ikke er addition i denne struktur).

Det må betones, at definitionerne af regulære, reducible og irreducible elementer og af associerede er gyldige i en vilkårlig integritetsring. Dersom det i en integritetsring gælder, at ethvert fra 0 forskelligt element på en og kun én måde (bortset fra faktorernes rækkefølge og associering) kan skrives som produkt af irreducible, vil vi sige, at ringen har entydig faktorisering; i så fald gælder de side 3,13-14 anførte resultater.

Vi har vist, at en hovedidealring har entydig faktorisering. Side 3,16 viser en integritetsring, som ikke er hovedidealring, og som ikke har entydig faktorisering. Vi skal senere møde en integritetsring (mængden af polynomier i to variable), som ikke er hovedidealring, men dog har entydig faktorisering.

Mængden af de på en åben cirkelskive A holomorfe funktioner udgør med sædvanlig regning en integritetsring; de regulære elementer er de nulpunktsfri funktioner, og de irreducible er funktionerne med netop ét nulpunkt som er af første orden; i ringen er faktorisering ikke altid mulig, idet en funktion med uendelig mange nulpunkter i A ikke kan skrives som produkt af irreducible. Ringens brøklegeme er mængden af de på A meromorfe funktioner.

Ethvert element i brøklegemet for en integritetsring $(I,+,.)$ kan skrives som brøk $\frac{a}{b}$, hvor $a,b \in I$; man ser, at hvis I har entydig faktorisering kan elementet på en og væsentlig kun én måde skrives som en uforkortelig brøk, hvormed menes, at a og b kun har regulære faktorer fælles, og at de er bestemt entydigt pånær regulære faktorer.

Lad der være givet en ring og i denne to idealer, I_1 og I_2. Ved idealsummen $I_1 + I_2$ forstås mængden af elementer af formen i_1+i_2 , hvor $i_1 \in I_1$ og $i_2 \in I_2$; der gælder, at idealsummen I_1+I_2 er et ideal, og netop det mindste ideal, som indeholder I_1 og I_2. Thi den opfylder Id1, da den er stabil overfor subtraktionen idet $(i_1'+i_2') - (i_1''+i_2'') = (i_1'-i_1'') + (i_2'-i_2'')$, og den opfylder Id2, hvilket ses af omskrivningerne $x(i_1+i_2) = (xi_1) + (xi_2)$ og $(i_1+i_2)x = (i_1x) + (i_2x)$, og det er klart, at den indeholder både I_1 og I_2 (da 0 er indeholdt i ethvert ideal), og et ideal, som indeholder disse kan ikke være mindre, da det skal være en additiv gruppe.

Vi har i det foregående mødt flere eksempler på denne idealsum, således ved beviset for sætningen om maximalideal (s. 6), hvor vi for et ideal I i en ring $(M,+,\cdot)$ med etelement betragtede $\{ma+i \mid m \in M \wedge i \in I\}$, som ses at være idealsummen (a)+I, og endvidere ved beviset for fællesmålsegenskaben (s. 12), hvor vi mødte det mindste ideal (d), som indeholder to idealer (a) og (b), og hvor altså (d) = (a) + (b).

Dannelsen af idealsummen er en komposition indenfor mængden af idealer i en ring, og man ser umiddelbart, at den er kommutativ, fordi ringadditionen er kommutativ, og endvidere er den associativ, idet $I_1+I_2+I_3$, uanset hvorledes man sætter parenteser, vil blive det mindste ideal, som indeholder I_1 , I_2 og I_3 . Det giver ingen mening at ville forsøge en subtraktion, idet f. eks. ligningen $X + I_o = I_o$ som løsning X har ethvert delideal i I_o.

Idealsummer kan indgå i mange formler. Som eksempel kan nævnes, at

$$(I_1 + I_2)/I_1 \approx I_2/(I_1 \cap I_2),$$

hvor $\approx$ betyder, at de to kvotientringe, hvori kompositionsangivelserne er udladt, er isomorfe, (og de er endda på naturlig måde "identiske"). Bevis: I_1 er kerne for en homomorfi φ af hele ringen, og betragtes restriktionen af φ til I_1+I_2, (som jo er en delring), vil kernen stadig være I_1, og billedringen er en realisation af formlens venstre side; billederne er af formen $\varphi(i_1+i_2) = \varphi(i_1) + \varphi(i_2) = \varphi(i_2)$. Betragtes den yderligere restriktion af φ til I_2, vil billedringen være uforandret, idet den stadig består af alle elementerne $\varphi(i_2)$, medens kernen nu er indskrænket til $I_1 \cap I_2$, og billedringen er altså nu formlens højre side, hvormed rigtigheden er eftervist. Taleksempel: Indenfor $(\check{Z},+,\cdot)$ betragtes idealerne (2) og (5); idealsummen er (1) (største fælles divisor !), og fællesmængden er (10); formlen giver så (idet kompositionsangivelserne medtages), at $((1),+,\cdot)/(2) = ((5), +, \cdot)/(10)$, hvilket jo også er rigtigt, da begge sider angiver en ring med to elementer.

Den kinesiske restklassesætning: Lad $(M, +, \cdot)$ være en kommutativ ring med etelement, og lad $I_1, I_2, \ldots, I_n$ være idealer, som er kerner for homomorfier, hhv. $\varphi_1, \varphi_2, \ldots, \varphi_n$. Dersom $k \neq j$ medfører, $I_k+I_j = M$, så vil der for ethvert sæt $(a_1, \ldots, a_n)$ af elementer fra M findes et $b \in M$, således at $(\varphi_1(b), \ldots, \varphi_n(b)) = (\varphi_1(a_1), \ldots, \varphi_n(a_n))$.

Sætningen udsiger altså, at ethvert element i værdimængden for afbildningen $(a_1,\ldots,a_n) \to (\varphi_1(a_1),\ldots,\varphi_n(a_n))$ vil antages for et element på diagonalen i originalmængden. Det pågældende b er ikke entydigt bestemt, men kun pånær en addend, som tilhører $\cap I_j$, thi en sådan vil jo afbildes i $(0,\ldots,0)$.

Bevis: Det vil være tilstrækkeligt at vise, at vi for ethvert j kan finde et b_j, således at $b_j - a_j \in I_j$, medens $k \neq j$ medfører $b_j \notin I_k$. Thi så er jo $\varphi_j(b_j) = \varphi_j(a_j)$ medens $k \neq j$ medfører $\varphi_k(b_j) = 0$, og så kan vi som b benytte summen af alle b_j, idet

$$\varphi_k(\Sigma_j b_j) = \Sigma_j \varphi_k(b_j) = \varphi_k(b_k) = a_k ,$$

da der i den optrædende sum kun kommer ét bidrag, nemlig for $j = k$. Vi holder nu j fast og efterviser det omtalte b_j. Ifølge forudsætning vil $k \neq j$ medføre $I_k + I_j = M$, og specielt kan altså etelementet skrives $e = i_k + i_j^{(k)}$, hvor det første led tilhører I_k og det andet I_j. Vi sætter så

$$b_j = a_j \prod_{k \neq j} i_k = a_j \prod_{k \neq j} (e - i_j^{(k)});$$

af det første produkt ses, at b_j indeholder en faktor i_k, og ifølge Id2 tilhører det så idealet I_k, og af det andet produkt ses, at b_j er lig a_j plus en sum af produkter, som alle indeholder en eller flere faktorer $i_j^{(k)}$, og ifølge Id2 og Id1 tilhører $b_j - a_j$ altså I_j. Dermed er sætningen vist.

En nærliggende anvendelse af den kinesiske restklassesætning er på ringen $(\dot{Z},+,\cdot)$. Et ideal er her af formen (m), og det er kerne for en homomorfi $\dot{Z} \to \dot{Z}_m$, og betingelsen $I_k + I_j$ lig ringen bliver til $(m_k) + (m_j) = (1)$, altså at $(m_k, m_j) = 1$. Vi får altså, at hvis $m_1, m_2, \ldots, m_n$ er parvis indbyrdes primiske hele tal, så vil der for ethvert sæt $a_1, a_2, \ldots, a_n$ af hele tal findes tal b, som ved division med $m_1, \ldots, m_n$ giver rester hhv. $a_1, \ldots, a_n$; disse b er bestemt pånær et multiplum af produktet $m_1 m_2 \ldots m_n$. Det sidste følger af en bemærkning ovenfor, idet idealernes fællesmængde jo netop består af de nævnte multipla. Taleksempel: Der findes tal, som ved division med 2,3 og 5, giver resterne hhv. 1,0 og 2, nemlig netop de tal, som ved division med 30 giver resten 27.

Eksempel til den kinesiske restklassesætning: De reelle funktioner tilhørende C^∞ på $[0,1]$ udgør med addition og multiplication en ring, kommutativ og med etelement (funktionen som er identisk lig 1). Den har også den egenskab, at i ringen er enhver nulpunktsfri funktion regulær. Mængden af funktioner, for hvilke $f(0), f'(0), f''(0), \ldots$, alle er lig 0, udgør et ideal I_0 i ringen, da de opfylder Id1 og Id2 (det sidste på grund af de Leibniz'ske formler for differentialkvotienterne af et produkt); det er kerne for en homofi φ_0

ved hvilken $f(t)$ går over i følgen $f(0),f'(0),f''(0),\ldots$, og additionen går over i komponentvis addition, og multiplikationen går over i den ved de Leibniz'ske formler bestemte komposition. Idealet er ikke trivielt, thi som bekendt indeholder det en funktion $a(t)$, der er positiv på $(0,1]$ (nemlig e^{-1/t^2}, plomberet i $t = 0$). Funktionerne, for hvilke $f(1),f'(1),f''(1),\ldots$, alle er lig 0, udgør et tilsvarende ideal I_1, og dette indeholder en funktion $b(t)$, som er positiv på $[0,1)$. Summen $I_0 + I_1$ udgør hele ringen, da en vilkårlig funktion $k(t)$ fra den kan skrives på formen

$$k(t) = \frac{k(t)}{a(t)+b(t)} \cdot a(t) + \frac{k(t)}{a(t)+b(t)} \cdot b(t)$$

hvori $a(t)+b(t)$ er positiv på $[0,1]$, således at begge brøkerne tilhører C^∞, og første led derfor tilhører I_0 og andet I_1. Den kinesiske restklassesætning viser så, at dersom $f(t)$ og $g(t)$ er C^∞-funktioner på $[0,1]$, så findes der en C^∞-funktion $h(t)$, for hvilken man for alle $j \geq 0$ har $h^{(j)}(0) = f^{(j)}(0)$ og samtidig $h^{(j)}(1) = g^{(j)}(1)$. (Det kan iøvrigt uden bevis bemærkes, at man som følge $f^{(j)}(0)$, $j \in \mathbb{N}_0$ kan benytte en vilkårlig talfølge, og altså tilsvarende for følgen $g^{(j)}(1)$, og to sådanne helt vilkårlige "funktionselementer" kan altså altid sammenføjes med en C^∞-funktion).

Øvelser til § 3.

1) Lad $(M,+,\cdot)$ være en ring. Gør rede for at mængden af samtlige automorfier af $(M,+,\cdot)$ udgør en gruppe (ringens "automorfigruppe"), som er undergruppe i den fuldstændige transformationsgruppe for mængden M.

Lad $a \in M$ være et element, som har et inverst a^{-1}. Vis, at afbildningen $x \to a \cdot x \cdot a^{-1}$ er en automorfi af $(M,+,\cdot)$ (en "indre automorfi").

Vis, at mængden af indre automorfier udgør en normal undergruppe i ringens automorfigruppe.

2) Lad $(M,+,\cdot)$ være en (ikke-kommutativ) ring. Vis, at der findes et mindste ideal I så $xy - yx \in I$ for alle $x,y \in M$, og gør rede for at dette er det mindste ideal I, for hvilket $(M,+,\cdot)/I$ bliver kommutativ.

3) Lad $(M,+,\cdot)$ være en kommutativ ring, der kun har trivielle idealer. Vis, at enten er den et legeme, eller også er alle produkter i den lig 0.

4) Lad $(M,+,\cdot)$ være kommutativ ring. Vis, at mængden af de nilpotente elementer udgør et ideal I (nilpotent defineret i §2, øv. 3). Vis, at faktorringen M/I ikke har andre nilpotente elementer end nulelementet.

5) Lad $(M,+,\cdot)$ være ringen af 2×2-matricer over $(\dot{Z},+,\cdot)$ med sædvanlig matrixregning. I M betragtes delmængderne

A = mængden af matricer $\begin{pmatrix} x & y \\ y & x \end{pmatrix}$

B = ... $\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}$

C = ... $\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$.

1) Vis, at disse er delringe af $(M,+,\cdot)$.

2) Vis at mængden af 2 x 2-matricer over de lige tal er et ideal I i $(M,+,\cdot)$.

3) Vis, at $I \cap A$ er et ideal i A; formuler og bevis en hertil svarende general sætning.

   En homomorfi med kerne I fører M over i en ring M_2, og fører A, B og C over i delringe A_2, B_2 og C_2 af denne. Disse kan repræsenteres ved at man i matricerne ovenfor lader elementerne være restklasser modulo 2.

4) Vis, at de additive grupper for A_2, B_2 og C_2 alle er isomorfe med den ikke-cykliske gruppe af orden 4.

5) Hvilke af ringene A_2, B_2 og C_2 har et etelement ?

6) Er nogen af dem en integritetsring ?

7) Vis, at A_2 og B_2 er isomorfe.

8) Giv et eksempel på en ikke-kommutativ ring med 4 elementer, som ikke er isomorf med A_2, B_2 eller C_2 (en sådan, D_2, kan let fås udfra C_2 !).

9) Giv eksempler på ringe med 4 elementer, som ikke er isomorfe med A_2, B_2, C_2 eller D_2.

10) Hvor mange ikke-isomorfe ringe med 4 elementer findes ?

6) Man betragter ringen $(M,+,\cdot)$ af kontinuerte reelle funktioner $x = x(t)$ på $0 \leq t \leq 1$ (se tekstens s.5). Vis, at følgende tre mængder er idealer, og undersøg hvilke af dem, der er hovedidealer:

$$I_1 = \{x(t) \mid x(t) = 0 \text{ for alle } t \text{ i en omegn af } t = 0\},$$

$$I_2 = \{x(t) \mid x(0) = 0\},$$

$$I_3 = \{x(t) \mid x(0) = 0 \wedge x(t) \text{ differentiabel i } t = 0\}.$$

7) Lad $(M,+,\cdot)$ være den i forrige øvelse betragtede ring, og $I = I_a = \{x(t) \mid x(a) = 0\}$, $a \in [0,1]$.
I er et ideal; eftervis, at det er et maximalideal.
Vis omvendt med benyttelse af Borel's overdækningssætning, at ethvert maximalideal er et ideal af formen I_a (vis, at hvis et ideal for ethvert a indeholder et $x(t)$ så $x(a) \neq 0$, så indeholder det et $x(t)$ som er $\neq 0$ for alle $t \in [0,1]$, hvoraf følger, at ethvert ægte delideal af M er indeholdt i et I_a).

8) Man betragter ringen af $n \times n$-matricer over $\mathbb{Q}$ med lutter 0 under diagonalen (smlgn. §2, øv. 3). Vis, at delmængden M_j bestående af matricer hvori $a_{jj} = 0$, udgør et ideal i ringen, og vis, at dette er et maximalideal. Eftervis, at der ikke findes andre maximalidealer end de nævnte ($1 \leq j \leq n$), og bestem derved samtlige homomorfier af $(M,+,\cdot)$ ind på $(\mathbb{Q},+,\cdot)$.

9) $(M,+,\cdot)$ er ringen af $n \times n$-matricer over $\mathbb{Q}$ med sædvanlig matrixregning. Vis, at der i ringen kun findes de to trivielle idealer (vis først, at hvis I indeholder $\underline{\underline{A}}$, så indeholder I den matrix, der fremgår af $\underline{\underline{A}}$ ved at erstatte alle elementer på nær et enkelt med 0; vis dernæst, at ved operationer indenfor I kan dette element flyttes hen på en vilkårlig plads i matricen). Vis, at der findes ikke-trivielle højre-idealer i ringen, hvormed menes delmængder af ringen som opfylder Id 1 og den første af betingelserne i Id 2.

10. Lad $(M,+,\cdot)$ være en kommutativ ring og I et ideal i ringen. Ved "radikalet" rad(I) forstås mængden $\bigcup_{n\in\mathbb{N}}\{a|a^n \in I\}$.
Vis, at rad(I) er et ideal.
Vis endvidere, at rad(rad(I)) = rad(I) og at $\text{rad}(I_1 \cap I_2) = \text{rad}(I_1) \cap \text{rad}(I_2)$.
Hvad bliver billedet af rad(I) ved den homomorfe afbildning med kernen I af ringen $(M,+,\cdot)$ på M/I ?
Det er klart, at $I \subsetneq \text{rad}(I)$; giv et eksempel på et ideal I i ringen $(\dot{Z},+,\cdot)$, således at I er en ægte delmængde af sit radikal.

11. Lad f være en homomorf afbildning af en ring $(M,+,\cdot)$, og lad I være homomorfiens kerne. Vis, at en delring af M afbildes i en delring af M/I og, at et ideal i M afbildes i et ideal i M/I. Vis, at afbildningen giver enentydig forbindelse mellem ringene M_1, hvor $I \subsetneq M_1 \subsetneq M$ og delringene af M/I, og enentydig forbindelse mellem idealerne I_1, hvor $I \subsetneq I_1 \subsetneq M$ og idealerne i M/I, og endda således, at vi med et "naturligt" valg af betegnelserne får $M/I_1 = (M/I)/(I_1/I)$ (smlgm.§2,øv. 22).

12. Lad $(M,+,\cdot)$ være en kommutativ ring og I_1 og I_2 to idealer i ringen. Vis, at mængden $\bigcup_{a_2\in I_2}\{x|xa_2 \in I_1\}$ er et ideal i ringen ("idealkvotienten" $I_1 : I_2$).
Giv ved hjælp af idealer af formen $\dot{Z}_m$ i ringen $(\dot{Z},+,\cdot)$ ekdempler på, at samme kvotientideal $(I_1 : I_2)$ kan for samme I_1 fremkomme ved forskellige I_2, og for samme I_2 kan det fremkomme ved forskellige I_1.

13. Vis, at mængden af komplekse tal $M = \{\frac{a + b\sqrt{-3}}{2}\}$, hvor $a,b \in \mathbb{Z}$ og a+b er lige, med sædvanlig addition og multiplikation udgør en ring. Vis, at $I = \{a + b\sqrt{-3}\}$, hvor $a,b \in \mathbb{Z}$ og a+b er lige, er et ideal i denne; er det et hovedideal ? Hvor mange elementer indeholder faktorringen M/I ? Vis, at nulreglen gælder i faktorringen, og dermed at denne er et legeme.

Bestem samtlige automorfier af M/I.

14. Man betragter ringen af kontinuerte funktioner x(t) på intervallet [0,1] med sædvanlig addition og multiplikation. Angiv mængden E af regulære elementer. Eftervis, at der ikke findes irreducible elementer. Find de fælles divisorer for $x(t) = t$ og $y(t) = t \sin \frac{1}{t}$, og vis derved, at ringen ikke har fællesmålsegenskaben.

15. Man betragter ringen af differentiable funktioner x(t) på intervallet [0,1] med sædvanlig addition og multiplikation. Angiv mængden E af regulære elementer. Vis, at ringen ikke har den opstigende kædes egenskab, men at der dog findes irreducible elementer. Vis, at de irreducible elementer netop er de x(t), som kun har et nulpunkt t_o, og som i omegnen af dette er således at $x(t)/(t - t_o)^2$ er divergent for $t \to t_o$.

16. Vis, at dersom der for et integritetsring gælder hovedsætningen om den entydige og altid mulige fremstilling som produkt af irreducible, så har integritetsring både fællesmålsegenskaben og den opstigende kædes egenskab (men det behøver ikke at være en hovedidealsring, smlgm. §5).

17. Lad $(M,\cdot)$ være en mængde med en komposition (betegnet multiplikation) som er associativ og kommutativ, og med et etelement, men ingen andre regulære elementer, og hvori divisionen er højst entydig (men ikke altid mulig). Ved fællesmultiplumsegenskaben forstår vi: Til to elementer a og b findes altid et m, (kaldet "mindste fælles multiplum for a og b"), så $a|g \wedge b|g \iff m|g$ for alle g.
Vis, at $(M,\cdot)$ vil have fællesmultiplumsegenskaben hvis, og kun hvis, den har fællesmålsegenskaben, og vis samtidig, at multiplikationen er distributiv m.h.t. mindste-fælles-multiplumsdannelsen.

18. Lad M være mængden bestående af de rationale tal, derkan skrives som en brøk, hvis tæller og nævner er hele tal, og hvori nævneren er en potens af 2. Vis, at $(M,+,\cdot)$ er en delring af $(\mathbb{Q},+,\cdot)$.
Bestem samtlige regulære elementer i $(M,+,\cdot)$.
Bevis, at $(M,+,\cdot)$ er en hovedidealring, og angiv frembringerelementer for idealerne. Angiv samtlige reducible og samtlige irreducible elementer i M.

19. Lad $(M,+,\cdot)$ være en integritetsring. Vis, at mængden K af ikke-regulære elementer i M er identisk med foreningsmængden af samtlige ægte delidealer i M.
Vis, at dersom K er en delring af $(M,+,\cdot)$, så er K et ideal, og at der yderligere i dette tilfælde gælder, at kvotientringen $(M,+,\cdot)/K$ er et legeme.
Giv eksempel på en integritetsring hvori K ikke er et ideal, og på en integritetsring hvori K er et ikke-trivielt ideal.

20. Godtgør, at i en hovedidealring er $(a,(b,c)) = ((a,b),c)$, så den fælles værdi kan betegnes (a,b,c) (altså: fællesmålsdannelsen er associativ). Vis, at de to udtryk

$$\frac{abc}{(ab,ac,bc)} \qquad \text{og} \qquad \frac{abc\cdot(a,b,c)}{(a,b)\cdot(a,c)\cdot(b,c)}$$

begge angiver mindste fælles multiplum af a,b og c.

21. Lad $(L,+,\cdot)$ være en ægte delring af de rationale tals legeme, og således at L indeholder mængden $\dot{Z}$ af de hele tal. Ethvert element af L skrives som en uforkortelig brøk $\frac{m}{n}$.

Vis, at $\frac{m}{n} \in L \Rightarrow \frac{1}{n} \in L$.

Godtgør, at der findes en mængde P_L af primtal, således at L netop er mængden af de rationale tal, for hvilke nævnernes primdivisorer tilhører P_L.

Vis, at et vilkårligt ikke-trivielt ideal i L netop er hovedidealet frembragt af m_I, hvor m_I er det mindste tal i $\dot{I} \cap \dot{N}$.

Angiv de værdier, som m_I kan antage.

Vis, at idealerne i L kan ordnes i en "nedstigende kæde" $I' \supset I'' \supset I''' \supset \cdots$, hvis og kun hvis der netop er ét maximalideal, og angiv for hvilke P_L dette indtræffer.

22. Udnyt Gauss'ring til at bestemme to talpar $x,y \in \mathbb{N}$, $x \gg y$, så $x^2+y^2 = 40049 \cdot 964 = 38607236$.

23. Man betragter mængden P af delmængder af en given mængde M. For to elementer fra P (altså delmængder) defineres kompositionen Δ ved $A \Delta B = (A \cup B) \setminus (A \cap B)$. Vis, at $\emptyset$ er neutral ved Δ, og at (P,Δ) er en kommutativ gruppe, i hvilken alle elementerne er af 2' orden.

Vis, at $(P,\Delta,\cap)$ er en kommitativ ring med et etelement, som ønskes angivet.

Vis, at mængden af alle delmængder af et $J \subseteq M$ opfylder Id1 og Id2, altså er et ideal, og angiv en homomorf afbildning af $(P,\Delta,\cap)$ for hvilken idealet er kerne. Er det et primideal ? Bestem idealsummen af to sådanne idealer svarende til J_1 og J_2.

Angiv et maximalideal og strukturen af det tilsvarende kvotientlegeme, og vis at alle maximalidealer er af den angivne type.

24. Vis, at det s. 21 omtalte ideal I_o i C^∞-funktionerne er et primideal. Er det et maximalideal ?

25. Bevis, at for $n = 2$ er i den kinesiske restklassesætning forudsætningen om eksistens af etelement overflødig.

§ 4. Kontinuert ordnet gruppe. De reelle tal.

I § 2 blev det vist, hvorledes man udfra de naturlige tal kan opbygge de rationale tals legeme. I den nærværende § skal det bl.a. vises, hvorledes man ved betragtninger - i hvilke begrebet "konvergens" spiller en afgørende rolle - udfra de rationale tal kan opbygge det reelle talsystem, og dette eksempel kan man have i tankerne ved de nærmest følgende siders behandling af en ordnet gruppes fuldstændiggørelse.

Lad $(M,+,<)$ være en kommutativ ordnet gruppe. Dens elementer betegnes $x,y,z,\ldots$; dog vil vi et par steder af konventionelle grunde lade ε stå for et vilkårligt positivt element, og nulelementet betegnes 0. Som omtalt i § 2 er $|x| = \max\{x,-x\}$, og for denne absolutte værdi gælder simple regneregler. Bogstaverne $n,m,j,k,\ldots$ skal betegne naturlige tal.

Ved en følge $[x_j]$ af elementer fra M, eller udførligere skrevet en følge $(x_1,x_2,\ldots)$, forstås som bekendt en afbildning $j \to x_j$ af $\mathbb{N}$ ind i M. Ved en delfølge af en følge $[x_j]$ forstås som bekendt en følge $[x_{m_j}]$, hvor $j \to m_j$ er en endomorfi af $(\mathbb{N},<)$. Når vi siger, at en egenskab gælder for alle elementerne fra et vist trin i en følge $[x_j]$, eller at den gælder "slutteligt" i følgen $[x_j]$, så menes dermed, at der eksisterer et $n \in \mathbb{N}$, således at egenskaben gælder for alle elementerne x_j, hvor $j > n$. Vi skal nedenfor uden nærmere kommentarer benytte forskellige evidente sætninger om delfølger, som f.eks.: "En delfølge af en delfølge af $[x_j]$ er selv en delfølge af $[x_j]$" og "hvis en egenskab gælder fra et vist trin for alle elementerne i en følge, så gælder den også fra et vist trin for all elementerne i en delfølge".

Mængden af følger $[x_j]$ af elementer fra gruppen $(M,+,<)$

kan organiseres som en gruppe ved en følgeaddition, betegnet med $\oplus$, bestående i elementvis addition, således at $[x_j] \oplus [y_j] = [x_j + y_j]$; den tilsvarende subtraktion betegnes med $\ominus$. Gruppens nulelement er den følge, hvis elementer alle er o.

Ved en nulfølge (forkortet nf) forstås en følge $[x_j]$ som er således beskaffen, at der til ethvert positivt ε findes et n, således at for alle $j > n$ gælder $|x_j| < \varepsilon$. Eksempel: En følge hvori elementerne fra et vist trin er lig o er en nulfølge. Man ser umiddelbart, at $[x_j]\text{nf} \iff [-x_j]\text{nf} \iff [|x_j|]\text{nf}$, og at enhver delfølge af en nf er nf. Endvidere, at hvis man for alle j har $|x_j| < y_j$, hvor $[y_j]\text{nf}$, så er $[x_j]\text{nf}$.

Mængden af nulfølger udgør med $\oplus$ en gruppe $(\{\text{nf}\},\oplus)$. Dertil mangler vi blot at vise, at summen af to nulfølger er en nulfølge. Ved beviset må man skelne mellem to tilfælde: I^o, hvis gruppen har et mindste positivt element ε_o (indtræffer f.eks. for $(\dot{Z},+,<)$), så ser man ved at vælge $\varepsilon = \varepsilon_o$ at enhver nulfølges elementer er sluttelig o, men så er elementerne i summen af sådan to følger jo sluttelig o, så at sumfølgen er en nulfølge. II^o, hvis gruppen ikke har noget mindste positivt element, så kan man til ethvert ε finde et mindre ε_1, og $\varepsilon_2 = \varepsilon - \varepsilon_1$ er da også positiv, og ethvert positivt element kan altså skrives som en sum $\varepsilon = \varepsilon_1 + \varepsilon_2$ af to positive elementer; til ε_1 kan bestemmes et n_1 så $|x_j| < \varepsilon_1$ for $j > n_1$, og til ε_2 kan bestemmes et n_2 så $|y_j| < \varepsilon_2$ for $j > n_2$, og så er $|x_j + y_j| < \varepsilon_1 + \varepsilon_2 = \varepsilon$ for $j > n = \max\{n_1,n_2\}$, hvormed beviset er ført.

Ved en konvergent følge (forkortet kf) forstås en følge $[x_j]$ som er således beskaffen, at der findes et x for hvilket følgen

$[x_j - x]$ er en nulfølge. Elementet x kaldes grænseværdi for følgen $[x_j]$; en følge kan kun have én grænseværdi, thi antages at både x og y betegner grænseværdi for $[x_j]$, så viser den for alle j gyldige ulighed $|x - y| \leq |x_j - x| + |x_j - y|$ at $x - y = o$, fordi ulighedens højre side er element i en nulfølge (nemlig sum af to nulfølger).

Eksempler: Nulfølgerne er netop de følger, som er konvergente med grænseværdien o. En følge hvori alle elementer er lig x er konvergent med grænseværdien x.

Man ser umiddelbart, at $[x_j]$kf med grænseværdien x $\iff$ $[-x_j]$kf med grænseværdien -x. Endvidere, at en delfølge af en konvergent følge er konvergent og med samme grænseværdi.

Summen af to konvergente følger er en konvergent følge, hvis grænseværdi er summen af grænseværdierne; dette er en umiddelbar konsekvens af at summen af to nf igen er nf. Heraf ses, at mængden af konvergente følger udgør med $\oplus$ en gruppe; den afbildning som til en konvergent følge lader svare dens grænseværdi er en homomorf afbildning af gruppen $(\{kf\},\oplus)$ over på gruppen $(M,+)$, og homomorfiens kerne er $\{nf\}$.

Ved en fundamentalfølge (forkortet ff) forstås en følge $[x_j]$ som er således beskaffen, at for en vilkårlig delfølge $[x_{m_j}]$ er følgedifferensen $[x_j] \ominus [x_{m_j}] = [x_j - x_{m_j}]$ en nulfølge. (Det bemærkes, at der i funktionsanalysen ofte anvendes en anden definition of ff, men man kan let se, at definitionerne er ækvivalente; smlgn. øv. 1).

Eksempel: Enhver konvergent følge er en fundamentalfølge, thi for en kf $[x_j]$ med grænseværdi x er $[x_j - x_{m_j}] = [x_j - x] \ominus [x_{m_j} - x]$ en nf (differens mellem to nf).

Man ser umiddelbart, at $[x_j]$ff $\iff$ $[-x_j]$ff. Endvidere er sum-

men af to ff, hhv. $[x_j]$ og $[y_j]$, igen en ff, thi omskrivningen $[(x_j + y_j) - (x_{m_j} + y_{m_j})] = [x_j - x_{m_j}] \oplus [y_j - y_{m_j}]$ viser, at dette udtryk er en nf (sum af to nf). Heraf ses at, mængden af fundamentalfølger udgør med $\oplus$ en gruppe $(\{ff\},\oplus)$. Denne gruppe har $\{nf\}$ som normal undergruppe (normal, idet $\oplus$ er kommutativ), og der eksisterer derfor en homomorf afbildning φ af $(\{ff\},\oplus)$ over på en faktorgruppe $(\{ff\},\oplus)/\{nf\}$. Da $(\{ff\},\oplus)$ også har $\{kf\}$ som undergruppe, og denne ved den afbildning som fører en kf over i sin grænseværdi overføres på $(M,+)$, homomorft og med $\{nf\}$ som kerne, så kan φ tages som en udvidelse af denne homomorfi, og faktorgruppen $(\{ff\},\oplus)/\{nf\}$ kan skrives på formen $(M^*,+)$, hvor denne sidste gruppe er en udvidelse (effektiv eller ej) af $(M,+)$. Man bemærker, at ved φ vil $\{ff\}\setminus\{kf\}$ afbildes på $M^*\setminus M$.

Da en fundamentalfølge og en delfølge af den afviger indbyrdes med en nulfølge ses, at en delfølge af en fundamentalfølge er igen en fundamentalfølge, som ved afbildningen φ får det samme billede i M^*. Specielt ses, at hvis en fundamentalfølge har en delfølge som er konvergent, så er fundamentalfølgen selv konvergent og med samme grænseværdi, og endnu mere specielt, at hvis en fundamentalfølge har en delfølge som er en nulfølge, så er fundamentalfølgen selv en nulfølge.

Hvis $M^* = M$ bliver $\{ff\}\setminus\{kf\} = \emptyset$, så at enhver fundamentalfølge er konvergent. Med en glose velkendt fra læren om metriske rum siger vi i dette tilfælde, at den ordnede gruppe $(M,+,<)$ er fuldstændig.

Dette indtræffer f.eks. hvis enhver nulfølge sluttelig er o, thi så er enhver ff sluttelig konstant (idet ifølge definitionen af ff - med $m_j = j + 1$ - er $[x_j - x_{j+1}]$ en nf), og dermed konvergent. Specielt indtræffer det i tilfældet I^o (side 2). Men der

findes også andre fuldstændigt ordnede grupper, som f.eks. det reelle talsystem der ønskes konstrueret.

Vi skal på M^* indføre en ordning, så der fremkommer en ordnet gruppe $(M^*,+,<)$, som er en udvidelse af $(M,+,<)$. Vi kalder en ff $[x_j]$ for plusfølge, hvis den ikke er nf, og hvis det for all j fra et vist trin gælder at $x_j > 0$. For en vilkårlig følge $[x_j]$ er åbenbart højst én af følgerne $[x_j]$ og $\Theta[x_j]$ en plusfølge, men for enhver ff, som ikke er nf, indtræffer altid en af de to muligheder. Thi i modsat fald ville $[x_j]$ have både en delfølge $[x_{m_j}]$, hvor alle $x_{m_j} \leqq 0$, og en delfølge $[x_{n_j}]$, hvor alle $x_{n_j} \geqq 0$, og for ethvert j gælder så $0 \leqq x_{n_j} \leqq x_{n_j} - x_{m_j}$, hvori det sidste udtryk er element i en nf (fordi $[x_j]$ var ff), så at uligheden ville medføre, at $[x_{n_j}]$ var nf, altså at $[x_j]$ havde en delfølge som var nf, og dermed at $[x_j]$ selv. var nf.

Hvis $[x_j]$ og $[y_j]$ er plusfølger gælder fra et vist trin $0 < x_j < x_j + y_j$, hvor dette sidste ikke kan være element i en nf (for så viser uligheden, at $[x_j]$ er nf), og dermed er vist, at plusf $\oplus$ plusf $=$ plusf, eller med andre ord, at $(\{\text{plusf}\},\oplus)$ er en halvgruppe. Endvidere er plusf $\oplus$ nf = plusf, thi summen kan ikke være en nf (da $(\{\text{nf}\},\oplus)$ er en gruppe), og hvis den ikke var plusfølge måtte den efter det ovenstående være Θplusf, og ved at flytte over lighedstegnet ville det give plus $\oplus$ plusf = nf.

Vi lader stadig φ betegne den kanoniske afbildning af $(\{\text{ff}\},\oplus)$ på $(\{\text{ff}\},\oplus)/\{\text{nf}\} = (M^*,+)$. På M^* definerer vi nu en ordning $>$, idet vi sætter $x^* = \varphi([x_j]) > y^* = \varphi([y_j])$ hvis og kun hvis $[x_j - y_j]$ er plusf. Dette er brugbart som definition, thi selvom de samme x^* og y^* kan fremgå ved φ af forskellige ff $[x_j]$, hhv. $[y_j]$, så vil disse

kun afvige indbyrdes med nulfølger, hvilket er uden indflydelse på om $[x_j-y_j]$ er plusf. For elementer $x,y \in M$ vil relationen $>$ stemme overens med den oprindeligt givne ordning $>$ på M, således at det ikke gør noget, at vi har valgt samme betegnelse; thi for $x,y \in M$ er x og y grænseværdien (d.v.s. billedet ved φ) af de kf, hvori samtlige elementer er x, hhv. y, og disse følgers differens har samtlige elementer lig x-y, så at differensfølgen er en plusfølge netop når $x > y$. Da enhver ff er af netop én af typerne nf, plusf eller ⊖plusf, bliver relationen irreflexiv, total og asymmetrisk, og anvendes plusf ⊕ plusf = plusf på $[x_j-y_j] \oplus [y_j-z_j] = [x_j-z_j]$ ses, at den er transitiv. Desuden ser man, at {plusf} netop afbildes på de positive elementer i M^*. Og da $x_j-y_j = (x_j+z_j) - (y_j+z_j)$ vil $x^* > y^* \Rightarrow x^* + z^* > y^* + z^*$, så at $(M^*,+,<)$ er en ordnet kommutativ gruppe. Og denne gruppe er altså en udvidelse af den ordnede gruppe $(M,+,<)$.

Hvis en følge af elementer fra M er nf, kf eller ff i $(M,+,<)$ vil den opfattet som følge i $(M^*,+,<)$ have samme egenskab. Det er åbenbart tilstrækkeligt at bevise det for nulfølger, da de to andre slags følger er definerede v.hj.a. disse, men på den anden side er det ikke nogen trivialitet, da der i definitionen af en nulfølge skal sammenlignes med alle positive elementer, og når der er flere elementer i M^* end i M, stilles der herved flere krav. Vi skal imidlertid godtgøre, at der til ethvert positivt $\varepsilon^* \varepsilon M^*$ findes et positivt $\varepsilon \in M$, hvor $\varepsilon \leqq \varepsilon^*$, for så er det jo tilstrækkeligt at sammenligne med alle ε i.st.f. med alle ε^*. Antag $\varepsilon^* = \varphi([\varepsilon_j])$ hvor $[\varepsilon_j]$ er en plusfølge; dersom $\varepsilon > \varepsilon^*$, så er følgen $[\varepsilon - \varepsilon_j]$ en plusfølge, og fra et vist trin gælder derfor $\varepsilon > \varepsilon_j$; men hvis dette er tilfældet for alle ε er $[\varepsilon_j]$ en nulfølge, hvormed beviset er ført. Derimod er det uden videre klart, at en følge af elementer fra M som er nf eller

ff i $(M^*,+,<)$ vil have samme egenskab i $(M,+,<)$; for en kf kan noget tilsvarende ikke påstås idet dens grænseværdi kunne ligge i $M^*\backslash M$.

En fundamentalfølge $[x_j]$ i $(M,+,<)$ vil opfattet som følge i $(M^*,+,<)$ være konvergent med grænseværdien $x^* = \varphi([x_j])$. Ifølge det ovenstående er det tilstrækkeligt at vise, at for ethvert $\varepsilon \in M$ gælder fra et vist trin $|x_j - x^*| < \varepsilon$, og vi kan gerne antage, at $x^* \notin M$, for ellers er følgen allerede kf i $(M,+,<)$. Vi skal altså blot vise, at der ikke findes vilkårligt store j, hvor der (med et passende fortegn) gælder $\pm(x_j-x^*) > \varepsilon$. Men for ethvert sådant j ville følgen $[\pm(x_j-x_k)-\varepsilon]$ (hvori nu k er følgeindex) være en plusfølge, og vi kunne angive et $k = k(j)$ så $\pm(x_j-x_k)-\varepsilon > 0$, eller $|x_j-x_k| > \varepsilon$. Dersom dette kunne gøres for uendelig mange j fik vi to delfølger $[x_j]$ og $[x_{k(j)}]$, for hvilke den sidste ulighed strider mod at de er udtaget af en fundamentalfølge.

Den ordnede gruppe $(M^*,+,<)$ er fuldstændig. Bevis: Foran (side 4) er bemærket, at dersom enhver nf sluttelig er 0, så er $(M,+,<)$ selv fuldstændig og $M = M^*$; vi behøver derfor blot at betragte tilfældet, hvor der i M findes en nf $[x_j]$ som ikke sluttelig er 0, og dermed altså en nf, nemlig en delfølge af $[|x_j|]$, som består af lutter positive elementer (man bør bemærke, at selvom der ikke findes noget mindste positivt ε_0, tilfældet II° side 2, så er eksistensen af en nf af positive elementer ikke sikret). Lad $[\varepsilon_j]$ betegne en nf af lutter positive elementer og lad $[x_j^*]$ være en ff i M^*. Ethvert x_j^* er φ-værdi for en ff af elementer fra M, og denne ff konvergerer (i M^*) mod x_j^*. Til ethvert $x_j^* \in M^*$ findes altså et $y_j \in M$ så $x_j^* = y_j + \delta_j^*$, hvor $|\delta_j^*| < \varepsilon_j$. Man ser, at følgen $[\delta_j^*]$ er nf i M^*, og den er altså både ff og kf i M^*. Da $y_j = x_j^* - \delta_j^*$ ses, at $[y_j]$ er ff i M^*, og da dens elementer alle tilhører M er den også ff i M og dermed kf i M^*. Men så er $[x_j^*] = [y_j] \oplus [\delta_j^*]$ skrevet

som en sum af to følger, som begge er kf i M^*, og dermed er $[x_j^*]$ selv kf i M^*. Dermed er påstanden vist.

Dermed har vi sætningen: Enhver ordnet kommutativ gruppe $(M,+,<)$ kan udvides til en fuldstændig ordnet gruppe i hvilken enhver fundamentalfølge fra M er konvergent, nemlig den konstruerede $(M^*,+,<)$.

Udvidelsen er en entydigt bestemt mindste udvidelse med den nævnte egenskab, idet der også gælder: Hvis en kommutativ ordnet gruppe $(M,+,<)$ er indeholdt i en kommutativ ordnet gruppe $(\overline{M},+,<)$ og enhver fundamentalfølge fra M er konvergent i $\overline{M}$, så vil $(\overline{M},+,<)$ indeholde en undergruppe isomorf med $(M^*,+,<)$.

Bevis: Lad os et øjeblik med $\overline{nf}$, $\overline{kf}$ og $\overline{ff}$ betegne følger som er hhv. nulfølger, konvergente følger og fundamentalfølger i $\overline{M}$, medens nf, kf og ff betegner følger af de samme arter i M. Da $\overline{M}$ indeholder flere positive ε end M er det klart, at hvis en følge af elementer fra M er $\overline{nf}$ så er den også nf, og hvis den er $\overline{ff}$ (specielt $\overline{kf}$) så er den også ff. Omvendt vil ifølge forudsætning enhver ff være $\overline{kf}$ og specielt enhver nf være $\overline{nf}$ (den er jo $\overline{kf}$, og grænseværdien må være 0, hvilket f.eks. ses ved i følgen at indskyde uendelig mange elementer = 0, hvorved den stadig er nf og dermed $\overline{kf}$). Når vi kun betragter følger af elementer $\in$ M er altså {nf} = {$\overline{nf}$} og {ff} = {$\overline{kf}$} og endvidere {plusf} = {$\overline{kf}$ med positiv grænseværdi}. Nu er ifølge det tidligere (side 3) gruppen $(\overline{M},+,<)$ netop billedet af gruppen $(\{\overline{kf}\},\oplus)$ ved en afbildning med {$\overline{nf}$} som kerne, og ordnet ved at de positive elementer er billederne af {$\overline{kf}$ med positiv grænseværdi}. Betragtes restriktionen af denne afbildning til mængden af følger, hvis elementer alle tilhører M, får vi som billede netop $(\{ff\},\oplus)/\{nf\} = (M^*,+)$, og ordnet ved at de positive elementer er billedet af {plusf}, altså netop $(M^*,+,<)$. Og da billedet ved

restriktionen er indeholdt i totalbilledet, vil $(M^*,+,<)$ være indeholdt i $(\overline{M},+,<)$.

Ved den sidst beviste sætning bør det fremhæves, at det er væsentligt, at vi kræver, at en ff fra M er kf i $\overline{M}$. Af en øvelse fremgår, at det er meningsløst at tale om "den mindste fuldstændigt ordnede gruppe, som indeholder en given ordnet gruppe".

Ved de reelle tals ordnede gruppe $(\dot{R},+,<)$ forstår man den (pånær isomorfi entydigt bestemte) ved ovenstående metode konstruerede udvidelsesgruppe $(\dot{Q}^*,+,<)$ til gruppen $(\dot{Q},+,<)$ af rationale tal. Det er let (men udskydes til lidt senere) at indføre en multiplikation på $(\dot{R},+,<)$ således at man får de reelle tals ordnede legeme $(\dot{R},+,\cdot,<)$.

Vi skal betragte nogle andre karakteriseringer af $(\dot{R},+,<)$ som ordnet gruppe.

Vi betragter en ordnet kommutativ gruppe $(M,+,\leqq)$, ved hvilken vi af praktiske grunde i det følgende benytter den reflexive ordningsrelation $\leqq$ i st.f. den tilsvarende irreflexive. En følge $[x_j]$ betegnes voksende, hvis $x_1 \leqq x_2 \leqq \ldots$, og på analog måde benyttes gloserne "aftagende" og "monoton".

Lad os minde om majorantbegrebet (AG, I,5,26-27)(for de følgende småbeviser kan man også bemærke den stærke lighed med beviserne for konjugerede underrum, AG III 12,6): Ethvert a har en majorantmængde $M'(a) = \{x|x \geqq a\}$ og en minorantmængde $M''(a) = \{x|x \leqq a\}$. En delmængde A harmajorantmængde og minorantmængde hhv. lig

$$M'(A) = \bigcap_{a\in A} M'(a) \quad \text{og} \quad M''(A) = \bigcap_{a\in A} M''(a).$$

Det er klart, at $A \subseteq M'(M''(A))$ og $A \subseteq M''(M'(A))$, og endvidere at $C \subseteq A \Rightarrow M'(C) \supseteq M'(A) \wedge M''(C) \supseteq M''(A)$. Øvre og nedre grænse for A defineres som $\sup A = \min M'(A)$ og $\inf A = \max M''(A)$, idet eksistens på den ene side af lighedstegnet medfører eksistens på den anden side.

Ved et snit (A,B) forstås to ikke-tomme delmængder A og B af M, for hvilke $B = M'(A)$ og $A = M''(B)$. Det er klart, at $A \cup B = M$, thi minorantmængden A for B vil med ethvert a også indeholde alle $x \leq a$, og de x som ikke kommer med herved er $>$ alle $a \in A$, og tilhører altså B = majorantmængden B for A. Hvis $c \in A \cap B$, så er samtidigt $c \in A$ og c majorant for A, altså $c = \max A = \inf B$, og analogt ses, at $c = \min B = \sup A$, og vi har altså $A = \{a \mid a \leq c\}$ og $B = \{b \mid b \geq c\}$, og specielt ses, at $A \cap B$ består af højst et element. Hvis blot ém af størrelserne max A, inf B, min B, sup A eksisterer, ser man at dette tilfælde forekommer, og snittet siges at være elementbestemt (ved c). Endvidere ses, at ethvert $c \in M$ på denne måde kan frembringe et elementbestemt snit. Hvis $A \cap B = \emptyset$, er snittet (A,B) ikke elementbestemt. Der findes grupper med snit som ikke er elementbestemte, f.eks. udgør i $(\mathbb{Q},+,\leq)$ mængderne $A = \{x \mid x^3 \leq 2\}$ og $B = \{x \mid x^3 \geq 2\}$ et snit som ikke er elementbestemt (løst sagt fordi $\sqrt[3]{2}$ er irrational).

For en kommutativ ordnet gruppe $(M,+,\leq)$ er nu følgende tre egenskaber ensbetydende

1) Ethvert snit er elementbestemt

2) For enhver ikke-tom opad begrænset delmængde C eksisterer sup C

3) Enhver voksende begrænset følge er konvergent

idet man naturligvis også kunne erstatte 2) med den tilsvarende egenskab for nedad begrænset og inf, og ligeså kunne erstatte 3) med

den tilsvarende egenskab for aftagende følge.

Først skal vises, at 1) medfører 2). Lad C være ikke-tom og opad begrænset; vi sætter B = M'(C) og den er ikke tom, og vi sætter A = M''(B), og da A = M''(B) = M''(M'(C)) $\supseteq$ C er den heller ikke tom. Endvidere vil C $\subseteq$ A medføre B = M'(C) $\supseteq$ M'(A), men samtidig har vi B $\subseteq$ M'(M''(B)) = M'(A), og tilsammen fås B = M'(A), og sammen med det forrige viser det, at vi har et snit. Når dette er elementbestemt så eksisterer min B, som ifølge sin definition er lig sup C, hvormed beviset er ført. (Vi bemærker, at det er trivielt, at 2) medfører 1), thi for et snit (A,B) er A opad begrænset, hvorefter eksistensen af dens sup viser, at snittet er elementbestemt).

Dernæst skal vises, at 2) medfører 3). Hvis $[x_j]$ er en voksende begrænset følge, så udgør dens elementer en voksende begrænset delmængde, og ifølge 2) findes der et $x = \sup\{x_j\}$ =mindste majorant for $\{x_j\}$, og for ethvert ε er derfor $x-\varepsilon$ ikke majorant, og der findes altså et x_n så $x-\varepsilon < x_n \leq x$, og for ethvert $j>n$ gælder så også $x - \varepsilon < x_j \leq x$, hvilket viser, at følgen er kf med grænseværdien x.

Endelig skal vi vise, at 3) medfører 1). Vi vil antage, at der findes et snit (A,B) som ikke er elementbestemt, men at enhver voksende begrænset følge er kf, og skal deraf udlede en modstrid. Da max A ikke eksisterer kan vi til ethvert $x \in A$ finde et $x + \varepsilon \in A$, og vi skal først vise, at det kan gøres på en sådan måde, at $x + 2\varepsilon \in B$; vi tager $x \in A$ og et positivt δ så $x + \delta \in A$, og betragter følgen $[x_j] = [x + 2^j\delta]$; følgen $[x_j]$ kan ikke være kf, fordi $[x_{j+1}-x_j] = [2^j\delta]$ ikke er nf (dens elementer er jo ikke fra et vist trin mindre end det positive δ), men da $[x_j]$ er voksende må den så være ubegrænset, og den må derfor have et element x_m større end et element $b \in B$; hvis vi tager det mindste j så $x_{j+1} \in B$ vil for $\varepsilon = 2^j\delta$ elementet $x_j = x+\varepsilon$ ligge i A, medens

til ethvert af dem findes altså et mindre x_j længere ude i følgen, og vi kan altså opnå en aftagende delfølge.

Egenskab 3) udsagde, at enhver monoton begrænset følge er konvergent. Først vises, at 3) medfører 5'). Da enhver kf også er ff, er første del af 5') opfyldt. For at vise anden del bemærker vi først, at enhver fundamentalfølge er begrænset; hvis dette ikke gjaldt kunne vi til ethvert x_j finde et $x_{k(j)}$ så $|x_j - x_{k(j)}| > \varepsilon$, i strid med at differensfølgen $[x_j - x_{k(j)}]$ skulle være nf. Af en ff kan derfor altid udtages en begrænset monoton delfølge, og når denne ifølge 3) er kf, så må fundamentalfølgen selv være konvergent. Dermed er anden del af 5') bevist.

Så vises, at 5') medfører 4). Enhver begrænset har en begrænset monoton delfølge, og 5') udsiger at denne er ff og dernæst at den er kf, hvormed 4) er vist.

Endelig vises at 4) medfører 3). En monoton begrænset følge $[x_j]$ har ifølge 4) en konvergent delfølge, og hvis grænseværdien kaldes x vil altså for ethvert ε uendelig mange x_j ligge mellem $x-\varepsilon$ og $x+\varepsilon$, men p.g.a. monotonien gælder dette så også for alle de mellemliggende indices, d.v.s. for alle x_j fra et vist trin, hvormed beviset er ført.

$x_{j+1} = x+2\varepsilon$ ligger i B, hvilket påstodes. Vi tager så et $y_o \in A$ og danner en følge $[y_j]$ af elementer $\in A$ og en følge $[z_j]$ af elementer $\in B$, idet vi efter y_{n-1} tager $y_n = y_{n-1} + \varepsilon_n \in A$ og $z_n = y_{n-1}+2\varepsilon_n \in B$; følgen $[y_n]$ er voksende og begrænset (f.eks. af et vilkårligt element fra B), altså kf, hvilket viser, at $[\varepsilon_n] = [y_n - y_{n-1}]$ er nf, og følgen $[z_n] = [y_n+\varepsilon_n]$ er derfor også kf og med samme grænseværdi. Lad os kalde den fælles grænseværdi x; hvis $x \in A$ findes et $x+\varepsilon \in A$, men det strider mod at fra et vist trin er $z_n < x+\varepsilon$ samtidig med at $z_n \in B$; hvis $x \in B$ findes et $x-\varepsilon \in B$, men det strider mod at fra et vist trin er $y_n > x-\varepsilon$ samtidig med at $y_n \in A$. Der kan altså ikke findes noget x (da jo $A \cup B = M$), hvormed den ønskede modstrid er opnået.

Dermed er vist, at 1), 2) og 3) er ensbetydende.

Vi vil yderligere vise, at egenskaberne 1), 2) og 3) er ensbetydende med

4) Enhver begrænset følge har en konvergent delfølge

5') Enhver voksende begrænset følge er fundamentalfølge, og enhver fundamentalfølge er konvergent.

Til det formål vil vi først vise, at <u>enhver følge har en monoton delfølge</u>. Lad $[x_j]$ være en given følge; vi vil forsøge at udtage en voksende delfølge, og viser, at hvis konstruktionen mislykkes findes der en aftagende delfølge. Vi tager om muligt k_1 så uendelig mange $x_j \geq x_{k_1}$; så tager vi om muligt $k_2 > k_1$, så $x_{k_2} \geq x_{k_1}$ og uendelig mange $x_j \geq x_{k_2}$; så tager vi om muligt $k_3 > k_2$, så $x_{k_3} \geq x_{k_2}$ og uendelig mange $x_j > x_{k_3}$; o.s.v.. Hvis konstruktionen stadig er mulig fremkommer der en voksende følge $[x_{k_j}]$. Hvis vi efter bestemmelsen af x_{k_n} ikke kan fortsætte konstruktionen, så skyldes det at for ethvert j_o blandt de uendelig mange j større end k_n, for hvilke $x_j \geq x_{k_n}$ vil fra et vist trin gælde at $x_j < x_{j_o}$;

skaberne er karakteristiske for de reelle tal:

Gruppen $(\dot{R},+,<)$ opfylder de fem ensbetydende betingelser

1) Ethvert snit er elementbestemt

2) For enhver ikke-tom opad begrænset delmængde C eksisterer sup C.

3) Enhver voksende begrænset følge er konvergent.

4) Enhver begrænset følge har en konvergent delfølge

5) Gruppen er arkimedisk og fuldstændig.

Omvendt vil enhver ordnet kommutativ gruppe som ikke har noget mindste positivt element og opfylder et af de fem krav være isomorf med $(\dot{R},+,<)$.

At $(\dot{R},+,<)$ opfylder f.eks. 5) ses let, idet den er fuldstændig, og til ethvert ε^* i den, altså i $(\dot{Q}^*,+,<)$, findes et $\varepsilon \in \dot{Q}$, så $\varepsilon \leqq \varepsilon^*$, og i undergruppen $\{n\varepsilon\}$ findes åbenbart til ethvert $a \in \dot{R}$ et $n\varepsilon \geqslant a$.

Beviset den anden vej skal ikke detailleres. Løst sagt beror det på at $(M,+,<)$ arkimedisk $\Rightarrow$ $(M,+,<)$ isomorf med en del af $(\dot{R},+,<)$, hvorefter "fuldstændig" medfører, at det er hele $\dot{R}$.

Vi skal endnu vise, at der gælder en til sætningen s.8 svarende sætning om udvidelse af et ordnet kommutativt legeme: Givet et ordnet kommutativt legeme; det kan - og pånær isomorf kun på én måde - udvides til et fuldstændigt ordnet legeme, således at enhver fundamentalfølge i det givne er konvergent i det udvidede.

"Ordnet legeme" er tidligere defineret. Gloserne "fundamentalfølge", "konvergent" og "fuldstændig" refererer til de additive grupper.

I det givne legeme $(L,+,\cdot,<)$ betragter vi den additive gruppe $(L,+,<)$, og denne udvides som i det foregående til $(L^*,+,<)$, hvor $(L^*,+) = (\{ff\}, \oplus)/\{nf\}$. Men vi skal vise, at $\{ff\}$ endda kan orga-

Egenskaben 5') kan udtrykkes lidt anderledes. Sidste del af den udsiger blot, at $(M,+,<)$ er fuldstændig. Første del skal vises at være ensbetydende med: Til to positive elementer ε og $a \in M$ findes altid et naturligt tal n, så $a < n\varepsilon$ (idet $n\varepsilon$ er et element $\varepsilon+\varepsilon\cdots+\varepsilon$; der er ikke tale om multiplikation), hvilket åbenbart også kan udtrykkes med ordene: for enhver ikke-triviel undergruppe (der jo specielt indeholder en mængde $\{n\varepsilon\}$) vil ethvert $a \in M$ ligge mellem elementer fra undergruppen. Vi kan udtrykke egenskaben kort ved at sige, at $(M,+,<)$ er <u>arkimedisk</u>, og konstaterer overensstemmelse med AT 2,20, idet et ordnet legeme er arkimedisk netop når dets additive gruppe er arkimedisk.

Først: Hvis $(M,+,<)$ ikke er arkimedisk, så findes a og ε, hvor a > alle $n\varepsilon$, men så er følgen $\varepsilon, 2\varepsilon, 3\varepsilon, \cdots$ åbenbart voksende og opad begrænset, og den er ikke ff, da $[x_{j+1}-x_j] = [\varepsilon]$ ikke er nf. Så den anden vej: Antag $[x_j]$ voksende, begrænset af a og ikke ff, så eksisterer et ε, for hvilket man for vilkårligt store j kan finde et $k = k(j) > j$, hvor $x_k - x_j \geq \varepsilon$; vi kan da for ethvert n finde et $x_m > n\varepsilon$, hvilket kan ses ved induktion, thi hvis $x_m > n\varepsilon$ kan vi tage et $j > m$, og et tilsvarende $k(j)$, og har så $x_k > x_j+\varepsilon \geq x_m+\varepsilon > (n+1)\varepsilon$; men da a er større end alle x_m, er gruppen ikke arkimedisk.

I St.f. 5') kan vi derfor sige 5) gruppen $(M,+,<)$ er arkimedisk og fuldstændig.

Da 5 ensbetydende betingelser opfyldes trivielt af en gruppe bestående af et element, og endvidere af enhver uendelig cyklisk gruppe $(\{n\varepsilon\},+,<)$, og man ser omvendt af 5), at hvis en gruppe har et mindste positivt element ε_0 og opfylder betingelserne, så må den være af denne art, altså isomorf med $(\mathbb{Z},+,<)$.

Der gælder nu følgende vigtige sætning, som udsiger at egen-

niseres som en ring $(\{ff\}, \oplus, \odot)$, idet vi som følgemultiplikation $\odot$ benytter elementvis multiplikation, altså $[x_j] \odot [y_j] = [x_j y_j]$, og at $\{nf\}$ bliver et maximalideal i denne ring. Thi så bliver jo kvotientringen $(\{ff\}, \oplus, \odot)/\{nf\}$ et legeme; af det foregående fremgår, at dets additive gruppe er fuldstændigt ordnet, og at enhver ff fra det givne legeme er kf i udvidelsen. Med hensyn til multiplikationen vil ordningen også være i orden, da produktet af to plusfølger åbenbart fra et vist trin har positive elementer og derfor er plusf eller nf, så at i kvotientlegemet bliver produktet af to positive elementer ≥ 0. Vi skal derfor blot vise de understregede påstande.

Det er foran s.13 vist, at enhver ff er begrænset, og dette medfører at nf $\odot$ff = nf, for hvis $[x_j]$nf og $[y_j]$ff, så findes et $z >$ alle $|y_j|$, hvoraf fås $|x_j y_j| < \varepsilon$, når blot $|x_j| < \varepsilon z^{-1}$ (NB her benyttes, at L er et legeme; det gælder ikke alment i en ring, at $\{ff\}$ udgør en ring).

Så følger at ff $\odot$ ff = ff, idet for to givne ff$[x_j]$ og $[y_j]$ bliver $x_j y_j - x_k y_k = x_j(y_j - y_k) + (x_j - x_k)y_k$, som er element i en nf (nemlig ff $\odot$nf $\oplus$ nf$\odot$ff). Da elementvis multiplikation endvidere er kommutativ og associativ og distributiv m.h.t. addition, har vi en ring $(\{ff\}, \oplus, \odot)$. Desuden er $\{nf\}$ et ideal i denne, for ovenfor er vist at Id2 er opfyldt, og fra tidligere ved vi at Id1 er opfyldt.

Så mangler vi blo at vise, at $\{nf\}$ er maximalideal. Hvis et ideal indeholder $\{nf\}$ og desuden en ff, som ikke er nf, så indeholder det en følge $[x_j]$, ikke nf, af elementer som alle er ulig 0 (nemlig en delfølge af den forrige). Følgen $[x_j^{-1}]$ er begrænset for ellers fandtes for ethvert ε^{-1}et større $|x_j^{-1}|$, d.v.s. for ethvert ε et mindre $|x_j|$, men så ville $[x_j]$ være nf. Men så er $[x_j^{-1}]$ff,

idet $x_j^{-1} - x_k^{-1} = (x_k - x_j)x_j^{-1}x_k^{-1}$ er et nulfølgeelement gange noget begrænset. Dernæst viser Id2 at idealet indeholder $[x_j] \odot [x_j^{-1}] = [e]$, som er etelementet i $(\{ff\}, \odot)$, og dermed indeholder idealet hele $\{ff\}$. Dermed er beviset fuldført.

Ved det reelle tallegeme $(\dot{R}, +, \cdot, <)$ forstår man det på denne vis konstuerede udvidelseslegeme til $(\dot{Q}, +, \cdot, <)$.

Øvelser til §4.

1. Vis, at den i teksten side 3 givne definition af fundamentalfølge er ækvivalent med definitionen: Følgen $[x_j]$ siges at være fundamentalfølge, dersom der for ethvert $\varepsilon > 0$ eksisterer et $n \in \dot{\mathbb{N}}$, så $j, k > n \Rightarrow |x_j - x_k| < \varepsilon$.

2. Lad $(G,+,<)$ være en ordnet kommutativ gruppe. Mængden $M = G \times \dot{\mathbb{Z}} = \{(g,z) \mid g \in G \wedge z \in \dot{\mathbb{Z}}\}$ organiseres som gruppe ved $(g_1, z_1) + (g_2, z_2) = (g_1+g_2, z_1+z_2)$, og ordnes ved

$$(g_1, z_1) < (g_2, z_2) \iff g_1 < g_2 \vee (g_1 = g_2 \wedge z_1 < z_2).$$

Vis, at der herved er dannet en kommutativ ordnet gruppe $(M,+,<)$ med en undergruppe isomorf med $(G,+,<)$. Er $(M,+,<)$ arkimedisk? Vis, at $(M^*,+,<) = (M,+,<)$, så at gruppen er fuldstændig. Kan man af $(G,+,<)$ indeholdt i $(M,+,<)$ slutte at $(G^*,+,<)$ indeholdt i $(M^*,+,<)$? Som eksempel kan betragtes $(\dot{\mathbb{Q}},+,<)$, og angiv her kardinaltallene for M^* og $\dot{\mathbb{Q}}^*$.

3. Lad $(G,+,<)$ være en arkimedisk ordnet gruppe. Vis, at for givne elementer $a,b \neq 0$, vil mængderne

$$\{\tfrac{m}{n} \mid ma \leqq nb\} \text{ og } \{\tfrac{m}{n} \mid ma \geqq nb\},\ m, n \in \dot{\mathbb{Z}},\ n \neq 0,$$

udgøre et snit i $(\dot{\mathbb{Q}},+,<)$, og benyt dette til at vise, at $(G,+,<)$ er isomorf med en undergruppe i $(\dot{\mathbb{R}},+,<)$.

KØBENHAVNS UNIVERSITETS MATEMATISKE INSTITUT
UNIVERSITETSPARKEN 5
2100 KØBENHAVN Ø, DANMARK
TELEFON (01) 35 31 33

M A T E M A T I K 2

AT	1970-71	0,11 (ny) - 0,17
	1965-66	5,1 - 5,3
	1968-69	5,4 - 5,4 a
	1965-66	5,5 - 5,11
	1963-64	2,22 - 2,27
	1968-69	2,27 a - 2,27 e (§5)
	1963-64	2,28 - 2,30
	1968-69	2,31 (§5)
	1965-66	5,øv. 1-14
	1968-69	5,øv. 15-19
	1964-65	2,øv. 27-29
	1969-70	6, 1-10
	1969-70	6,øv. 1-6

§ 5. Polynomier.

Lad $(M,+,\cdot)$ være en integritetsring. Ved et polynomium a over M forstår vi et endeligt sæt $(a_0,a_1,\ldots,a_n)$ af elementer fra M, indicerede på den angivne måde; elementerne a_j kalder vi polynomiets koefficienter, begrundelsen for denne betegnelse vil fremgå nedenfor. Da vi ofte samtidig skal betragte sæt af forskellige længder, kan det være praktisk og vil ikke skade at betragte polynomiet a som en følge $(a_0,a_1,\ldots)$ hvori elementerne er 0 fra et vist trin. Det største index m for hvilket $a_m \neq 0$ kaldes for polynomiets grad.

Mængden af polynomier over M organiseres som en ring, polynomiumsringen $(M[X],+,\cdot)$ ved følgende kompositioner (hvor det ikke vil volde besvær, at vi vælger de samme kompositionstegn + og · som i M):

Additionen defineres ved at sætte $a + b = c$, hvor $c = (c_0,c_1,\ldots)$ med $c_j = a_j + b_j$, altså som koefficientvis addition. Man ser, at polynomierne med addition udgør en kommutativ gruppe, hvis neutralelement er nulpolynomiet $(0,0,\ldots)$. Multiplikationen defineres ved at sætte $a\cdot b = c$, hvor $c = (c_0,c_1,\ldots)$ med $c_j = \Sigma a_k b_{j-k}$, hvor der summeres idet k løber fra 0 til j, eller med andre ord $c_j = \Sigma a_k b_l$ hvor der summeres over alle par (k,l) hvis sum er lig j. Man ser, at multiplikationen bliver kommutativ (idet multiplikationen i M var kommutativ), og den bliver associativ, idet man finder

$$a\cdot b\cdot c = d = (d_0,d_1,\ldots), \text{ hvor } d_j = \sum_{k+l+m=j} a_k b_l c_m ,$$

uafhængigt af hvorledes man sætter parenteser i produktet $a\cdot b\cdot c$. Endvidere bliver multiplikationen distributiv m.h.t. additionen,

hvilket let ses (hvis man i udtrykket $c_j = \Sigma a_k b_i$ ovenfor erstatter a_k med $a_k' + a_k''$ får man c_j erstattet med $c_j' + c_j''$). Der findes et etelement (neutral multiplikatór), nemlig $(e,0,0,\ldots)$, hvor e betegner etelementet i M. Og endelig ser man, at nulreglen gælder, thi hvis a og b ikke er nulpolynomiet og har hhv. a_r og b_s som højestegradskoefficienter, så vil c_{r+s} ifølge produktdefinitionen blive $a_r b_s$, som er ulig 0 (idet M var en integritetsring). Dermed er vist, at <u>polynomiumsringen</u> $(M[X],+,\cdot)$, <u>eller kortere</u> $M[X]$, <u>over en integritetsring</u> $(M,+,\cdot)$ <u>er en integritetsring</u>.

Ovenfor blev defineret graden af et egentligt polynomium a. Nulpolynomiet kan man tilskrive en grad $-\infty$, og man ser så, at graden af summen af to polynomier er mindre end eller lig med den maximale af addendernes grader, og at graden af produktet af to polynomier er lig summen af faktorernes grader (idet man på en selvfølgelig måde regner med $-\infty$).

Polynomiumsringen $M[X]$ indeholder en delmængde bestående af polynomierne af 0'te grad, "<u>konstanterne</u>", $(a_0,0,0,\ldots)$, og af definitionerne på additionen og multiplikationen ser man let, at de udgør en delring, som ved afbildningen $(a_0,0,0,\ldots) \leftrightarrow a_0$ ses at være isomorf med $(M,+,\cdot)$. Vi kan derfor, om vi vil, udskifte betegnelserne, og i st.f. $(a_0,0,0,\ldots)$ blot skrive a_0, og så opfatte $M[X]$ som en nyskabt udvidelsesring for $(M,+,\cdot)$.

Polynomiet $(0,e,0,0,\ldots)$ vil vi betegne X. Udregnes de successive potenser af X findes

$$X = (0,e,0,0,\ldots)$$

$$X^2 = (0,0,e,0,\ldots)$$

$$X^3 = (0,0,0,e,\ldots)$$

o.s.v.,

og af multiplikationens definition fås let, at $a_kX^k = (a_k,0,0,\ldots)$. $(0,0,\ldots,e,\ldots)$ bliver lig $(0,0,\ldots,a_k,\ldots)$ (med 0 undtagen på den k'te plads), hvoraf vi ser, at polynomiet $a = (a_0,a_1,\ldots,a_n,0,\ldots)$ kan skrives på en form, som vi ofte vil betegne a(X), nemlig

$$a = a(X) = a_0 + a_1X + \ldots + a_nX^n .$$

Regning med polynomierne indenfor M[X] bliver derved reduceret til en simpel (og fra skolen tilvant) form, uden at man behøver at opfatte X som et mystisk variabelbegreb.

Selvom $(M,+,\cdot)$ er en hovedidealring behøver M[X] ikke at være en hovedidealring; f.eks. er $\dot{Z}[X]$ ikke en hovedidealring, idet mængden af polynomier $a_0 + a_1X + \ldots + a_nX^n$ hvori a_0 er et lige tal let ses at være et ideal (opfylder Id1 og Id2), men ikke er mængden af multipla af et frembringerelement. Men der gælder sætningen: Hvis M er et kommutativt legeme, så er polynomiumsringen M[X] en hovedidealring.

For at vise sætningen skal vi bemærke, at til to polynomier D(X) ("dividend") og d(X) ("divisor"), hvor d(X) ikke er nulpolynomiet, er det muligt at bestemme et q(X) ("kvotient"), således at "resten"

$$r(X) = D(X) - d(X)\cdot q(X)$$

bliver af lavere grad end d(X). Metoden hertil er en velkendt divisionsalgoritme, ved hvilken koefficienten til højestegradsleddet i d(X) divideres op i visse andre elementer fra M. Herved benyttes virkelig, at M er et legeme.

Lad nu I være et ideal i M[X]. Nulidealet er trivielt et hovedideal, så vi kan antage, at I indeholder egentlige polynomier.

Lad os i I tage et egentligt polynomium d(X) af den lavest forekommende grad, vi vil da vise, at et vilkårligt $D(X) \in I$ er et multiplum af d(X). Dertil bestemmer vi i divisionsligningen ovenfor et q(X), således at r(X) bliver af lavere grad end d(X), men ifølge Id1 og Id2 gælder $r(X) \in I$, som medfører at r(X) = 0. Altså vil D(X) være delelig med d(X).

Lad os stadig antage, at M er et kommutativt legeme, så at M[X] er en hovedidealring. Vi kan anvende den i § 3 udviklede teori for faktoropløsning. Gruppen af de regulære elementer i M[X] ses at bestå af mængden af de fra 0 forskellige konstanter, medens de ikke-regulære elementer er polynomierne af grad større end 0. Et polynomium er reducibelt, hvis det kan skrives som produkt af to polynomier som ikke er konstanter, og i modsat fald er det irreducibelt.

Eksempler:

Et førstegradspolynomium er altid irreducibelt.

Et polynomium er deleligt med førstegradspolynomiet X-c (hvor $c \in M$) hvis og kun hvis det har c som rod (rodbegrebet omtales nærmere senere), og et polynomium af grad større end eller lig 2 er derfor reducibelt, hvis det har en rod $\in M$. Man ser, at for polynomier af grad 2 eller 3 er denne betingelse både nødvendig og tilstrækkelig. F.eks. er polynomiet X^3-X^2+e over legemet $(\mathbb{Z}_2,+,\cdot)$ (altså over legemet af restklasser modulo 2, og hvor e betegner etelementet i dette legeme) irreducibelt, thi ved prøve ses, at ingen af de to elementer fra $\mathbb{Z}_2$ giver polynomiet værdien 0.

Hvis M er brøklegeme for en integritetsring $(I,+,\cdot)$ med entydig faktorisering, og $a(X) \in M[X]$, så findes et $m \in I$ således at $ma(X) \in I[X]$, f.eks. m = "fællesnævneren" for koefficienterne i a(X); et førstegradspolynomium rX-s, hvor r og s er primiske, $r,s \in I$ kan da kun være faktor i polynomiet dersom r går op i koefficienten til højestegradsleddet og s går op i det konstante led i polynomiet ma(X). Et simpelt bevis kommer senere i denne §. Reglen generaliserer en fra skolen velkendt regel ("hvis en uforkortelig brøk $\frac{s}{r}$ er rod i et polynomium med heltallige koeffocienter, så vil r gå op i polynomiets højestegradskoefficient og s gå op i dets konstante led") og er nyttig ved opsøgning af førstegradsfaktorer.

Den såkaldte "algebraens fundamentalsætning" - som vi ikke skal bevise her, da den naturligt falder ind under den matematiske analyse - udsiger (I): $c(X) \in \mathbb{C}[X]$ og irreducibel medfører at c(X) er af første grad, men kan også udtrykkes (II): $r(X) \in \mathbb{R}[X]$ og irreducibel medfører at r(X) er af første eller anden grad. Thi (I) $\Rightarrow$ (II): $r(X) \in \grave{\mathbb{C}}[X]$, har altså en rod $a \in \grave{\mathbb{C}}$; hvis $a \in \grave{\mathbb{R}}$ er X-a reel faktor i r(X), og hvis $a \in \grave{\mathbb{C}} \setminus \grave{\mathbb{R}}$ er $(X-a)(X-\bar{a})$ reel faktor i r(X). Og (II) $\Rightarrow$ (I): $c(X)\cdot\bar{c}(X) \in \grave{\mathbb{R}}[X]$, og har altså en faktor af første eller anden grad i $\grave{\mathbb{R}}[X]$, og i begge tilfælde vil c(X) så have en rod $\in \grave{\mathbb{C}}$.

Sætningen om den entydige primopløsning indenfor en hovedidealring giver: Ethvert polynomium af grad større end 0 kan på en og kun én måde skrives som produkt af irreducible polynomier fra M[X] (idet disse dog kun er bestemt pånær konstante faktorer).

Eksempel: I $\hat{R}[X]$ kan polynomiet $3(X^4-2)$ skrives som produkt af irreducible, nemlig som

$$3(X^4-2) = (3X-3\sqrt[4]{2})(X+\sqrt[4]{2})(X^2+\sqrt{2}),$$

og samtlige sådanne produktfremstillinger fås ved på forskellig måde at fordele den konstante faktor 3 på højre sides parenteser. Opfattes det samme polynomium som polynomium over $\hat{Q}$ er det irreducibelt, thi hvis det indenfor $\hat{Q}[X]$ kunne skrives som produkt $a(X)\cdot b(X)$ ville dette også være en faktoropløsning indenfor $\hat{R}[X]$, og kunne derfor bortset fra konstanterne fremgå af den ovenstående opløsning ved at to af parenteserne samledes til en, men hvorledes det end gøres kan der ikke derved opstå polynomier fra $\hat{Q}[X]$.

Vi betragter igen polynomiumsringen M[X] over et kommutativt legeme $(M,+,\cdot)$; vi antager, at M består af mere end nulelementet, for ellers ville alt blive trivielt. Lad endvidere $(M,+,\cdot)$ være indeholdet i en integritetsring $(L,+,\cdot)$, og lad c være et vilkårligt element fra L.

Der findes netop én homomorf afbildning af M[X] ind i L, ved hvilken M's elementer er fixelementer, og således at $X \to c$, nemlig afbildningen

$$a = a(X) = a_0 + a_1X + \ldots + a_nX^n \to a_0 + a_1c + \ldots a_nc^n,$$

thi denne afbildning er åbenbart en homomorfi med de ønskede egenskaber, og man ser også umiddelbart, at en sådan ikke kan være anderledes. Vi beskriver afbildningen kort ved at sige, at vi

sætter X lig c i polynomiet, og billedet af a = a(X) kalder vi for a(c). Da M[X] er en kommutativ ring med etelement, vil den ved homomorfien føres over i en kommutativ ring med etelement, og da billedet ligger i integritetsringen L, vil nulringen gælde for billedet; dette er derfor en integritetsring, og vi betegner den M[c], og kalder den for integritetsringen fremgået af M ved adjunktion af c; dens elementer er altså alle udtryk af formen $a_0 + a_1c + \ldots a_nc^n$, hvor alle a_j tilhører M.

Homomorfiens kerne er et ideal $I \subset M[X]$. Her gælder skarpt inklusionstegn, da de fra 0 forskellige konstanter $a_0 \in M$ er fixe ved afbildningen, og derfor ikke føres over i nulelementet og altså ikke tilhører kernen. Integritetsringen M[c] ses ifølge definition at være en realisation af faktorringen $(M[X],+,\cdot)/I$.

Der kan nu indtræffe to muligheder:

Enten er $I = \{0\}$, det trivielle nulideal. Så indeholder kernen kun et element, og homomorfien er bijektiv, altså en isomorfi. I så fald er $a(c) \neq 0$ for ethvert polynomium a forskelligt fra nulpolynomiet, og vi har isomorfien mellem M[X] og M[c], idet $a_0 + a_1X + \ldots + a_nX^n \leftrightarrow a_0 + a_1c + \ldots + a_nc^n$. I dette tilfælde siger vi, at c er transcendent over M. Eksempel: Lad $(L,+,\cdot)$ være de reelle tals legeme $(\acute{R},+,\cdot)$, og lad M være mængden af rationale tal $\acute{Q}$. Man kan vise, at $\pi = 3{,}14159..$ er transcendent over $\acute{Q}$ (beviset kræver en del teknik), og vi har isomorfi mellem $\acute{Q}[X]$ og $\acute{Q}[\pi] \subset (\acute{R},+,\cdot)$, idet $q_0+q_1X+\ldots q_nX^n \leftrightarrow q_0+q_1X+\ldots+q_n\pi^n$, alle q_j rationale.

Eller I er et ikke-trivielt ideal i M[X]. I dette tilfælde siger vi, at c er algebraisk over M. For ethvert $a(X) \in I$ bliver $a(c) = 0$, og vi siger, at c er rod i polynomiet a(X). Da M[X] er en hovedidealring bliver I netop mængden af multipla af et egentligt polynomium $d(X) \in M[X]$, og her må d(X) have en grad større

end 0, altså ikke være en konstant, fordi I er en ægte del af M[X]. Man har altså, at den nødvendige og tilstrækkelige betingelse for at c er rod i et polynomium a(X) er, at a(X) er delelig med d(X), hvor d(X) er et ved c bestemt polynomium; d(X) er bestemt entydigt pånær en konstant faktor, nemlig som et egentlig polynomium af lavest grad med c som rod.

Polynomiet d(X) er irreducibelt over M. Thi ellers kunne det skrives som et produkt $d_1(X) \cdot d_2(X)$, hvor begge faktorerne var af lavere grad, og derfor ikke delelige med d(X); idet nu $d(c) = d_1(c) \cdot d_2(c) = 0$, og nulreglen jo gælder i L, måtte c være rod i et af faktorpolynomierne, hvilket strider mod, at c kun er rod i polynomier, der er delelige med d(X).

Resultaterne kan sammenfattes i følgende sætning: Lad inte indeholde dellegemet (M,+,·) gritetsringen (L,+,·); ethvert $c \in L$ er enten transcendent over M, og i så fald er det ikke rod i noget polynomium fra M[X], eller også er det algebraisk over M, og i så fald er det rod i netop eet irreducibelt polynomium d(X) fra M[X] (dog kun entydigt pånær en konstant faktor), og samtlige polynomier i hvilke c er rod er netop de polynomier, der er delelige med d(X).

Hvis man indenfor en integritetsring (L,+,·) har en delintegritetsring M og et element c, så betegner man almindeligt med M[c] den mindste integritetsring indenfor (L,+,·), for hvilken $M \subsetneq M[c]$ og $c \in M[c]$. Vi siger, at M[c] er integritetsringen fremgået af M ved adjunktion af c (indenfor L). Benævnelsen ses at stemme overens med alt det foregående, og specielt bemærkes, at hvis man som L benytter M[X], så bliver M[X] virkelig den mindste integritetsring der indeholder X = (0,e,0,0,...).

For legemer benyttes analoge betegnelser med runde parenteser: Hvis man indenfor et legeme (L,+,·) har et dellegeme M og et element c, så betyder M(c) det mindste legeme indenfor (L,+,·) for

hvilket $M \subsetneq M(c)$ og $c \in M(c)$. Vi siger, at $M(c)$ er legemet fremgået af M ved adjunktion af c (indenfor L). Man ser, at $M(c)$ netop er brøklegemet for $M[c]$. Specielt ses, at $M(X)$ er mængden af "polynomiumsbrøker"

$$\frac{a_o+a_1X+\ldots+a_nX^n}{b_o+b_1X+\ldots+b_mX^m},$$

og at $M[X]$ er en ægte del af $M(X)$, idet f.eks. $\frac{1}{X} \notin M[X]$ (hvis $\frac{1}{X}$ var et polynomium skulle det have en ikke-negativ grad, og der fremkommer så en modstrid mod reglen om at graden af et produkt er summen af faktorernes grader). Hvis c er transcendent over M gælder det også, at $M[c]$ er en ægte del af $M(c)$, på grund af isomorfien mellem $M[X]$ og $M[c]$.

Derimod gælder der, at hvis c er algebraisk over legemat M, så er integritetsringen $M[c]$ et legeme og altså sit eget brøklegeme, så at $M[c] = M(c)$. Thi når c er algebraisk over M er det rod i et irreducibelt polynomium $d(X)$ over M, og så vil mængden I af multipla af $d(X)$ være et maximalideal i $M[X]$ (idet $I \subset I_1$ hvis og kun hvis det for frembringerelementerne gælder at d har d_1 som ægte divisor); ifølge en tidligere sætning er så $M[c] = M[X]/I$ et legeme. Da $M[c]$ er mængden af elementer af formen $a_o+a_1c+\ldots+a_nc^n$ betyder det, at kvotienten mellem to elementer af denne form atter kan skrives på samme form.

Eksempel: indenfor $(\dot{R},+,\cdot)$ er $\sqrt[3]{2}$ algebraisk over $(\dot{Q},+,\cdot)$, idet den er rod i det irreducible polynomium $X^3 - 2$; idet $\dot{Q}[\sqrt[3]{2}]$ er et legeme er det indenfor denne mængde altid muligt at "skaffe rational nævner", f.eks. er (tilfældige tal)

$$(3\sqrt[3]{2^2} - 2\sqrt[3]{2} + 4)^{-1} = \frac{1}{150}(-4\sqrt[3]{2^2} + 13\sqrt[3]{2} + 14).$$

Hvis $c \in M$, så er c algebraisk over M, idet c åbenbart er rod i polynomiet X-c, som tilhører M[X]; dersom c er rod i a(X), så er a(X) delelig med X-c. Heraf kan ses, at antallet af rødder i et polynomium er mindre end eller lig dets grad. Thi tager vi som M et legeme, der indeholder de rødder vi vil betragte, og desuden alle polynomiets koefficienter, så vil polynomiet tilhøre M[X], og vi kan inden for M[X] foretage en faktoropløsning, idet vi for enhver rod c får en faktor X-c i polynomiet, og antallet af disse faktorer er mindre end eller lig graden (herved benyttes sætningen om den entydige fremstilling som produkt af irreducible, og at førstegradspolynomier er irreducible).

Hvis $a(X) \in M[X]$ og $c \in M$, så vil $c \to a(c)$ være afbildning af M ind i M. Til ethvert polynomium a(X) svarer altså en "polynomiumsfunktion" $c \to a(c)$, og vi har med selvfølgelige kompositionsregler en homomorfi af M[X] ind i mængden af afbildninger af M ind i M. Disse polynomiumsfunktioner spiller som bekendt en stor rolle i analysen. I ethvert kommutativt legeme M kan den sædvanlige Lagranges interpolationsformel anvendes til at bestemme et polynomium, som for endelig mange givne $c_j \in M$ antager opgivne værdier $\in M$. Specielt ses heraf, at for et endeligt legeme er enhver afbildning af M ind i M en polynomiumsfunktion $c \to a(c)$ (hvor polynomiet a(X) endda ikke er entydig bestemt, idet man f.eks. altid til det kan addere $\Pi(X-c_j)$, hvor $\{c_j\} = M$). Hvis M er uendelig gælder noget tilsvarende ikke, og f.eks. en afbildning ved hvilken uendelig mange (men ikke alle) c_j afbildes i 0 er ikke en polynomiumsfunktion, da et polynomium kun har endelig mange rødder.

Vi har hidtil betragtet polynomier $d(X) \in M[X]$ og en integritetsring L med M som dellegeme, og så mødt muligheden af at et $c \in L$ kunne være rod i d(X). Dersom der findes en sådan rod c, så

er strukturen af legemet M(c) givet, nemlig som en kvotientring $(M[X],+,\cdot)/I$, hvor I er mængden af multipla af d(X). Men selvom vi kun har givet legemet M og et irreducibelt polynomium $d(X) \in M[X]$, så vil der altid findes et legeme $(L,+,\cdot)$ der har M som dellegeme og som indeholder en rod i d(X), nemlig løst sagt: den nævnte kvotientring. Udførligt: Mængden af multipla af d(X) er et ideal $I \subset M[X]$, og ifølge den almindelige homomorfisætning eksisterer der en homomorf afbildning $a = a(X) \to a'$ af M[X], ved hvilken I er kerne; billedet er en kvotientring $(M[X],+,\cdot)/I$, og den er et legeme fordi d er irreducibel så I er et maximalideal. Da $M \cap I = \{0\}$ bliver afbildningen af M's elementer injektiv, altså en isomorfi, og vi kan derfor identificere M's elementer med deres billeder, hvorved vi opnår at M er dellegeme af $(L,+,\cdot)$. Billedet af X vil vi kalde for c, og det vil i kvotientringen være rod i d(X), thi da alle elementerne i M , og altså specielt koefficienterne i d(X), er fixelementer ved afbildningen, vil $d(X) \to d(c)$, og da d(X) ligger i kernen er $d(c) = 0$.

Som et vigtigt eksempel kan betragtes polynomiet X^2+1, som er irreducibelt over de reelle tals legeme. Dette legeme kan udvides til et legeme, der indeholder en rod i polynomiet; en sådan rod kaldes sædvanligvis i, og $\mathbb{R}[i] = \mathbb{R}(i)$ er da de komplekse tals legeme $(\mathbb{C},+,\cdot)$. På et tidligere sted (i AG, II, §3) er komplexe tal konstrueret (v.hj. af talpar) som et mindste udvidelseslegeme af $(\mathbb{R},+,\cdot)$ der indeholdt en på særlig vis konstrueret løsning til $X^2 = -1$, men strukturen er den samme som strukturen af det her konstruerede $\mathbb{R}(i)$, thi ifølge det foregående er det strukturen af kvotientringen $\mathbb{R}[X]/I$, hvor I er hovedidealet frembragt af X^2+1.

Polynomiet X^2+1 kan i $\mathbb{R}(i)$ spaltes helt til bunds som et produkt af førstegradsfaktorer, nemlig $X^2+1 = (X-i)(X+i)$, og man ser almindeligt, at hvis man til et legeme adjungerer en rod i et

irreducibelt andengradspolynomium, så vil udvidelseslegemet indeholde begge polynomiets rødder. For polynomier af højere grad gælder noget tilsvarende ikke: f.eks. er X^3-2 irreducibelt over $(\dot{Q},+,\cdot)$, og $\dot{Q}(\sqrt[3]{2})$ indeholder en rod til polynomiet, men da $\dot{Q}(\sqrt[3]{2}) \subset \dot{R}$ kan det ikke indeholde nogen af de komplexe rødder, og først hvis man yderligere adjungerer en af disse får man et legeme, som indeholder alle tre rødder, og hvori polynomiet kan skrives som produkt af førstegradsfaktorer.

Hvis c er algebraisk over M gælder ifølge det tidligere, at $M(c) = \{a_0+a_1c+\ldots+a_mc^m\}$. Hvis det irreducible polynomium d(X) hvori c er rod er af grad n, kan man i fremstillingen af elementerne fra M(c) nøjes med exponenter $m < n$, thi ved at benytte $d(c) = 0$ kan man få c^n udtrykt som en linearkombination af lavere potenser af c, og ved gentagen anvendelse heraf kan man få bortskaffet alle potenser af c med exponent $\geq n$. F.eks. er jo $\dot{R}(i) = \{r_1+ir_2\}$. Dette fænomen skal vi nu nærmere undersøge.

Lad os betragte et legeme $(L,+,\cdot)$, som har et dellegeme M. Man kan da med legemets kompositionsregler + og · opfatte L som et vektorrum over legemet M, idet man altsaa opfatter dette sidste som skalarlegeme. For at godtgøre dette skal man eftervise, at de til definition af vektorrum benyttede betingelser V.1 - V.10 er opfyldt, men det ses let; betingelserne V.1 - V.5 omhandler kun vektoraddition og er opfyldt fordi (L,+) er en gruppe; betingelserne V.6 - V.9 omhandler regning med vektorer og skalarer, og er opfyldt fordi disse alle ligger i ringen $(L,+,\cdot)$; endelig omhandler V.10 eksistensen af en enhedsskalar, og er opfyldt, da M indeholder et etelement.

Dimensionen af L opfattet som vektorrum over M kaldes for graden af L over M og betegnes $[L:M]$. Denne grad angiver antallet af elementer i en basis for L over M. Som eksempel kan man betragte $L = M(c)$, hvor c er algebraisk over M; ifølge en tidligere sætning (S.19 øverst) kan man som en basis for M(c) benytte $1, c, c^2, \ldots, c^{n-1}$ (disse er lineært uafhængige, for ellers ville c være rod i et egentligt polynomium af lavere end n'te grad), og vi har altsaa, at $[M(c):M] = n$, hvor n er graden af det irreducible polynomium over M med c som rod. F.eks. er $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$.

Lad $(L,+,\cdot)$ have et dellegeme K og dette igen et dellegeme M, da er $[L:M] = [L:K][K:M]$. Bevis: Lad $\alpha_1, \ldots, \alpha_r$ være en basis for L over K, idet $[L:K] = r$, således at ethvert $l \in L$ på netop een måde kan skrives på formen

$$l = k_1 \alpha_1 + \ldots + k_r \alpha_r,$$

hvor alle $k_i \in K$; lad $\beta_1, \ldots, \beta_s$ være en basis for K over M, idet $[K:M] = s$, således at ethvert k_i på netop een måde kan skrives på formen

$$k_i = m_{i1}\beta_1 + \ldots + m_{is}\beta_s,$$

hvor alle $m_{ij} \in M$. Indsættes for k_i får man

$$(A) \qquad 1 = \sum_i \sum_j m_{ij}\,\alpha_i\beta_j,$$

således at ethvert 1 er en linearkombination af $\alpha_i\beta_j$ med koefficienter $m_{ij} \in M$, og desuden er fremstillingen entydig - således at elementerne $\alpha_i\beta_j$ udgør en basis - thi et udtryk af arten (A) kan jo skrives på formen

$$1 = \sum_i \left(\sum_j m_{ij}\beta_j\right)\alpha_i,$$

hvori parenteserne er elementer tilhørende K, og da $\{\alpha_i\}$ var en basis for L over K, bliver disse parenteser entydigt bestemt, og da $\{\beta_j\}$ var en basis for K over M, bliver dernæst elementerne m_{ij} entydigt bestemt. Men dette viser, at [L:M] er lig antallet elementer $\alpha_i\beta_j$, altså lig r·s, hvormed sætningen er bevist.

Hvis et legeme $(L,+,\cdot)$ har endelig mange elementer, er dets karakteristik et primtal p, og antallet af dets elementer er en potens af p. Thi (se AT 1,22) karakteristikken for L må være et primtal p, og primlegemet P for L (som jo var det mindste egentlige dellegeme af L) indeholder altså p elementer; endvidere må graden [L:P] være endelig, altså lig et tal n, således at der er en basis med n elementer $\alpha_1,\ldots,\alpha_n$, og dersom vi i fremstillingen

$$1 = p_1\alpha_1 + \cdots + p_n\alpha_n$$

lader alle p_i uafhængigt af hinanden gennemløbe P, får vi netop samtlige elementer $1 \in L$, og hvert kun en gang; antallet mulige valg af $p_1,\ldots,p_n$ ses at være p^n, og dette er altså elementantallet for L, hvormed sætningen er vist.

En udvidelse af et legeme $(M,+,\cdot)$ til et legeme M(c), hvor c er algebraisk over M, kaldes en simpel algebraisk udvidelse, og det blev foran vist, at graden [M(c):M] er endelig. Kombineres det-

te med den foregående sætning ses, at dersom et legeme L fremgår af et legeme M ved et endeligt antal sukcessive simple algebraiske udvidelser, så er [L:M] endelig.

Dersom man omvendt har et legeme $(L,+,\cdot)$ og et dellegeme M, og graden [L:M] er endelig, så kan L fremgå af M ved et endeligt antal sukcessive simple algebraiske udvidelser, og endvidere er ethvert element $c \in L$ algebraisk over M. Lad os bevise den sidste påstand først: Følgen $1, c, c^2, c^3, \ldots$ indeholder uendelig mange elementer, og disse kan derfor ikke være lineært uafhængige over M, og der findes derfor en egentlig linearkombination af dem, som er 0, men det betyder at c er rod i et polynomium over M, altså algebraisk over M. Dersom vi til M adjungerer et element $c \in L$, men hvor $c \notin M$, så er $[M(c):M] > 1$, og derfor $[L:M(c)] < [L:M]$, og ved et endeligt antal gentagelser af denne proces når vi frem til et legeme M^*, hvor $[L:M^*] = 1$, d.v.s. at $L = M^*$.

De foregående sætninger medfører, at dersom c_1 og c_2 er algebraiske over M, så er deres sum og deres produkt og deres differens og deres kvotient også algebraiske over M. Thi vi kan jo ved to simple algebraiske udvidelser nå fra M til et legeme $M(c_1,c_2)$, som indeholder dem begge, og da $[M(c_1,c_2):M]$ er endelig, er ethvert element fra $M(c_1,c_2)$ algebraisk over M. F.eks. er $\sqrt{2}+\sqrt{3}$ algebraisk over $(\mathbb{Q},+,\cdot)$; som et polynomium hvori størrelsen er rod kan nævnes $x^4 - 10\,x^2 + 1$.

Dersom c er transcendent over M, så er $[M(c):M] = \infty$, da elementerne $1, c, c^2, c^3, \ldots$ er lineært uafhængige over M.

Man bør bemærke, at det derimod meget vel er muligt, at $[L:M] = \infty$, selvom hvert enkelt element fra L er algebraisk over M. Som eksempel kan man betragte mængden A af alle reelle tal som er algebraiske over $(\mathbb{Q},+,\cdot)$; ifølge det ovenstående vil denne mængde med to elementer indeholde deres sum og produkt og differens og

kvotient, og mængden A er derfor et legeme. Dersom nu graden $[A:\mathbb{Q}] = n$, skulle ethvert $a \in A$ være rod i et irreducibelt polynomium over $\mathbb{Q}$ og af grad mindre end eller lig n, men dette er ikke tilfældet, da der findes irreducible polynomier over $\mathbb{Q}$ af vilkårlig høj grad, f.eks. $X^m - 2$ for alle m (dette kan f.eks. ses ved at benytte resultatet fra øvelse 14).

Iøvrigt kaldes A ofte for mængden af algebraiske tal, idet det altså er underforstået, at det er de reelle tal, som er algebraiske over det rationale legeme.

I begyndelsen af denne § har vi indført begrebet "polynomier af en variabel over et integritetsområde", idet et polynomium blot var et på en bestemt måde indiceret elementsæt (ofte kaldet "polynomiets koefficienter") fra integritetsområdet; for disse elementsæt indførtes bestemte regneregler, og X var en betegnelse for elementsættet $(0,1,0,0,\ldots)$. Vi skal nu betragte den tilsvarende indførelse af polynomier af flere variable, idet vi for tydelighedens skyld især vil betragte polynomier af to variable.

Lad $(M,+,\cdot)$ være et integritetsområde. Ved et <u>polynomium i to variable over M</u> forstås et sæt af elementer a_{jk}, hvor $j,k \in \{0\} \cup \mathbb{N}$, og således at kun endelig mange af dem er forskellige fra 0 (elementerne a_{jk} kaldes ofte "polynomiets koefficienter"). For disse elementsæt indføres addition, idet $a = \{a_{jk}\}$ og $b = \{b_{jk}\}$ får summen $c = \{c_{jk}\}$, hvor $c_{jk} = a_{jk}+b_{jk}$, og der indføres multiplikation, idet deres produkt $d = \{d_{jk}\}$ defineres ved

$$d_{jk} = \sum_{m=0}^{j} \sum_{n=0}^{k} a_{mn} b_{j-m,k-n}.$$

Disse polynomier ses let at udgøre et integritetsområde (smlgn. side 1 i denne §, vedrørende nulreglen se også nedenfor . Hvis man definerer X_1 som elementsættet a, hvor $a_{10} = 1$ medens alle andre $a_{jk} = 0$, og endvidere definerer X_2 som elementsættet b, hvor $b_{01} = 1$ medens alle andre $b_{jk} = 0$, ser man, at $a = \{a_{jk}\}$ bliver lig $\sum\sum a_{jk} X_1^{\,j} X_2^{\,k}$. Ved de videre regninger med polynomierne er det lettest at benytte dette udtryk og betegne polynomiet $a(X_1,X_2)$. <u>Integritetsområdet af polynomier i to variable over M betegnes $M[X_1,X_2]$,</u> og man ser af udtrykket, at det er det samme som man ville få, dersom man først betragtede integritetsområdet af polynomier $M[X_1]$ over M (hvor vi har skrevet X_1 i st.f. X), og dernæst over

dette betragtede integritetsområdet af polynomier, altså $(M[X_1])[X_2]$ (hvor vi har skrevet X_2 i st.f. X). Denne sidste betragtning viser også, at der virkelig bliver tale om et integritetsområde, således at nulreglen gælder.

Man bemærker, at $M[X_1]$ ikke er noget legeme, og man kan derfor ikke slutte, at $(M[X_1])[X_2] = M[X_1,X_2]$ er en hovedidealring. At dette sidste virkelig ikke er tilfældet kan ses af at mængden af polynomier $a(X_1,X_2)$ uden konstantled, d.v.s. for hvilke $a_{00} = 0$, er et ideal, som ikke er noget hovedideal. Vi skal ikke gå nærmere ind på hvorledes man alligevel kan vise en sætning om entydig faktoropløsning.

Lad integritetsområdet $(M,+,\cdot)$ være indeholdt i et integritetsområde $(L,+,\cdot)$, og lad endvidere $c_1 \in L$ og $c_2 \in L$. Ved $M[c_1,c_2]$ forstås det mindste integritetsområde (indenfor L), som indeholder M og c_1 og c_2; det siges at være fremgået ved adjunktion af c_1 og c_2 til M, og dets elementer er netop samtlige udtryk $\sum\sum m_{jk}c_1^{\,j}c_2^{\,k}$. Man ser, hvorledes benævnelsen stemmer med det foregående, idet man ved dannelsen på denne måde af $M[X_1,X_2]$ som L benytter det tidligere definerede $M[X_1,X_2]$. Uden at gå nærmere ind derpå, skal vi bemærke, at man for legemer benytter tilsvarende betegnelser med rund parentes.

På ganske analog måde kan man definere integritetsområdet $M[X_1,\ldots,X_n]$ af polynomier i n variable over M, og man ser, at man får inklusionskæden

$$M \subset M[X_1] \subset M[X_1,X_2] \subset \ldots \subset M[X_1,\ldots,X_{n-1}] \subset M[X_1,\ldots,X_n],$$

i hvilken ethvert led er et integritetsområde $M^{(j)}$, og det påfølgende led er ringen af polynomier (i en variabel) derover,

altså $M^{(j)}[X_{j+1}] = M^{(j+1)}$.

For et polynomium $a(X_1,\ldots,x_n)$ definerer man graden (= deg a) som den maximale værdi af summen af eksponenterne til $X_1,\ldots,X_n$. Der gælder så, at graden af et produkt er summen af faktorernes grader, deg ab = deg a + deg b. Vi nøjes med at give beviset for n = 2, det gennemføres for vilkårligt n på analog måde. Lad

$$a = \sum_{j,k} a_{jk} X_1^{\,j} X_2^{\,k} \quad \text{og} \quad b = \sum_{l,m} b_{lm} X_1^{\,l} X_2^{\,m} ,$$

hvor alle a_{jk} og b_{lm} er ulig 0; deg a = max(j+k) og deg b = max(l+m). Ved multiplikationen fremkommer led med eksponentsummen $(j+l)+(k+m) \leq$ deg a + deg b, og produktets grad kan derfor ikke være større end dette tal; det kan nu ske, at nogle af leddene ophæver hinanden, men tager man fra a leddet (entydigt bestemt) med j+k = deg a og hvor j er maximal, og fra b leddet med l+m = deg b og l maximal vil det i produktet give et led af grad deg a + deg b, og med en maximal eksponent til X_1 som ikke nås af andre led af denne grad, og med en koefficient $a_{jk}b_{lm} \neq 0$.

Selvom (M,+,·) er et legeme vil - som foran bemærket - polynomier i flere variable over M ikke udgøre en hovedidealring, men vi vil vise, at de dog udgør en integritetsring med entydig faktorisering. Der gælder : Dersom (I,+,·) er en integritetsring med entydig faktorisering, så har integritetsringen I[X] af polynomier over I også entydig faktorisering.

Først skal vises: Hvis Π er et primideal i integritetsringen $(I,+,\cdot)$, så er $\Pi[X]$ et primideal i $I[X]$. Vi skal altså vise, at hvis $a(X) \notin \Pi[X]$ og $b(X) \notin \Pi[X]$, så vil $a(X)b(X) \notin \Pi[X]$. Lad a have koefficientsættet $(a_0,a_1,\ldots)$, og lad heri a_j være den første koefficient, som ikke tilhører Π, og lad b have koefficientsættet $(b_0,b_1,\ldots)$ hvor b_k er den første koefficient, som ikke tilhører Π. I produktet vil koefficienten til X^{j+k} være lig

$$(a_0b_{j+k} + \ldots + a_{j-1}b_{k+1}) + a_jb_k + (a_{j+1}b_{k-1} + \ldots + a_{j+k}b_0),$$

og da alle de første a_r tilhører Π vil hele første parentes tilhøre Π, og analogt ses at anden parentes tilhører Π, men midterleddet vil ikke tilhøre Π fordi hverken a_j eller b_k gør det, og Π var et primideal; koefficienten til X^{j+k} tilhører altså ikke Π, hvormed lemmaet er vist, idet det ses, at $\Pi[X]$ opfylder Id1 og Id2.

Lad nu $(I,+,\cdot)$ være en integritetsring med entydig faktorisering, og lad dens brøklegeme hedde M. Så gælder Gauss' Sætning: Hvis $p(X) \in I[X]$, og $p(X)$ er reducibel i $M[X]$, så er $p(X)$ også reducibel i $I[X]$. Thi lad to polynomier (ikke konstanter) fra $M[X]$ have produktet $p(X)$, så kan man ved at multiplicere hvert af dem med fællesnævneren for koefficienterne opnå to polynomier $\in I[X]$, hvis produkt er $mp(X)$, hvor $m \in I$; lad f_a hhv. f_b betegne en største fælles divisor indenfor I (eksisterende!) for koefficienterne i det første hhv. det andet polynomuim, vi har da

$$m \cdot p(X) = f_a \cdot a(X) \cdot f_b \cdot b(X),$$

hvor koefficienterne i a(X) hhv. b(X) tilhører I, men ikke har nogen fælles ikke-regulær divisor. Dernæst bortforkortes heri de fælles irreducible faktorer (tilhørende I) for m og f_a og f_b, og herved bliver hele m bortforkortet, for hvis der fra m resterede en irreducibel faktor i_r, så ville (i_r) være primideal Π (og maximalideal) i I, og venstresiden ville tilhøre $\Pi[X]$, medens a(X) og b(X) med sikkerhed ikke gør det, og enten f_a eller f_b måtte altså gøre det, d.v.s. være delelig med i_r. Men når hele m er bortforkortet har vi åbenbart p(X) skrevet som et produkt indenfor I[X].

Vi skal dernæst udnytte den entydige faktorisering i $(I,+,\cdot)$ til at vise, at dersom p(X) og q(X) er irreducible polynomier, ikke konstanter, i I[X] og de er associerede i M[X], så er de også associerede i I[X]. Når p(X) er irreducibel i I[X] kan dets koefficienter ikke have nogen fælles ikke-regulær divisor fra I, thi ellers kunne en sådan jo trækkes ud som en faktor $\in$ I[X], og tilsvarende gælder for q(X). At de er associerede i M[X] betyder, at deres forhold er en konstant $\in$ M, altså en uforkortelig brøk $\frac{a}{b}$, hvor $a,b \in I$; men så er $bp(X) = aq(X)$, hvilket viser, at a går op i alle koefficienterne på venstre side, og da a ikke har faktorer fælles med b må a gå op i alle koefficienter i p(X), altså være regulær, og tilsvarende ses at b er regulær, alt i I. Heraf følger, at $\frac{a}{b}$ er regulær i I, hvilket viser påstanden.

Vi kan nu let vise den annoncerede sætning, altså at hvis integritetsringen $(I,+,\cdot)$ har entydig faktorisering, så

har I[X] det også. For lad indenfor I[X]

$$p_1'(X)\cdot,\ldots\cdot p_r'(X)\cdot i_1' \ldots i_s' = p_1''(X) \ldots p_t''(X)\cdot i_1'' \ldots i_v''$$

være produkter af irreducible elementer, som hvis de er konstanter (altså irreducible i I) er betegnet i_j og hvis de ikke er konstanter er betegnet $p_j(X)$. Vi kan nu opfatte ligningen som en ligning indenfor M[X], derved bliver konstanterne alle regulære, og ifølge Gauss' sætning er alle $p_j(X)$ irreducible (de er ikke reducible, og åbenbart heller ikke regulære); da vi fra tidligere ved, at der gælder entydig faktorisering i M[X] , må alle $p_j'(X)$ og $p_j''(X)$ være parvis associerede i M[X], og ifølge den lige beviste hjælpesætning er de så også associerede i I[X]. Bortforkortes alle $p_j(X)$ vil der restere to produkter af irreducible fra I, og disse er også parvis associerede p.g.a. den entydige faktorisering i I. Dermed er beviset fuldført.

Vi har nu: <u>Når (I,+,·) er en integritetsring med entydig faktorisering - specielt kan det være et kommutativt legeme [+]) - så er der entydig faktorisering i integritetsringen $I[X_1,\ldots,X_n]$ af polynomier i n variable over I</u>. Påstanden følger umiddelbart af den viste sætning ved induktion efter n.

[+]) I et kommutativt legeme er alle elementer $\neq 0$ regulære, så "entydig faktorisering" er indholdsløs. Det bemærkes, at i noterne siderne 2,22-30 (gammelt tryk) skal der overalt ved ordet "legeme" tilføjes "kommutativt".

Eksempel: I $(I,+,\cdot) = \mathbb{Z}[2i]$ er der ikke entydig faktorisering, og elementerne ± 2 og $\pm 2i$ er irreducible (AT 3,16); i $I[X]$ er der heller ikke entydig faktorisering, f.eks. er i ligningen $(2X+2i)(2X-2i) = 2\cdot 2\cdot(X^2+1)$ alle faktorerne irreducible.

Eksempel: Man betragter X^2+Y^2-e over et legeme med et-element e. Hvis det er reducibelt er det produkt af to førstegradspolynomier, altså af typen $(aX+bY+c)$; sættes $X = \pm e$ bliver polynomiet til Y^2, og faktorerne må i så fald være reduceret til formen bY, og $X = \pm e$ er altså rødder i $aX+c$; men da antallet rødder i et polynomium er $\leq$ graden fås en modstrid, således at polynomiet er irreducibelt, dette såfremt $e \neq -e$. Hvis legemet har karakteristik 2 er $e = -e$, og i dette tilfælde er virkelig

$$X^2+Y^2-e = (X+Y-e)^2.$$

Eksempel: Polynomiet X^m-2 er irreducibelt over $\mathbb{Q}$ (omtalt side 25). Ifølge Gauss' sætning er det nok at betragte $X^m-2 = p(X)q(X)$ indenfor $\mathbb{Z}[X]$. Koefficienterne i p og q betegnes $p_0,p_1,\ldots$ og $q_0,q_1,\ldots$, og vi kan gerne antage $p_0 = 2$ og $q_0 = -1$ (da vi evt. kan ombytte p og q og skifte fortegn for dem). Nu kan $p(X)$ ikke have lutter lige koefficienter, og lad p_j være den første ulige, så vil X^j i produktet få koefficienten $p_0q_j+p_1q_{j-1}+\ldots+p_jq_0$, som er ulige, altså er $j \geq m$, så at deg $p \geq m$, hvilket viser det ønskede.

Lovet bevis: Den øverst s.5.4a nævnte sætning ses let, thi i $I[X]$ er $rX-s$ irreducibel, og ifølge Gauss er derfor $ma(X) = (rX-s)\cdot b(X)$ i $I[X]$, hvoraf ses, at r og s går op som påstået.

altså $M^{(j)}[X_{j+1}] = M^{(j+1)}$.

Vi antager, at $(M,+,\cdot)$ består af mere end nulelementet (for ellers ville alt blive trivielt), og lad M være indeholdt i integritetsområdet $(L,+,\cdot)$, og lad $c_1,\ldots,c_n$ være elementer fra L. Der findes netop een homomorf afbildning af $M[X_1,\ldots,X_n]$ ind i L, ved hvilken M's elementer er fixelementer, og således at $X_j \to c_j$ for $j = 1,\ldots,n$, nemlig den afbildning som vi kort kan beskrive ved at sige, at vi for ethvert polynomium sætter $(X_1,\ldots,X_n)$ lig $(c_1,\ldots,c_n)$ i polynomiet, og billedet af $a = a(X_1,\ldots,X_n)$ kalder vi $a(c_1,\ldots,c_n)$. Billedmængden af $M[X_1,\ldots,X_n]$ bliver netop $M[c_1,\ldots,c_n]$.

Ved denne homomorfi kan der indtræffe to muligheder: Enten er afbildningens kerne lig $\{0\}$, det trivielle nulideal. Så indeholder kernen kun et element, og afbildningen er bijektiv, altså en isomorfi. I så fald er $a(c_1,\ldots,c_n) \neq 0$ for ethvert polynomium a forskelligt fra nulpolynomiet. I dette tilfælde siger vi, at $c_1,\ldots,c_n$ er algebraisk uafhængige over M. For $n = 1$ betyder algebraisk uafhængig det samme som transcendent. Trivielt – men opmærksomhed værdigt – er det, at indenfor $M[X_1,\ldots,X_n]$ er $X_1,\ldots,X_n$ algebraisk uafhængige, idet ethvert polynomium a forskelligt fra nulpolynomiet er forskelligt fra 0 (= nulpolynomiet). I modsat fald, altså hvis $a(c_1,\ldots,c_n)$ kan blive 0 for et egentligt polynomium a, siger vi, at $c_1,\ldots,c_n$ er algebraisk afhængige over M. F.eks. er de reelle tal π og $\sqrt{\pi}$ algebraisk afhængige over $\mathbb{Q}$.

Ved et symmetrisk polynomium $a = a(X_1,\ldots,X_n) \in M[X_1,\ldots,X_n]$ forstås et polynomium, som overføres i sig selv ved enhver permutation af $X_1,\ldots,X_n$. F.eks. er $3X_1^2X_2 + 3X_2^2X_1$ et symme-

trisk polynomium i $\hat{Q}[X_1,X_2]$. Da regning med symmetriske polynomier fører til symmetriske polynomier igen, er mængden af symmetriske polynomier åbenbart en delring af $M[X_1,\ldots,X_n]$.

Vigtige eksempler på symmetriske funktioner er de elementarsymmetriske funktioner i $M[X_1,\ldots,X_n]$

$$s_1 = X_1+X_2+\ldots+X_n,$$
$$s_2 = X_1X_2+X_1X_3+\ldots+X_{n-1}X_n,$$
$$\ldots\ldots\ldots$$
$$s_n = X_1X_2\ldots X_n,$$
$$s_r = 0 \quad \text{for } r > n,$$

som defineres ved at s_j er summen af alle mulige forskellige produkter af j forskellige af $X_1,\ldots,X_n$.

Der gælder nu den vigtige sætning: De elementarsymmetriske funktioner $s_1,\ldots,s_n$ er algebraisk uafhængige indenfor $M[X_1,\ldots,X_n]$, og endvidere er $M[s_1,\ldots,s_n]$ netop ringen af symmetriske polynomier i $M[X_1,\ldots,X_n]$. Anderledes udtrykt udsiger sætningen, at ethvert symmetrisk polynomium kan udtrykkes på netop een måde ved hjælp af de elementarsymmetriske funktioner.

Vi har $M[X_1,\ldots,X_{n-1}] \subset M[X_1,\ldots,X_n]$, og lad os i det følgende bevis kort betegne dem henholdsvis $M^{(n-1)}$ og $M^{(n)}$. Endvidere bemærker man, at dersom man sætter $X_n = 0$ i en symmetrisk funktion fra $M^{(n)}$ fremkommer der en symmetrisk funktion i $M^{(n-1)}$, og specielt vil s_j fra $M^{(n)}$ gå over i s_j fra $M^{(n-1)}$.

Beviserne for sætningens to dele føres ved induktion efter n.

Først den algebraiske uafhængighed: Lad a være et egentligt polynomium i n variable, vi skal vise, at $a(s_1,\ldots,s_n)$ er et egentligt polynomium i $M^{(n)}$. Først udtrækker vi af $a(s_1,\ldots,s_n)$ faktoren s_n så mange gange som det er muligt, så at $a(s_1,\ldots,s_n) =$

$s_n^k \cdot b(s_1,\ldots,s_m)$, hvor b er et polynomium med mindst et led (ikke-forsvindende), der ikke indeholder s_n som faktor, eller anderledes udtrykt, hvor $b(s_1,\ldots,s_{n-1},0)$ ikke er et nulpolynomium i $s_1,\ldots,s_{n-1}$. Da $s_n^k = (X_1\ldots X_n)^k$ skal vi blot vise, at $b(s_1,\ldots,s_n)$ ikke er nulpolynomiet i $X_1,\ldots,X_n$, og det gør vi ved at sætte $X_n = 0$ i det, hvorved netop fremkommer det samme som ved i $b(s_1,\ldots,s_{n-1},0)$ at indsætte de elementarsymmetriske funktioner fra $M^{(n-1)}$, og det er ifølge induktionsforudsætningen et egentligt polynomium.

Dernæst den anden del af sætningen: Vi skal vise, at et symmetrisk polynomium $p(X_1,\ldots,X_n)$ fra $M^{(n)}$ kan fremstilles ved hjælp af $s_1,\ldots,s_n$. Vi betragter $p(X_1,\ldots,X_{n-1},0)$ som er en symmetrisk funktion fra $M^{(n-1)}$, og ifølge induktionsforudsætningen er den lig et polynomium $a(s_1,\ldots,s_{n-1})$ i de elementarsymmetriske funktioner fra $M^{(n-1)}$. Vi betragter nu indenfor $M^{(n)}$ funktionen $d(X_1,\ldots,X_n) = p(X_1,\ldots,X_n) - a(s_1,\ldots,s_{n-1})$, sætter man $X_n = 0$ i d bliver det nulpolynomiet, men det vil sige, at samtlige ikkeforsvindende led i d har X_n som faktor, og som differens mellem to symmetriske funktioner er d selv symmetrisk, så at alle dens led har $X_1\ldots X_n = s_n$ som faktor, og kvotienten $p_1 = d:s_n$ bliver igen symmetrisk. Vi har altså opnået, at

$$p(X_1,\ldots,X_n) = a(s_1,\ldots,s_{n-1}) + s_n \cdot p_1(X_1,\ldots,X_n),$$

hvor p_1 er symmetrisk og af lavere grad end p. Derpå kan man gentage processen med p_1 o.s.v., og i løbet af endelig mange skridt bliver man færdig.

Uden nærmere definition ses, at hovedsætningen mere slående kan udtrykkes: De elementarsymmetriske funktioner $s_1,\ldots,s_n$ udgør en "algebraisk basis" for de symmetriske polynomier i $M[X_1,\ldots,X_n]$.

Et polynomium, hvis højestegradskoefficient er etelementet, kaldes monisk. Det moniske polynomium med rødder $X_1,\ldots,X_n$ er $(X-X_1)(X-X_2)\ldots(X-X_n)$, og multipliceres ud får man netop $X^n-s_1X^{n-1}+s_2X^{n-2}-\ldots\pm s_n$, så at i det moniske polynomium med rødder $X_1,\ldots,X_n$ er koeffocienten til X^{n-j} lig $(-1)^j s_j$.

Man bemærker også, at ethvert element i brøklegemet $M(X_1,\ldots,X_n)$ som ved enhver permutation af $X_1,\ldots,X_n$ går over i sig selv, vil tilhøre $M(s_1,\ldots,s_n)$.

Eksempel: I $M(a,b,c)$ er

$$U = \frac{a}{b}+\frac{a}{c}+\frac{b}{c}+\frac{b}{a}+\frac{c}{a}+\frac{c}{b} = \frac{a^2c+a^2b+b^2a+b^2c+c^2b+c^2a}{abc}$$

åbenbart symmetrisk i a,b,c, og det kan skrives med fællesnævneren s_3. For at udtrykke den store tæller ved s_1,s_2,s_3 kan vi sætte c=0 (smlgn. beviset forrige side), hvorved fås a^2b+b^2a, som i $M[a,b]$ er lig s_1s_2; så er tælleren (stadig ifølge beviset) af formen $s_1s_2-s_3\cdot p(s_1,s_2,s_3)$, og ved udregning findes let $p = 3$. Altså er

$$U = \frac{s_1s_2 - 3\,s_3}{s_3} \quad ;$$

hvis a,b,c er rødderne $\in \mathbb{C}$ til polynomiet $X^3 - 4X + 1$ er $s_1 = 0$, $s_2 = -4$, $s_3 = -1$, og man får $U = -3$.

Øvelser til § 5.

1) Lad M være en integritetsring. Mængden af følger $(a_0,a_1,\ldots)$ af elementer fra M kan organiseres som en ring M[[X]], idet man definerer addition og multiplikation på ordret samme måde, som det på tekstens side 1 er gjort for polynomier. Idet X betegner følgen $(0,e,0,\ldots)$, kan følgen $(a_0,a_1,\ldots)$ opfattes som en formel potensrække $a(X)=a_0+a_1X+a_2X^2+\ldots$, og M[[X]] betegnes sompotensrækkeringen over M; den vil som delring have polynomiumsringen over M. Godtgør, at M[[X]] er en integritetsring.

Vis, at de regulære elementer i M[[X]] netop er følgerne $(a_0,a_1,\ldots)$, hvor a_0 er regulær i M.

2) Undersøg brøklegemet for potensrækkeringen M[[X]] (se øv.1) over et kommutativt legeme M, og vis, at det er integritetsringen der fremgår ved adjunktion af $\frac{1}{X}$ til M[[X]].

3) Bestem samtlige idealer i potensrækkeringen M[[X]] (se øv.1) over et kommutativt legeme M, og vis, at bortset fra nulidealet kan de ordnes i en "nedstigende kæde" $I \supsetneq I' \supsetneq I'' \supsetneq \ldots$. Vis, at M[[X]] er en hovedidealring. Angiv (pånær isomorfi i billedet) samtlige homomorfe afbildninger af M[[X]].

4) Indenfor potensrækkeringen M[[X]] (se øv.1) over et kommutativt legeme M betragtes mængden L af potensrækker a(X) hvori $a_1 = 0$. Vis, at $(L,+,\cdot)$ er en integritetsring. Bestem de irreducible elementer i $(L,+,\cdot)$. Vis, at der findes hovedidealer (d) frembragt af irreducible elementer d(X) således

at nulreglen ikke gælder i faktorringen $(L,+,\cdot)/(d)$. Bestem samtlige idealer i $(L,+,\cdot)$, og gør rede for at det ikke er en hovedidealring. Giv et konkret eksempel på et element, som på to væsentlig forskellige måder kan skrives som produkt af irreducible.

5) Bestem samtlige endomorfier (d.v.s. homomorfier ind i sig selv), ved hvilke M's elementer er fixe, af potensrækkeringen M[[X]] over et legeme M, og angiv specielt samtlige automorfier (d.v.s. isomorfier ind på sig selv).

6) Bestem samtlige endomorfier, ved hvilke M's elementer er fixe, af polynomiumsringen M[X] over et legeme M, og angiv specielt samtlige automorfier.

7) Vis, at en homomorfi af en integritetsring $(M,+,\cdot)$ på en integritetsring $(L,+,\cdot)$ kan udvides til en homomorfi af M[X] på L[X], ved hvilken $X \in M[X]$ afbildes i $X \in L[X]$. De egentlige polynomier $a(X) \in \acute{Z}[X]$ kan opdeles i ækvivalensklasser $(a(X))'$ af indbyrdes proportionale. Vis, at dersom a(X) kan skrives som produkt $b(X)\cdot c(X)$ af to polynomier af lavere grad fra $\acute{Z}[X]$, så gælder det samme for ethvert polynomium i klassen $(a(X))'$ (vis først ud fra homomorfien $(\acute{Z},+,\cdot) \to (Z_p,+,\cdot)$, at hvis alle koefficienter i a(X) har et primtal p som fælles divisor, så gælder det samme for b(X) eller c(X)).

Mængden af ækvivalensklasserne betegnes M', og det foregående giver en klassemultiplikation. Vis, at for strukturen $(M',\cdot)$ gælder, at ethvert element på en og kun een måde kan skrives som produkt af irreducible. Gør rede for at de irreducible elementer

i $\acute{Z}[X]$ er dels $\pm$ primtallene, og dels de polynomier, som er irreducible over $\acute{Q}[X]$, og hvori koefficienterne ikke har nogen fælles faktor større end 1. Vis, at hovedsætningen om altid mulig og væsentlig entydig primopløsning gælder i $\acute{Z}[X]$ (skønt $\acute{Z}[X]$ som omtalt i texten ikke er en hovedidealring).

8) Vis, at polynomiet $a(X) = (X-1)(X-2)\ldots(X-n) - 1$ er irreducibelt indenfor $\grave{Z}[X]$ (og dermed ifølge øv. 7 indenfor $\grave{Q}[X]$). (til hjælp: betragt $a(X) = b(X)c(X)$ for $X = 1,2\ldots,n$).

9) Angiv legemer, dellegemer af $(\acute{C},+,\cdot)$ og så små som muligt, indenfor hvilke hhv. $X^3-1, X^3-8, X^4-1, X^4-8$ kan skrives som produkt af førstegradsfaktorer.

10) Lad $(M,+,\cdot)$ være et legeme med to elementer, f.eks. legemet $(\grave{Z}_2,+,\cdot)$ Undersøg, om $a(X) = X^2 + X + e$ er et irreducibelt polynomium i $M[X]$. Lad c være en vilkårlig rod i $a(X)$. Opskriv samtlige elementer i $M(c)$, og angiv deres antal og hvilke af dem, der er rødder i $a(X)$.

Idet man i stedet for $(M,+,\cdot)$ benytter et legeme $(N,+,\cdot)$ med tre elementer, f.eks. $(\grave{Z}_3,+,\cdot)$, og nu $a(X) = X^2 + X + e \in N[X]$, ønskes de samme spørgsmål besvaret. Bogstavet e betegner etelementet.

11) I det følgende er a et helt tal forskelligt fra -1, og

$$p(X) = (X-1)(X+1)(X-a) + 1 = (a+1) - X - aX^2 + X^3.$$

Vis, at betragtet som element i polynomiumsringen $\grave{Q}[X]$ er $p(X)$ irreducibel. Hvad kan man sige om $p(X)$ betragtet som element i $\grave{Z}[X]$?

Vis, at betragtet som element i potensrækkeringen $\grave{Q}[[X]]$ er $p(X)$

regulær (potensrækkering defineret i øv. 1).
Undersøg for a = -2, a = 1 og a = 5 om p(X) betragtes som element i $\dot{Z}[[X]]$ er regulær, reducibel eller irreducibel. Hvis p(X) er reducibel ønskes angivet de tre første koefficienter i to ikke-regulære potensrækker, der har p(X) som produkt.

12) Lad (P,+,·) være et legeme med to elementer, f.eks. $(\dot{Z}_2,+,\cdot)$; etelementet betegnes e, og nulelementet o. Vis, at $X^3 + X^2 + e$ er irreducibel over P. En rod i dette polynomium betegnes c; vis, at P(c) har 8 elementer, og at disse alle er rod i $X^8 - X$. Vis, at der ikke findes noget legeme K, så $P \subset K \subset P(c)$.

13) Lad (L,+,·) være et legeme med 3 elementer, f.eks. $(\acute{Z}_3,+,\cdot)$; etelementet betegnes e og nulelementet betegnes o. Vis, at polynomiet $X^2 + e$ er irreducibelt over L.
Idet en rod i dette polynomium betegnes c, skal man undersøge strukturen af L(c), idet antallet af elementer bestemmes, og det undersøges om grupperne (L(c),+) og $L(c)\setminus\{o\},\cdot)$ er cykliske.

14) Vis, at legemet A af de reelle algebraiske tal (se side 25) er "algebraisk afsluttet" indenfor de reelle tal, hvormed menes, at ethvert reelt tal, som er algebraisk over A, vil tilhøre A. Godtgør, at $[\acute{R}:A] = \infty$. Findes der irreducible polynomier over A af højere end første grad ?

15) Vis, at når $f_h(X,Y)$ betegner det homogene polynomium bestående af leddene af maximal grad i polynomiet $f(X,Y)$, så vil f_h irreducibel medføre f irreducibel.

Vis, at for alle a er

$$f(X,Y) = X^4 + Y^4 + 4X^2 + 4Y^2 + a$$

irreducibel over $\dot{\mathbb{Q}}$.

Vis, at for netop èn værdi af a er dette f reducibelt over $\dot{\mathbb{R}}$, og angiv faktoropløsningen.

16) Vis, at hvis $a(X) \in I[X]$, hvor I er en integritetsring og Π et primideal i denne, og

$$a(X) = a_o + a_1X + \ldots + a_nX^n,$$

med $a_o, a_1, \ldots, a_{n-1} \in \Pi$ medens $a_n \notin \Pi$, så vil a reducibel medføre at a_o er produkt af to elementer, begge $\in \Pi$ ("Eisensteins kriterium", smln. eks. X^m-2 på side 27$^{e}_{e}$, som er et specialtilfælde).

17) Vis v.hj.a. Eisensteins kriterium (øv16), at

$$f(X) = X^{p-1}+X^{p-2}+\ldots+X+1 = \frac{X^p-1}{X-1}$$

er irreducibelt over $\dot{\mathbb{Q}}[X]$; p er et primtal. (Benyt, at $f(X)$ reducibel $\Leftrightarrow$ $f(X+1)$ reducibel).

18) Bestem det moniske polynomium af 3'grad, hvis rødder er kvadraterne på de tre rødder $\in \dot{\mathbb{C}}$ til polynomiet $X^3+dX^2+eX + f$, og angiv det moniske polynomium, hvis rødder er de reciprokke af kvadraterne.

19) Man betragetr i $M(a,b,c,d)$ den symmetriske sum U af led af formen $\frac{1}{a^2b}$. Hvor mange led indeholder U? FindU udtrykt ved de elementarsymmetriske funktioner af a,b,c,d. Bestem værdien af U når a,b,c,d er rødderne $\in \dot{\mathbb{C}}$ til X^4+X^3-7X+2.

27. De i det følgende betragtede legemer er dellegemer af de komplekse tals legeme.
Vis, at polynomiet $X^3 - X^2 - 1$ er irreducibelt over de rationale tals legeme $\mathbb{Q}$. En rod i dette polynomium kaldes c; angiv graden $[\mathbb{Q}(c):\mathbb{Q}]$.
Angiv endvidere graden $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$, og vis ved hjælp af denne, at $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(C) = \mathbb{Q}$. Bestem graden $[\mathbb{Q}(\sqrt{2},c):\mathbb{Q}]$, (hvor $\mathbb{Q}(\sqrt{2},c)$ betyder de mindste legeme, som indeholder $\sqrt{2}$ og c).
Man betragter desuden legemet $\mathbb{Q}(c\sqrt{2})$; godtgør, at graden $[\mathbb{Q}(c\sqrt{2}:\mathbb{Q}]$ går op i 6.
Vis, at $c = c^4 - c^2 - 1 \in \mathbb{Q}(c\sqrt{2})$, og benyt dette til at udlede at $\mathbb{Q}(c\sqrt{2}) = \mathbb{Q}(\sqrt{2},c)$.

28. Indenfor $M[X_1,\ldots,X_n]$ betragtes potenssummerne $P_h = X_1^h + \ldots + X_n^h$. Find P_1, P_2 og P_3 udtrykt ved de elementarsymmetriske funktioner

29. Godtgør, at $X_1, \ldots, X_n$ er rødder i polynomiet $X^n - s_1X^{n-1} + s_2X^{n-2} + \ldots + (-1)^n s_n$, og vis, at for $h > n$ gælder følgende formel mellem potenssummerne (se. øv. 28) og de elementarsymmetriske funktioner

$$P_h - s_1P_{h-1} + s_2P_{h-2} - \ldots + (-1)^n s_nP_{h-n} = 0.$$

Find for $h \leq n$ en formel, der forbinder $P_1, \ldots, P_h$ og de elementarsymmetriske funktioner.

Mere om grupper.

Tidligere er defineret produktet (det "Cartesiske produkt") af to mængder X og Y som mængden af ordnede par (x,y) af elementer fra mængderne, - om man vil, kan det også udtrykkes som mængden af afbildninger af parret (1,2), hvorved 1 afbildes ind i x og 2 afbildes ind i y.

Udfra to givne grupper $(G,\cdot)$ og $(H,\cdot)$, (vi benytter samme kompositionstegn i dem), kan man analogt danne deres direkte produkt betegnet $(G,\cdot) \times (H,\cdot)$, hvormed man mener en gruppe, hvis elementer er par (g,h), hvor $g \in G$ og $h \in H$, og hvor kompositionen skal være komponentvis komposition : $(g,h)\cdot(g',h') = (g\cdot g', h\cdot h')$. Det er nemlig klart, at der derved er defineret en associativ komposition på G×H, og der er et neutralelement (e_1,e_2) dannet af neutralelementerne i hhv. $(G,\cdot)$ og $(H,\cdot)$, og som det inverse $(g,h)^{-1}$ har man (g^{-1}, h^{-1}). Man bemærker, at det direkte produkt af to abelske grupper igen er en abelsk gruppe.

Når man taler om direkte produkt af grupper, ser man ofte bort fra isomorfi, således at enhver gruppe, der er isomorf med den ovenfor definerede $(G,\cdot) \times (H,\cdot)$, betegnes som direkte produkt af $(G,\cdot)$ og $(H,\cdot)$. På denne måde kan man sige, at direkte-produkt-dannelse er en kommutativ komposition for grupper, idet afbildningen $(g,h) \leftrightarrow (h,g)$ ses at give en isomorfi mellem $(G,\cdot) \times (H,\cdot)$ og $(H,\cdot) \times (G,\cdot)$. Ligeledes bliver det en associativ komposition, idet $(G,\cdot) \times (H,\cdot) \times (K,\cdot)$, uanset i hvilken rækkefølge man regner det ud, ses at være mængden af tripler (g,h,k) med komponentvis komposition. Det har således mening at tale om det direkte produkt af et endeligt antal

grupper, og ligeledes at danne potenser af en gruppe, $(G,\cdot)^n$, hvor $n \in \mathbb{N}$.

Eksempler: Det n-dimensionale vektorrum $(\mathbb{R}^n,+)$ med vektoraddition ses at være lig $(\mathbb{R},+)^n$. Gruppen $(\mathbb{Q}\setminus\{0\},\cdot)$ er direkte produkt af grupperne $(\mathbb{Q}_+,\cdot)$ og $(\{1,-1\},\cdot)$, idet vi for $q \in \mathbb{Q}_+$ kan lade $(q,1)$ svare til q og $(q,-1)$ svare til $-q$. Analogt er $(\mathbb{R}\setminus\{0\},\cdot)$ direkte produkt af $(\mathbb{R}_+,\cdot)$ og "gruppen bestående af fortegnene + og -". Den entydige fremstilling af tallene i $\mathbb{Q}_+$ som uforkortelige brøker viser, at $(\mathbb{Q}_+,\cdot)$ er direkte produkt af en uendelig cyklisk gruppe, f.eks. $(\{2^z \mid z \in \mathbb{Z}\},\cdot)$, og en gruppe $(M,\cdot)$ bestående af alle rationale tal, der kan skrives som brøker med ulige tæller og ulige nævner.

Det direkte produkt $(G,\cdot) \times (H,\cdot)$ har en undergruppe isomorf med $(G,\cdot)$, nemlig mængden af par (g,e) hvor e er et element i $(H,\cdot)$, og analogt har det en undergruppe isomorf med $(H,\cdot)$, nemlig mængden af par (e,h), og man ser, at to vilkårlige elementer fra disse undergrupper kommuterer, fordi $(g,e)\cdot(e,h) = (g,h) = (e,h)\cdot(g,e)$. Iøvrigt ser man, at disse undergrupper er normale undergrupper , idet f.eks. $\{(g,e)\}$ netop udgør kernen ved den homomorfe afbildning $(g,h) \to (e,h)$ ved hvilken produktgruppen afbildes på $(H,\cdot)$.

Eksempel: Et egentligt direkte produkt må have mindst to ikke-trivielle normale undergrupper, hvis ordeners produkt er lig gruppens orden, og heraf ses f.eks., at tetraedergrupperne T og T_d (AG II,2) ikke kan skrives som direkte produkt af to grupper (af orden >1)

Omvendt: Hvis $(M,\cdot)$ har undergrupper G og H, og et-

hvert produkt gh kommuterer, altså gh = hg (hvor g ∈ G og h ∈ H), og endvidere den eneste måde på hvilken etelementet e kan skrives på formen gh er som e = ee, så vil mængden af elementer gh udgøre en undergruppe i M, som er direkte produkt af G og H. Thi til (g,h) ∈ G × H lader vi svare gh ∈ M, og denne afbildning af G × H ind i M er homomorf, for til parrene (g_1,h_1) og (g_2,h_2) med produktet (g_1g_2,h_1h_2) vil i M svare elementerne g_1h_1 og g_2h_2 med produktet $g_1h_1g_2h_2 = (g_1g_2)\cdot(h_1h_2)$; entydighedsforudsætningen viser, at afbildningens kerne er (e,e), den består altså kun af ét element, så afbildningen er injektiv, og påstanden er dermed vist. Det er umiddelbart, at dersom under sætningens forudsætninger ethvert element i M er et produkt gh, så er (M,·) selv direkte produkt af sine undergrupper G og H.

Eksempel: Indenfor den multiplikative gruppe af n×n - matricer over $\mathbb{Z}$ med determinant 1 har man, idet n = r+s, en undergruppe bestående af de matricer, som har alle elementer lig 0 udenfor r×r - kvadratet øverst til venstre og s×s - kvadratet nederst til højre. Denne er direkte produkt af en undergruppe G, bestående af matricerne med tal ulig 0 indenfor r×r - kvadratet og 1 i resten af diagonalen og en analog undergruppe H dannet udfra s×s - kvadratet.

Uden at gå nærmere ind på det, bør det nævnes, at man på analog måde kan tale om direkte produkt (sommetider "sum") af ringe, idet man ved (K,+,·) × (M,+,·) forstår mængden af par (k,m) og som kompositioner på parmængden benytter komponentvis addition og komponentvis multiplikation. Eksempler: Ringen af funktioner, som afbilder en mængde med to elementer

ind i en ring $(M,+,\cdot)$, ses at være det direkte produkt $(M,+,\cdot)^2$. Den kinesiske restklassesætning (§3, p. 19): hvis man gennemtænker betydninger af de indgående homomorfe afbildninger, ser man, at sætningen udtrykker, at hvis $(M,+,\cdot)$ er en ring med etelement, og $I_1,\ldots,I_n$ er idealer, hvor $j \neq k \Rightarrow I_j+I_k=M$, så er kvotientringen $(M,+,\cdot)/\cap I_j$ lig det direkte produkt af kvotientringene $(M,+,\cdot)/I_j$; som taleksempel ses, at restklasseringen $\dot{Z}_{30}$ er det direkte produkt af restklasseringene $\dot{Z}_2$, $\dot{Z}_3$ og $\dot{Z}_5$.

Vi skal nu vise den fundamentale basissætning for endelige abelske grupper: Enhver endelig abelsk gruppe er det direkte produkt af cykliske grupper (Frobenius og Stickelberger, 1879). Her er gruppens orden åbenbart produktet af de cykliske gruppers orden, og af beviset vil iøvrigt fremgå, at disse kan vælges som potenser af primtal. En cyklisk gruppe $(\dot{Z}_r,+)$ kan opfattes som forskydningerne af mængden $\dot{Z}$ af heltallige punkter på en linie over i sig selv betragtet modulo et interval af længden r, og basissætningen kan derfor løst udtrykkes: Enhver endelig abelsk gruppe er isomorf med en gruppe af forskydninger af et flerdimensionalt heltalspunktgitter $\dot{Z}^m$ betragtet modulo et m-dimensionalt interval (akseparallelt parallelepipedum) med heltallige kantlængder.

Først vises: En endelig abelsk gruppe er direkte produkt af undergrupper, således at i hver undergruppe er samtlige elementordener potenser af et og samme primtal.

Lad $(G,\cdot)$ være endelig abelsk, af orden $n = p^a \cdot s$, hvor p er et primtal, og p/s. Vi sætter $H = \{w^{p^a} | w \in G\}$ og $K = \{w^s | w \in g\}$. Så er H og K undergrupper i G, fordi de er billederne af $(G,\cdot)$ ved endomorfierne $w \to w^{p^a}$ hhv. $w \to w^s$

(den sidste er en endomorfi, fordi $w^s \cdot w^s = (wv)^s$, og den første analogt). Så er $H \times K = G$, hvilket vi ser, idet vi (ligesom tidligere) betragter den homomorfe afbildning $(x,y) \to z = xy$ af $H \times K$ ind i G (her $x \in H$ og $y \in K$). Afbildningen er surjektiv, thi et vilkårligt $z \in G$ kan skrives på formen $z = z^c z^{1-c}$, og ifølge den kinesiske restklassesætning findes et c, som ved division med p^a og med s giver resterne 0 hhv. 1, så at p^a går op i c, og s går op i 1-c, hvoraf følger , at $z^c \in H$ og $z^{1-c} \in K$, så at z er skrevet på formen xy. Afbildningen er injektiv; for at indse det bemærkes, at $x \in H$ medfører $x^s = (w^{p^a})^s = w^n = e$ (ifølge Lagranges sætn.) så at ordenen af x går op i s, og analogt ses, at $y \in K$ medfører, at ordenen af y går op i p^a, og for et (x,y) liggende i afbildningens kerne, altså med $xy = e$, er derfor ord. x = ord. y^{-1} = en fælles divisor for s og p^a, altså lig 1, så både x og y er e; kernen består altså kun af ét element, og afbildningen er injektiv. Dermed er vist, at $G = H \times K$.

Som lige nævnt vil $y \in K$ medføre, at ord. $y \mid p^a$, og K er derfor en gruppe, hvori alle elementordener er potenser af p. For en given orden $n > 1$ af $(G,\cdot)$ er det virkelig muligt at vælge p^a således, at H bliver en ægte undergruppe af G, thi G indeholder med sikkerhed et element w af en orden større end 1, og hvis denne orden skrives som pm, hvor p er et primtal, så vil w^m være af p'orden, og med dette p (som jo er divisor i n ifølge Lagrange) går det, for vi har jo vist, at $x \in H \Rightarrow$ ord.$x \mid s$, og derfor $w^m \notin H$. Vi kan altså skrive $(G,\cdot)$ som et produkt, hvori der indgår en faktor K

af den ønskede type, og hvori den anden faktor H er af lavere orden end ord.G, dernæst opløse H på samme måde og blive ved indtil $(G,\cdot)$ er helt opløst på den ønskede måde.

Dermed har vi eftervist den påståede første opløsning af en abelsk gruppe. Vi bemærker, at dersom specielt $(G,\cdot)$ var cyklisk af orden $n = p^a \cdot s$, så bliver H cyklisk af s'orden og K cyklisk af p^a'orden, og dermed ser vi, at enhver cyklisk gruppe er direkte produkt af cykliske grupper, hvis ordener er potenser af forskellige primtal (og disse primpotenser er netop de, som forekommer i faktoropløsningen af n = den cykliske gruppes orden). Da vi jo også den modsatte vej kan samle delprodukter, finder vi: <u>En cyklisk gruppe af orden rs, hvor $(r,s) = 1$ er direkte produkt af to cykliske grupper af ordener r og s.</u>

Taleksempel: En cyklisk gruppe af 12'orden er direkte produkt af en cyklisk gruppe af 4'orden og en af 3'orden (smlgn. iøvrigt det foran under omtalen af direkte produkt af ringe anførte om restklasseringe $(\check{Z}_m,+,\cdot)$, der specielt giver det her nævnte om grupper $(\check{Z}_m,+)$).

<u>Vi skal så give anden halvdel af beviset for basissætningen</u>, nemlig vise, at hvis $(G,\cdot)$ er en endelig abelsk gruppe, i hvilken enhver elementorden er potens af et fast primtal p, så er gruppen direkte produkt af cykliske grupper (hvis ordener er potenser af p hvorafmfølger, at ord. G også er en potens af p). Beviset skal føres ved induktion efter gruppens orden, idet påstanden åbenbart er gyldig for en gruppe af 1'orden; vi antager ord.G > 1.

må det være {e}alene). Vi har altså et direkte produkt $K_1 = C \times C_1 \times C_2 \times \ldots \subseteq G$. Hvis $K_1 = G$, er vi færdige. I modsat fald vil $K_1 \subset G$ ligesom før medføre, at $M \not\subset K_1$, og vi kan så tage et $z' \in M \setminus K_1$ og får et direkte produkt $C' \times C \times C_1 \times C_2 \times \ldots \subseteq G$, og hvis det er lig G, er vi færdige. Efter et endeligt antal skridt af denne art får vi den ønskede fremstilling.

Basissætningen er dermed bevist.

I produktfremstillingen af en abelsk gruppe er de cykliske gruppers ordener ikke entydigt bestemt; vi havde jo foran sætningen om, at en gruppe af orden rs med (r,s) = 1 er produkt af grupper af ordener r og s, men der er ikke anden flertydighed end den, som udspringer heraf. Anderledes udtrykt: hvis (G,·) skrives som produkt af cykliske grupper af primtalsorden, så er denne mængde af primtalpotenser entydig bestemt. Disse primpotenser kaldes gruppens <u>invarianter</u> og bestemmer altså dens struktur. Første halvdel af beviset gav jo netop en opspaltning efter de forskellige primtal p, og senere fremgik det, at det samtidig var en opspaltning af gruppens orden n efter p (idet gruppen bestående af de elementer, hvis orden var potenser af p, selv fik en orden, som var en potens af p, -det omvendte er trivielt ifølge Lagranges sætn.), og for et givet p er det klart, at der må være en cyklisk faktor, hvis orden er den maximale elementorden, og ved først at uddrage denne og så gentage ser man entydigheden. Men kombineres forskellige primtal, kan

flertydigheden opstå, hvis f.eks. $(G,\cdot)$ er direkte produkt af tre cykliske af ordener 2, 4 og 9, så er den også produkt af to cykliske af ordener 2 og 36 eller af to af ordener 4 og 18, (men så er der ikke flere muligheder).

Man ser let, at basissætningens bevis (begge halvdele) kunne skærpes til at give: For en endelig abelsk gruppe $(G,\cdot)$ med en undergruppe U er det muligt at skrive G som direkte produkt af cykliske undergrupper C_j af primpotens orden, og således at samtidig U er det direkte produkt af undergrupper i de enkelte C_j. Heraf fås umiddelbart : En endelig abelsk gruppe $(G,\cdot)$ har en undergruppe isomorf med $(U,\cdot)$ hvis, og kun hvis invarianterne for G og U (de sidste om fornødent suppleret med nogle 1-taller) kan parres sammen således, at enhver invariant for G er delelig med den tilsvarende for U. Taleksempel: en gruppe med invarianter 4, 2 og 9 har en undergruppe med invarianter 4 og 3, men ingen med invarianter 4, 4 og 3.

Af det foregående fremgår, at for abelske grupper er de cykliske grupper vigtige byggestene, som ved produktdannelse kan opbygge alle endelige og talrige af de uendelige grupper.

Som standardtype for ikke-abelske kan man benytte grupper af n×n matricer(med forskellige n) og blandt disse endda nøjes med matricer, som er unitære (altså ortogonale dersom reelle). Repræsentationsteorien for grupper omhandler homomorfe (spec. isomorfe) afbildninger af grupper på matrixgrupper.

Lad os her blot bemærke, at enhver endelig gruppe $(G,\cdot)$

kan repræsenteres isomorft ved en matrixgruppe. Thi $(G, \cdot)$ er isomorf med en gruppe af permutationer, og til en permutation $j \to k(j)$, $j = 1,\ldots, n$ lader vi blot svare en matrix, som udtrykker den tilsvarende permutation af koordinatakserne i et n-dimensionalt koordinatsystem, (den er ortogonal), og dens elementer er 1-taller og nuller).

Øvelser til § 6.

1. Illustrer $(\check{Z}_{12},+) = (\check{Z}_3,+) \times (\check{Z}_4,+)$ ved til gitterpunkterne i et 3×4-rektangel at angive de tilsvarende gruppeelementers orden og de tilsvarende abscisser fra et lineært interval af længde 12. Hvor mange isomorfe afbildninger findes der fra interval til rektangel?
2. Hvor mange ikke-isomorfe abelske grupper findes der af orden 2^5 ? Og af orden $2^5 \cdot 7^3$?
3. For hvilke n er alle abelske grupper af n'orden isomorfe? For hvilke n findes netop 2 ikke-isomorfe ? Samme spørgsmål med 3 og 4.
4. Et endeligt legeme $(M,+,\cdot)$ har karakteristik p. Hvad er strukturen af gruppen $(M,+)$? Vis, at $(M,+,\cdot)$ er bestemt entydigt pånær isomorfi for $[M:\check{Z}_p] = 2$ eller 3.
5. En endelig abelsk gruppe har invarianter 2^4, 2, 5^2, 5. Hvor mange ikke-isomorfe undergrupper har den ? Hvor mange ikke-isomorfe undergrupper af 100'orden har den ? Hvor mange, gerne isomorfe, undergrupper af 2'orden har den ?
6. En endelig abelsk gruppe $(G,\cdot)$ har invarianter 2^4, 2, 5^2, 5. Angiv invarianterne for undergruppen $H = \{x^6 \mid x \in G\}$. Angiv alment invarianterne for $H = \{x^t \mid x \in G\}$ udtrykt ved t og invarianterne for G.

Nogle trykfejl i AT-stoffet (Th. Bang):

Side 0,8 nederst og 0,9:	tegnet for normal er $\dashv$		
- 0,8 i noten:	"eller distributiv m.h.t. en anden komposition" udgår.		
- 2,8 linie 2:	for M_+	læs $M_+ \cup \{0\}$	
- 2,1o - 17:	for L	læs M	
- 2,18 - 4 f.n.:	for $\grave{N}$	læs $\grave{Z}$	
- 3,2o - 8:	for $\notin$	læs $\in$	
- 6,7 - 12:	for $e= x_j^{s_1}..$	læs $e= x_1^{s_1}$	
- 6,7 nederst:	for H	læs K (3 steder)	
- 6,8 linie 15:	for primtalsorden læs primpotensorden.		
- 6,8 - 2:	for $K_1= C \times C_1 \times ..$	læs $K_1= C \times K$	
- 6,8 - 5:	for $C' \times C \times C_1 \times C_2..$	læs $C' \times K_1$	
- 6,9 - 5:	for let	læs ret let (d.v.s. teksten giver ikke bevis for sætningen).	