Københavns Universitets Matematiske Institut

M A T E M A T I K 2

1962-63

Th. Bang

Forelæsninger

over

A L G E B R A OG T A L T E O R I.

§ 1. Ringe. Idealer. Legemer.

I AG II er nogle af algebraens grundbegreber beskrevet; vi skal af hensyn til det følgende resumere noget derfra, idet vi iøvrigt henviser til det nævnte kapitel.

Ved en komposition indenfor en mængde M forstås en afbildning af M × M ind i M, almindeligt betegnet ved en skrivemåde som x $ y = z.

I de følgende udsagn står a, b og c for vilkårlige elementer fra M.

Kompositionen er associativ, såfremt a $ (b $ c) = (a $ b) $ c.

Kompositionen er kommutativ, såfremt a $ b = b $ a.

Et neutralt element e opfylder e $ a = a $ e = a, (og det vistes, at der findes højst eet sådant).

Hvis e er neutralt element kaldes a regulær, såfremt der findes et element, betegnet a^{-1}, så a $ a^{-1} = a^{-1} $ a = e og a^{-1} kaldes inverst til a, (og det vistes, at ved en associativ komposition har et regulært element kun eet inverst).

Forkortningsreglen kunne udtrykkes: hver af ligningerne a $ x = b og x $ a = b har højst een løsning (og det vistes, at såfremt kompositionen er associativ og ethvert element er regulært, så gælder forkortningsreglen).

Det vigtigste tilfælde af en mængde med een komposition blev behandlet i AG II, 2, nemlig begrebet en gruppe. Derved fp forstås en mængde med en komposition, som er associativ, hvor der findes neutralt element, og hvor alle elementer er regulære. Forkortningsreglen gælder altså, og endda i den stærkere forstand, at enhver af de nævnte ligninger har netop een løsning x. Såfremt kompositionen er kommutativ, kaldes gruppen kommuta-

tiv. Vi skal nu betragte mængder M med to kompositioner, og skal minde om definitionen på, at Ь er distributiv med hensyn til $, hvilket betyder, at

$$x \text{ Ь } (y \$ z) = (x \text{ Ь } y) \$ (x \text{ Ь } z)$$

$$(y \$ z) \text{ Ь } x = (y \text{ Ь } x) \$ (z \text{ Ь } x)$$

gælder for alle $x,y,z \in M$.

En ved to kompositionsforskrifter organiseret mængde M kaldes en ring, såfremt M ved den første komposition ("ringadditionen") udgør en kommutativ gruppe, og endvidere den anden komposition ("ringmultiplikationen") er associativ og distributiv med hensyn til den første.

Til den anden komposition kan man eventuelt forstærke kravene: såfremt den anden komposition er kommutativ, vil vi tale om en kommutativ ring, såfremt den anden komposition har et neutralt element ("et-element ved ringmultiplikationen") taler vi om ring med et-element, og dersom vi siger, at et element i ringen har et inverst skal det også referere til den anden komposition.

Som antydet vil vi sædvanligvis betegne den første komposition som addition og benytte tegnet +, og for a+a+a+a vil vi skrive 4a, o.s.v; den anden komposition betegner vi som multiplikation og benytter tegnet · (der evt. kan udelades), og a·a·a·a vil vi skrive som a^4, o.s.v. Dette vil kun sjældent komme til at kollidere med betegnelserne fra sædvanlig talregning, men i de tilfælde, hvor det kan give anledning til misforståelser, må vi naturligvis benytte andre betegnelser (smlgn. eks. 2 nedenfor).

Additionens neutrale element vil vi betegne som nul-element, og ofte skrive 0. Da $0 = 0+0$ finder vi med benyttelse af den distributive lov, at $0\cdot a = (0+0)\cdot a = 0\cdot a + 0\cdot a$, hvoraf ses,

at $0 \cdot a = 0$ for alle $a \in M$, og analogt ses, at $a \cdot 0 = 0$.

Løsningen x til ligningen $a + x = b$ betegnes $b - a$, idet vi dog for $0 - a$ nøjes med at skrive $-a$. Det herved indførte minustegn opfylder de sædvanlige regler. Således er $b + (-a) = b - a$, hvilket ses af ligningen $b = b + 0 = b + ((-a) + a) = (b + (-a)) + a$; endvidere er $(-a) + (-b) = -(a + b)$, hvilket ses af ligningen $((-a) + (-b)) + (a + b) = (-a) + (-b) + a + b = (-a) + a + (-b) + b = 0 + 0 = 0$; endelig er $a(b - c) = ab - ac$, hvilket ses af at $a(b - c) + ac = a((b - c) + c) = ab$.

Det eventuelle inverse element til a betegnes a^{-1}, og ganske som det bevistes for grupper (AG II, 2) ser man, at de sædvanlige potensregler er opfyldt, idet $a^p \cdot a^q = a^{p+q}$ og $(a^p)^q = a^{pq}$ for alle $p,q \in \check{Z}$. Eventuelle løsninger x til ligningerne $ax = b$ og $xa = b$ behøver ikke at være ens, men såfremt vi har at gøre med en kommutativ ring bliver de ens, og vi kan da benytte brøkskrivemåden $x = \frac{b}{a}$; for denne brøkstreg gælder lignende bemærkninger som for minustegnet ovenfor.

Ligeledes vil vi benytte den sædvanlige talaritmetiks konventioner om udeladelse af parenteser, således, at hvor ikke andet er angivet ved parenteser skal man i sammensatte udtryk først foretage potensopløftninger, så multiplikationer (og divisioner) og sluttelig additioner (og subtraktioner).

Da $0 \cdot a = a \cdot 0 = 0$ for ethvert $a \in M$, ser man, at forkortningsreglen ikke kan gælde generelt for ringmultiplikationen, idet man ikke kan "forkorte med 0". Men forudsættes det, at $xz = yz$ for $z \neq 0$ medfører $x = y$, så gælder <u>nulreglen</u>

$$\forall_M x,y((xy = 0) \Rightarrow (x = 0) \vee (y = 0))$$

(i ord: et produkt er kun 0, hvis en af faktorerne er 0); beviset er umiddelbart, thi enten er $y = 0$, eller også får man ved at sammenligne formlerne $0 \cdot y = 0$ og $xy = 0$, hvori $y \neq 0$, at

$x = 0$. (Smlgn. AG II, 1 øv. 3). Hvis omvendt nulreglen gælder, så vil $(xz = yz) \wedge (z \neq 0)$ medføre $xz - yz = (x - y)z = 0$, og dermed $x = y$. Med andre ord: nulreglen er ensbetydende med, at en ligning $xa = b$, hvori $a \neq 0$, højst har en løsning. Analogt ser man, at nulreglen er ensbetydende med, at en ligning $ax = b$, hvori $a \neq 0$, højst har een løsning.

Eksempler på ringe $(M,+,\cdot)$:

1) $(\acute{R},+,\cdot)$, $(\acute{C},+,\cdot)$ og $(\acute{Z},+,\cdot)$. I den sidste af dem har kun tallene +1 og -1 inverse elementer.

2) Lad M være $\acute{R}_+$; ringadditionen defineres som multiplikation af elementerne, og ringproduktet af tallene x og y defineres ved $e^{(\log x)(\log y)}$. I dette eksempel kan man ikke umiddelbart benytte + og · som kompositionstegn. Iøvrigt fremgår eksemplet af den første ring i eksempel 1) ved en isomorfi $x \to e^x$.

3) Lad $(M,+)$ være en vilkårlig kommutativ gruppe; ringmultiplikationen defineres ved at sætte ethvert produkt lig gruppens neutrale element, altså $xy = 0$ for alle $x,y \in M$. Nulreglen svigter til overflod (forudsat M indeholder mere end eet element).

4) M er mængden af funktioner $x = x(t) : A$ ind i $\grave{R}$, $t \in A$, hvor A indeholder mindst to elementer; ringaddition $x + y = x(t)+y(t)$, $t \in A$, og ringmultiplikation $x \cdot y = x(t) \cdot y(t)$, $t \in A$. Nulreglen gælder ikke.

5) M er mængden af $n \times n$-matricer, og kompositionerne er matrixaddition og matrixmultiplikation (AG III, 6). Ringen er i modsætning til de forrige eksempler ikke kommutativ (for $n > 1$).

6) $(\acute{Z}_m,+,\cdot)$; her betyder $\acute{Z}_m$ mængden af hele tal som er multipla af et tal $m \in N$. Ringen har i modsætning til de forrige

eksempler (på nær 4)) ikke noget et-element (forudsat m > 1).

Ved en <u>delring</u> (eller underring) (L,+,·) i en ring (M,+,·) forstås en delmængde L af M, som organiseret ved restriktionen af kompositionsforskrifterne + og · til L udgør en ring. Dette indebærer åbenbart dels, at (L,+) skal være en undergruppe af (M,+), og dels, at restriktionen af kompositionen · til L skal være en komposition indenfor L, d.v.s. at $x,y \in L$ medfører $x \cdot y \in L$. Disse to krav er også tilstrækkelig til at en delmængde L af M er en delring, thi de medfører jo, at restriktionerne af + og · fra M til L bliver kompositioner i L; og når kompositionen + er kommutativ, og kompositionen · er associativ og distributiv med hensynttil +, alt indefor M, så gælder det samme for deres restriktioner til L.

I stedet for at sige at (L,+,·) er delring i ringen (M,+,·), vil vi ofte blot sige, at L er delring i ringen (M,+,·), idet det er underforstået, at kompositionerne er restriktionerne af kompositionerne i M. Analogt vil vi istedet for at sige, at (H,$) er undergruppe i (G,$) blot sige, at H er undergruppe i (G,$).

<u>Hvis L er fællesmængden for (endelig eller uendelig mange) delringe L_j i en ring (M,+,·), så vil L selv også være delring i (M,+,·)</u>.

Bevis: Lad os vise, at $x,y \in L$ medfører $x \cdot y \in L$, idet vi benytter, at den tilsvarende egenskab er opfyldt for alle L_j; det sker således

$$x,y \in L \iff \forall_j(x,y \in L_j) \Rightarrow \forall_j(x \cdot y \in L_j) \iff x \cdot y \in (\cap_j L_j).$$

På ganske analog måde kan vi vise, at $x,y \in L$ medfører $x+y \in L$, og at $x \in L$ medfører $-x \in L$ ved at benytte, at de tilsvarende egenskaber er opfyldt for alle L_j. Dette viser, at restriktionen af kompositionerne ·, + og - til L bliver kompositioner

indenfor L. Og det er klart, at egenskaberne kommutativ, associativ og distributiv bevares ved restriktion, hvormed sætningens bevis er fuldført. Lad os iøvrigt bemærke, at beviset samtidig indeholder et bevis for en analog sætning om undergrupper (se AG II, 2, 3):

Hvis H er fællesmængden for (endelig eller uendelig mange) undergrupper H_j i en gruppe (G,$), så er H selv en undergruppe i (G,$).

Eksempler: Enhver ring har sig selv samt {0} som delringe. Til eksempel 1) foran: (Ċ,+,·) har som delring Ŕ, og denne har igen delringen Ź. Til eksempel 6) foran: ($\acute{Z}_m$,+,·) er delring i i ($\acute{Z}_n$,+,·) da, og kun da når m er et multiplum af n; (Ź,+,·) har som delringe $\acute{Z}_2$ og $\acute{Z}_3$, hvis fællesmængde er delringen $\acute{Z}_6$; fællesmængden for alle $\acute{Z}_m$, $m \in \acute{N}$ er delringen {0}.

Lad os betragte en homomorf afbildning af en ring (M,+,·). Mængden M afbildes ved homomorfien oven på en mængde M', og indenfor M' har vi to kompositioner $\oplus$ og $\odot$, således at (M,+,·) afbildes på (M',$\oplus$,$\odot$). Det er tidligere bevist (AG II,2,9), at når (M,+) er en gruppe, så vil (M',$\oplus$) også være en gruppe, således at neutralt element afbildes i neutralt element og inverse elementer afbildes i inverse elementer, og endvidere er det vist (AG I,1,8 ff), at egenskaberne kommutativ, associativ og distributiv ved homomorfien overføres fra kompositionsforskrifterne + og · til $\oplus$ og $\odot$. Vi har derfor:

Lad (M,+,·) være en ring og (M',$\oplus$,$\odot$) en ved to kompositionsforskrifter $\oplus$ og $\odot$ organiseret mængde. Hvis der findes en homomorf afbildning f af (M,+,·) på (M',$\oplus$,$\odot$), så er (M',$\oplus$,$\odot$) ligeledes en ring. Dennes nulelement er billedet ved f af nulelementet i M; hvis M har et etelement e, så vil M' også have et

etelement, nemlig f(e); hvis $x \in M$ har et inverst x^{-1} ved kompositionen $\cdot$, så vil $f(x) \in M'$ også have et inverst ved kompositionen $\odot$, nemlig $f(x^{-1})$. Hvis ringen $(M,+,\cdot)$ er kommutativ, så er ringen $(M,\oplus,\odot)$ også kommutativ.

Eksempler: Lad $(M,+,\cdot)$ være ringen fra eksempel 4) for en bestående af funktioner $x(t)$, $t \in A$; for et fast $t_0 \in A$ vil $x(t) \to x(t_0)$ være en homomorf afbildning af $(M,+,\cdot)$ over på $(\dot{R},+,\cdot)$; vi bemærker, at nulreglen gælder for $(\dot{R},+,\cdot)$, medens den jo ikke gælder for $(M,+,\cdot)$. At det omvendte kan ske, at nulreglen gælder for en ring, men ikke for dens billede ved en homomorfi, kan ses af følgende eksempel: ringen $(\acute{Z},+,\cdot)$ vil ved afbildningen $p \to p+\acute{Z}_m$ blive afbildet homomorft over på en ring af restklasser modulo m (se AG II,2,side 14 og AG II,2 øvelse 16; vi skal iøvrigt senere udførligt behandle dette eksempel), og for denne ring gælder nulreglen kun, hvis m er et primtal.

Lad $(M,\$)$ være en mængde med en kompositionsforskrift, og lad f være en homomorfi, der afbilder den ind på $(M',\$')$. For elementerne i M definerer vi en relation $\equiv$, idet vi sætter $x \equiv y$ når $f(x) = f(y)$. Det er klart, at relationen bliver en ækvivalensrelation indenfor M, idet den er refleksiv, symmetrisk og transitiv, og ækvivalensklasserne er $f^{-1}(x')$, $x' \in M'$. Men det vil endda være en ækvivalensrelation harmonerende med kompositionen $\$$, hvormed vi mener, at $x \equiv x_1$ og $y \equiv y_1$ medfører $x \$ y \equiv x_1 \$ y_1$; dette ses let, thi ifølge definitionen af $\equiv$ er $f(x) = f(x_1)$ og $f(y) = f(y_1)$, og ved at benytte homomorfien får vi så $f(x \$ y) = f(x) \$' f(y) = f(x_1) \$' f(y_1) = f(x_1 \$ y_1)$, altså $x \$ y \equiv x_1 \$ y_1$. Hvis der i M findes flere kompositionsforskrifter, så vil en homomorf afbildning give anledning til en ækvivalensrelation i M harmonerende med alle kompositionsforskrifterne. Specielt får vi, at en homomorf afbildning f af en ring $(M,+,\cdot)$

giver anledning til en ækvivalensrelation harmonerende med kompositionerne + og ·, idet vi sætter x og y ækvivalente, når f(x) = f(y). En ækvivalensrelation for elementerne i en ring harmonerende med ringkompositionerne kaldes ofte en "kongruensrelation".

Lad der omvendt være givet en mængde med en eller flere kompositionsforskrifter (M,$,Ь,..), og i mængden en ækvivalensrelation ≡ harmonerende med kompositionerne. Da eksisterer der en homomorf afbildning f af (M,$,Ь,..), således at x ≡ y netop når f(x) = f(y). Bevis: Da ≡ er en ækvivalensrelation giver den anledning til en klassedeling af mængden M (se AG I,7,13), således at ethvert x tilhører netop en klasse som kaldes f(x) eller x'. Dermed har vi en afbildning af M ind på et M', nemlig på mængden af klasser. Ethvert x' kan angives ved hjælp af et vilkårligt af de elementer x den indeholder, og vi siger, at x er repræsentant for klassen x'. I M' definerer vi nu kompositionen x' $ y' på følgende måde: vi tager repræsentanter x og y for hhv. x' og y', danner x $ y, og den klasse ∈ M', der indeholder dette element altså (x $ y)', tages som x' $' y'; dette er virkeligt brugbart som definition, thi selvom vi tog andre repræsentanter $x_1 \in x'$ og $y_1 \in y'$, så blev $x_1 \equiv x$ og $y_1 \equiv y$ og derfor x_1 $ $y_1 \equiv x \$ y$ (da ækvivalensrelationen er harmonerende med $), således at vi føres til den samme klasse ∈ M'. Og da (se fem linier ovenfor) x' $' y' = (x $ y)', er afbildningen af (M,$) på (M',$') en homomorfi. På tilsvarende måde kunne vi i M' definere en komposition Ь', og også med hensyn til denne komposition vil afbildningen af M på M' være en homomorfi; o.s.v. Men dermed har vi opnået en homomorfi af den organiserede mængde (M,$,Ь,..) ind på (M',$',Ь',..).

Hvis vi betragter en vilkårlig homomorfi $x \to g(x) = x''$,

der afbilder (M,$,Ł,..) (det samme som ovenfor) ind på (M'',$'',Ł'',..), og således, at $x \equiv x_1$ medfører $g(x) = g(x_1)$, så vil vi vise, at der findes en homomorf afbildning h af M' ind på M'', således at $g = h \circ f$. Vi definerer $h(x')$ som $g \circ f^{-1}(x') = g(x)$, hvor x er et element $\in$ M, for hvilket $f(x) = x'$; det er ligegyldigt, hvilket x inden for $f^{-1}(x')$ vi vælger, thi vælger vi et andet, x_1, så er jo $x \equiv x_1$, og derfor $g(x) = g(x_1)$, så vi får samme billede $h(x')$. Og h er en homomorfi, thi betragter vi f.eks. kompositionen $', så får vi ved at benytte, at f og g er homomorfier, at

$$h(x'\$'y') = g \circ f^{-1}(x'\$'y') = g(x\$y) = g(x)\$''g(y) = h(x')\$''h(y').$$

Dersom specielt g er således, at $g(x) = g(x_1)$ netop når $x \equiv x_1$, d.v.s. når $f(x) = f(x_1)$, kan vi også lade f og g bytte roller i det ovenstående bevis, så at h^{-1} bliver en homomorf afbildning af M'' ind på M', og M' og M'' er altså i dette tilfælde isomorfe.

Alt i alt: Enhver homomorf afbildning f af en mængde med kompositionsforskrifter giver anledning til en ækvivalensrelation $\equiv$ harmonerende med kompostitionerne, således at $x \equiv y$ netop når $f(x) = f(y)$. Omvendt vil der til enhver ækvivalensrelation $\equiv$ i mængden harmonerende med kompositionerne svare en homomorf afbildning f (hvor dens billedmængde med kompositioner er bestemt entydigt pånær isomorfi), således at $f(x) = f(y)$ netop når $x \equiv y$.

Lad nu f være en homomorf afbildning af en ring $(M,+,\cdot)$, og $\equiv$ den dertil svarende ækvivalensrelation i M. Ved homomorfiens kerne I forstår vi mængden af de med 0 ækvivalante elementer i M. Da $\equiv$ er harmonerende med ringaddition (og -subtraktion), og da $y \equiv y$, fås at $x \equiv y$ netop når $x - y \equiv 0$, altså netop når $x - y \in$ I. Kernen bestemmer derfor ækvivalensrelationen entydigt,

og billedet $(M',\oplus,\odot)$ af $(M,+,\cdot)$ er derfor pånær isomorfi bestemt entydigt ved I. Den ved $(M,+,\cdot)$ og kernen I pånær isomorfi entydigt bestemte billedring $(M',\oplus,\odot)$ kaldes <u>faktorringen $(M,+,\cdot)/I$</u> (eller kortere M/I). Betegnelsen er suggestivt heldig: hvis I er "stor", får mange elementer det samme billede ved homorfien, så M' bliver "lille". Hvis M er endelig, bliver I og M' endelige, og for elementantallene får man formlen $m' = \frac{m}{i}$. Bevis: for fast y_0 er $x \equiv y_0$ ensbetydende med $x - y_0 \equiv 0$, som er opfyldt af i forskellige elementer $(x - y_0)$; den tilfældige ækvivalensklasse $(y_0)'$ indeholder altså også i elementer, og antallet af forskellige ækvivalensklasser bliver derfor $\frac{m}{i}$.

En delmængde I af en ring $(M,+,\cdot)$ kaldes et ideal i ringen, hvis der findes en homomorf afbildning af ringen, ved hvilken I er kerne.

Dersom vi inden for en ring har givet nogle (endelig eller uendelig mange) ækvivalensrelationer, harmonerende med ringkompositionerne, så kan vi definere en ny relation $\equiv$, idet vi sætter $x \equiv y$, hvis og kun hvis x og y er ækvivalente ved samtlige de givne ækvivalensrelationer. Så bliver $x \equiv y$ åbenbart også en ækvivalensrelation harmonerende med kompositionerne, og det tilsvarende ideal ses at blive netop fællesmængden for de til de givne ækvivalensrelationer svarende idealer. Vi har derfor: <u>Fællesmængden for (endelig eller uendelig mange) idealer i en ring er et ideal i ringen</u>.

Eksempler på ringe $(M,+,\cdot)$ med homomorfier f og tilsvarende ækvivalensrelationer:

1) Lad f være en isomorfi i en vilkårlig ring; enhver ækvivalensklasse består af et element, og kernen er nulelementet, hvoraf vi ser, at <u>$\{0\}$ er et ("trivielt") ideal</u> i ringen.

2) Enhver ring kan ved en homomorfi afbildes over i ringen bestående af et eneste element (dette er samtidig nulelement og etelement i billedringen); hele ringen udgør altså en ækvivalensklasse, som er afbildningens kerne, og M er altså et ("trivielt") ideal i $(M,+,\cdot)$.

3) Lad $(M,+,\cdot)$ være ringen fra eksempel 4) (side 4) af funktioner $x(t)$, $t \in A$; afbildningen $x(t) \to x(t_o)$ vil (som også omtalt side 7) være en homomorf afbildning af ringen; enhver ækvivalensklasse består af mængden af $x(t)$, hvor $x(t_o)$ har en fast værdi $c \in \dot{R}$; afbildningens kerne er $\{x(t) \mid x(t_o) = 0\}$, og denne mængde er altså et ideal i ringen.

4) De hele tals ring $(\dot{Z},+,\cdot)$ blev ved $p \to p + \dot{Z}_m$ afbildet homomorft over på restklasserne modulo m; kernen er $\dot{Z}_m$, som altså er et ideal.

5) Af de nedenstående egenskaber Id1 og Id2 følger umiddelbart, at ethvert ideal er en delring. Men ikke enhver delring er et ideal; f.eks. er $(\dot{Z},+,\cdot)$ en delring af $(\dot{R},+,\cdot)$, men den er ikke et ideal, thi en homomorfi af $\dot{R}$, hvorved $\dot{Z}$ føres over i nulelementet, vil specielt føre 1 over i nul, og dermed $a = a\cdot 1$ over i nul for ethvert a, så at homomorfiens kerne er hele $\dot{R}$.

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

Id1: I er en undergruppe i ringens additive gruppe $(M,+)$.

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

Ifølge idealets definition skal vi vise, at Id1 og Id2 karakteriserer mængderne $I = \{x \mid x \equiv 0\}$ for samtlige ækvivalensrelationer $\equiv$ harmonerende med + og $\cdot$.

Lad os først vise betingelsernes nødvendighed. Hvis $a \equiv 0$ og $b \equiv 0$ får vi $a + b \equiv 0$, hvilket viser Id1. Hvis $a \equiv 0$ får vi $a \cdot x \equiv 0 \cdot x = 0$ og $x \cdot a \equiv x \cdot 0 = 0$, hvilket viser Id 2.

Dernæst vises betingelsernes tilstrækkelighed. Lad I opfylde Id 1 og Id 2. Vi definerer relationen $\equiv$ ved $a \equiv b$, når $a-b \in I$. Relationen er refleksiv, fordi $a-a = 0 \in I$, symmetrisk fordi $a-b \in I$ medfører $b-a \in I$ og transitiv fordi $a-b \in I$ og $b-c \in I$ medfører $a-c \in I$, altsammen på grund af Id 1. Det er altså en ækvivalensrelation. Endvidere vil $a-a_1 \in I$ og $b-b_1 \in I$ medføre $(a+b)-(a_1+b_1) \in I$, så at $a \equiv a_1$ og $b \equiv b_1$ medfører $a+b \equiv a_1+b_1$. Og endelig vil $a-a_1 \in I$ og $b-b_1 \in I$ medføre $a(b-b_1)+(a-a_1)b_1 = ab-a_1b_1 \in I$, idet både Id 1 og Id 2 er benyttet, så at $a \equiv a_1$ og $b \equiv b_1$ medfører $a \cdot b \equiv a_1 \cdot b_1$. Dermed er tilstrækkeligheden bevist.

For kommutative ringe behøver man kun at stille et af de to i Id 2 anførte krav, idet det andet så af sig selv er opfyldt, hvorimod man for ikke-kommutative ringe må stille begge krav. For de sidstnævnte ringe kan man foruden de ovenfor definerede idealer ("tosidede") betragte "højreidealer", hvormed menes mængder der kun opfylder Id 1 og den første af betingelserne i Id 2, så altså $a \in I$ og $x \in M$ medfører $a \cdot x \in I$; analogt kan man definere "venstreidealer" ved kun at forlange det sidste af kravene i Id 2. Men da vi i det følgende næsten udelukkende skal betragte kommutative ringe, skal vi ikke behandle disse "ensidede" idealer udførligere.

Hvis vi for grupper anvender den almindelige homomorfisætning (side 9), får vi resultater, der på betydningsfuld måde kompletterer tidligere resultater om homomorf afbildning af en gruppe (AG II,2,9): En homomorf afbildning f af en gruppe (G,$) giver anledning til en ækvivalensrelation $\equiv$ i G harmonerende med $, således at $x \equiv y$ netop når $f(x) = f(y)$, og samtlige ækvivalensrelationer harmonerende med $ kan frembringes på denne måde. Endvidere (smlgn. AG II,2,10): Idet kernen N defineres som mængden af de med elementet ækvivalente elementer, så vil $x \equiv y \iff x\$y^{-1} \in N$, hvoraf ses, at kernen bestemmer ækvivalensrelationen entydigt, og dermed homomorfiens billedgruppe (G',$') entydigt paanær isomorfi. Den ved gruppen (G,$) og kernen N paanær isomorfi entydigt bestemte billedgruppe (G',$') kaldes faktorgruppen G/N (eller udførligere (G,$)/N). Det er tidligere vist, at enhver kerne er normal undergruppe (AG II,2,10), og omvendt kan enhver normal undergruppe N virkelig forekomme som kerne, fordi den giver anledning til en ækvivalensrelation harmonerende med gruppekompositionen (se øvelse 7). Alt i alt: Hvis en gruppe (G,$) afbildes homomorft ind på en mængde med komposition (G',$'), vil (G',$') være en gruppe; homomorfiens kerne $N = f^{-1}(e')$ er en normal undergruppe i (G,$). Omvendt vil der til enhver normal undergruppe N i (G,$) eksistere en homomorfi med N som kerne, og den på nær isomorfi entydigt bestemte billedgruppe ved afbildningen betegnes som faktorgruppen (G,$)/N.

Vi vender tilbage til ringene. Det mindste ideal I, som indeholder et givet element a fra ringen (M,+,·) kaldes det af a frembragte hovedideal. Dersom ringen er kommutativ og har et etelement, hvilket oftest vil indtræffe ved vore anvendelser, bliver det af a frembragte hovedelement $I = \{x \cdot a \mid x \in M\}$, for denne mængde opfylder åbenbart Id 1 og Id 2, og den kan ikke

være mindre, når den skal indeholde a og opfylde Id 2. (Uden de simplificerende forudsætninger om ringen blev hovedidealet $I = \{na+x\cdot a+a\cdot y+\sum z_j\cdot a\cdot w_j \mid x,y,z_j,w_j \in M \wedge n \in \check{Z}\}$ (!)). Eksempel: Indenfor $(\check{Z},+,\cdot)$ er det af m frembragte hovedideal netop $\check{Z}_m$. Og et eksempel på et ideal, som ikke er et hovedideal: Lad $(M,+,\cdot)$ være den i eks. 4) betragtede ring af funktioner $x(t)$, $t \in A$; lad I være mængden af funktioner $x(t)$, som hver for sig kun er forskellig fra 0 for endelig mange t; I opfylder åbenbart Id 1 og Id 2, men dersom A er en uendelig mængde, kan I ikke frembringes som mængden af multipla af et $a(t) \in I$.

En ring $(M,+,\cdot)$, hvori $(M \setminus \{0\},\cdot)$ er en gruppe, kaldes et legeme. Af definitionen ser man, at man også kan karakterisere et legeme som en ring, hvori nulreglen gælder og med et-element og således at ethvert element $\neq 0$ har et inverst (thi nulreglen udsiger jo netop at $\cdot$ er en komposition indenfor $M \setminus \{0\}$). Endvidere ser man af det tidligere (side 3-4) om nulreglen anførte, at man også som karakterisering kan benytte, at et legeme er en ring, hvori enhver divisionsligning $a\cdot x = b$ og $x\cdot a = b$ (hvor $a \neq 0$) har netop een løsning, nemlig henholdsvis $x = a^{-1}b$ og $x = ba^{-1}$.

Ved et dellegeme L i et legeme $(M,+,\cdot)$ forstås en delmængde L af M, som organiseret ved restriktionen af kompositionsforskrifterne + og $\cdot$ til L udgør et legeme. Dette giver åbenbart som nødvendige og tilstrækkelige betingelser for at L er et dellegeme af $(M,+,\cdot)$, at $(L,+)$ skal være en undergruppe af $(M,+)$ og $(L \setminus \{0\},\cdot)$ skal være en undergruppe af $(M / \{0\},\cdot)$. Med et bevis af ganske samme art som tidligere for ringe (side 5) får vi: Hvis L er fællesmængden for (endelig eller uendelig

mænge) dellegemer L_j i et legeme $(M,+,\cdot)$, så er L også selv dellegeme i $(M,+,\cdot)$.

Eksempler på legemer: $(\acute{C},+,\cdot)$, $(\acute{R},+,\cdot)$ og $(L_1,+,\cdot)$ hvor $L_1 = \{q_1+iq_2 \mid q_1,q_2 \in \acute{Q}\}$; her er $\acute{R}$ og L_1 dellegemer i $(\acute{C},+,\cdot)$; endvidere er $\acute{R} \cap L_1 = \acute{Q}$, som er dellegeme i alle de tre andre. Lad P_o og P_1 være to punkter på en ret linie, og lad M være mængden af tal $r \in \acute{R}$, med den egenskab at $r \cdot \vec{P_oP_1} = \vec{P_oP_r}$ hvor P_r kan konstrueres med passer og lineal ud fra P_o og P_1; da er $(M,+,\cdot)$ et legeme -- dellegeme af $(\acute{R},+,\cdot)$ - fordi man kan konstruere sum og differens af liniestykker og endvidere produkt og kvotient (fjerdeproportionalkonstruktion). Der eksisterer også endelige legemer, f.eks. det ("uegentlige") legeme, der kun består af eet element, og endvidere et legeme med to elementer, idet ringen af restklasser af hele tal modulo 2 let ses at være et legeme; vi skal iøvrigt senere udtrykkelig gøre rede for, for hvilke m ringen af restklasser modulo m er et legeme.

Da et legeme er en ring, kan man spørge om idealer i et legeme, men svaret bliver, at der findes kun de to trivielle, M og $\{0\}$. Thi dersom idealet blot indeholder et element $a \neq 0$, så indeholder det (ifølge Id 2) ethvert $b = a \cdot x$, d.v.s. alle legemets elementer. Heraf ser vi, at ved en homomorfi vil enten legemet blive overført i legemet bestående af kun et element, nemlig når homomorfiens kerne er M, eller også vil homomorfien være en isomorfi, nemlig når dens kerne er $\{0\}$.

Når homomorfier er isomorfier, kunne man tro, at de ikke frembyder større interesse, men lad os på dette sted blot bemærke, at allerede isomorfier af et legeme på sig selv (og iøvrigt også af en ring på sig selv), altså automorfier, giver bemærkelsesværdige fænomener. Således har legemet $(\acute{Q},+,\cdot)$ ikke andre automorfier end identiteten, thi det er tidligere vist

(løsning til øv. 8, AG II,1) at en homomorfi af blot $(\acute{Q},+)$ ind i $(\acute{Q},+)$ har formen $x \to cx$, og da desuden etelement skal gå over i etelement, skal c være 1. Endvidere har legemet $(\acute{R},+,\cdot)$ ikke andre automorfier end identiteten; for en ordenstro automorfi følger det umiddelbart af det tidligere viste (stadig løsning til øv. 8, AG II,1), idet en ordenstro homomorfi af blot $(\acute{R},+,<)$ ind i $(\acute{R},+,<)$ har formen $x \to cx$, og her må atter c være 1; og en automorfi f af $(\acute{R},+,\cdot)$ må nødvendigvis være ordenstro, da $a = b^2$ medfører $f(a) = f(b)^2$, så at et tal ≥ 0 afbildes i et tal ≥ 0, og derfor $x \geq y \iff x-y \geq 0$ medfører $f(x-y) \geq 0 \iff f(x) \geq f(y)$. Lad nu M betegne mængden af reelle tal af formen $r + s\sqrt{2}$, hvor $r,s \in \acute{Q}$; af AG II,1,øv.7 fremgår, at denne mængde er et legeme, og at den har en ikke-triviel homomorfi, som endda er en automorfi, nemlig afbildningen $r + s\sqrt{2} \to r - s\sqrt{2}$. Dette indtræffer tiltrods for, at $(M,+,\cdot)$ både har $(\acute{Q},+,\cdot)$ som dellegeme, og selv er dellegeme i $(\acute{R},+,\cdot)$.

Kommutative legemer er langt de vigtigste, og i alt det følgende skal vi kun betragte sådanne. Som eksempel på et ikke-kommutativt legeme kan vi nævne "kvaternionerne" (se øvelse 3).

Lad $(L,+,\cdot)$ være et legeme, som indeholder en delring $(M,+,\cdot)$ med mindst to elementer. Så må $(M,+,\cdot)$ være en kommutativ ring, hvori nulreglen gælder. Der findes et mindste legeme L_o, som er dellegeme i $(L,+,\cdot)$ og således at $M \subseteq L_o$, nemlig L_o = fællesmængden for alle de dellegemer i $(L,+,\cdot)$, der indeholder M, (der eksisterer sådanne dellegemer, f.eks. L selv).

Dette L_o må i hvert fald indeholde $L^* = \{\frac{a}{b} \mid a,b \in M \wedge b \neq 0\}$, men faktisk er $L_o = L^*$, idet L^* i sig selv udgør et dellegeme af L. For at indse dette bemærker vi først,

at $0 \in L^*$, thi $0 = \frac{0}{b}$ for et vilkårligt $b \neq 0$; endvidere, at $x = \frac{a}{b} \in L^*$ medfører $-x \in L^*$, da $-\frac{a}{b} = \frac{-a}{b}$ (begrundelsen for denne omskrivning findes på side 3 ved omtalen af minustegn og brøkstreger, det samme gælder nogle af de følgende småomskrivninger); endvidere, at $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \in L^*$ (her er benyttet, at det er tilladt at multiplicere tæller og nævner i en brøk med det samme element $\neq 0$ (det er tilladt at "forlænge" og "forkorte" brøker), rigtigheden følger af, at $x \cdot b = a \iff x \cdot (bg) = ag$ ifølge nulreglen såfremt $g \neq 0$). Hermed er vist, at $(L^*,+)$ er undergruppe i $(L,+)$. For at godtgøre, at $(L^* \setminus \{0\},\cdot)$ er undergruppe i $(L \setminus \{0\},\cdot)$ skal vi tilsvarende først bemærke, at $1 = \frac{b}{b} \in L^*$, endvidere at $x = \frac{a}{b} \in L^*$ medfører $x^{-1} = \frac{b}{a} \in L^*$, og endelig at $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in L^*$ (her er $a,b,c,d \neq 0$ og ifølge nulreglen derfor også ac og $bd \neq 0$). At endelig L^* indeholder M er klart, da ethvert $a = \frac{ab}{b}$. Forudsætningen om at M indeholder mindst to elementer må med, for ellers fandtes intet $b \in M \wedge b \neq 0$, så konstruktionen af L svigtede. Alt i alt:

Når et kommutativt legeme $(L,+,\cdot)$ har en delring M med mindst to elementer, så eksisterer der et mindste dellegeme L_0 af L, således at $M \subseteq L_0$, og dette består netop af mængden af kvotienter $\frac{a}{b}$, hvor $a,b \in M \wedge b \neq 0$. Det kaldes M's kvotientlegeme.

Da $\frac{a}{b} = \frac{ad}{bd}$ og $\frac{c}{d} = \frac{bc}{bd}$ ses, at de to brøker er ligestore da og kun da, når $ad = bc$, og man ser, at man da kan komme fra den ene til den anden ved først at forlænge, og dernæst forkorte med elementer $\neq 0$ fra ringen. Endvidere ser man af formlerne for sum og produkt af to brøker, at kompositionerne indenfor kvotientlegemet er entydigt bestemt ved kompositionerne indenfor ringen. Derfor: Isomorfe ringe vil have isomorfe kvotientlegemer.

Lad os nu vende situationen om, og antage, at der er givet

vet en ring, og så spørge, om der eksisterer et legeme, i hvilket den er delring. Ifølge det foregående ved vi, at hvis der findes et sådant, så findes der også et kvotientlegeme for ringen, og endvidere, at dette uanset legemet er bestemt entydigt paanær isomorfi. Svaret bliver positivt, idet vi vil vise, at vi til den givne ring kan skabe et kvotientlegeme; ved denne skabelse råder vi selv over benævnelserne, og det er derfor klart, at kvotientlegemet kun bliver bestemt paanær isomorfi.

Lad $(M,+,\cdot)$ være en kommutativ ring med mindst to elementer, og i hvilken nulreglen gælder. Da kan ringen udvides til et kommutativt legeme $(L,+,\cdot)$ som er kvotientlegeme for ringen, og dette er paanær isomorfi bestemt entydigt ved ringen.

Bevis: Vi betragter $M \times (M\setminus\{0\})$, d.v.s. mængden $\{(a,b) \mid a,b \in M \wedge b \neq 0\}$, men i stedet for at skrive (a,b), vil vi skrive parret som en "formel brøk" $\frac{a}{b}$. Indenfor mængden af formelle brøker definerer vi relationen $\equiv$ ved $\frac{a}{b} \equiv \frac{c}{d}$, når $\frac{a}{b}$ ved først at forlænges og dernæst forkortes kan overføres til $\frac{c}{d}$ (forlængelse og forkortning skal ske med elementer fra M forskellige fra nulelementet). Relationen $\equiv$ ses umiddelbart at være reflexiv og symmetrisk, og den er transitiv, da vi i stedet for at forlænge med l_1, forkorte med k_1, forlænge med l_2 og forkorte med k_2 kan forlænge med $l_1 l_2$ og forkorte med $k_1 k_2$. Det er altså en ækvivalensrelation indenfor mængden af formelle brøker. Vi kalder mængden af ækvivalensklasser for L. Enhver ækvivalensklasse kan angives ved en af sine repræsentanter, og lad $\left(\frac{a}{b}\right)'$ betegne den ækvivalensklasse, der indeholder repræsentanten $\frac{a}{b}$.

Vi definerer en komposition + indenfor mængden af ækvivalensklasser ved

$$\left(\frac{a}{b}\right)' + \left(\frac{c}{d}\right)' = \left(\frac{ad+bc}{bd}\right)' ;$$

dette er virkelig brugbart som definition, idet det kun tilsyneladende afhænger af valget af repræsentanterne indenfor klasserne, thi hvis vi f.eks. erstatter $\frac{a}{b}$ med en brøk der fremgår af den ved at forlænge med l og forkorte med k, så bliver den formelle brøk i parentesen på højre side af lighedstegnet også forlænget med l og forkortet med k. Man ser umiddelbart, at kompositionen + er kommutativ. Den er associativ, idet man får

$$\left(\frac{a}{b}\right)' + \left(\frac{c}{d}\right)' + \left(\frac{e}{f}\right)' = \left(\frac{adf + bcf + bde}{bdf}\right)' ,$$

uanset hvorledes man sætter parenteser før udregningen af venstresiden. Der findes et neutralt element ved +, nemlig klassen $\left(\frac{0}{b}\right)'$, og endvidere har enhver klasse $\left(\frac{a}{b}\right)'$ en invers ("modsat") ved +, nemlig $\left(\frac{-a}{b}\right)'$; begge dele ses umiddelbart ved at indsætte i definitionen af klassekompositionen +.

Vi definerer en komposition · indenfor mængden af ækvivalensklasser ved

$$\left(\frac{a}{b}\right)' \cdot \left(\frac{c}{d}\right)' = \left(\frac{ac}{bd}\right)' ;$$

dette er virkeligt brugbart som definition, idet det kun tilsyneladende afhænger af valget af repræsentanterne indenfor klasserne, thi hvis vi forlænger og forkorter i en af de formelle brøker på venstre side, så får vi forlænget og forkortet tilsvarende i den formelle brøk på højre side. Man ser umiddelbart, at kompositionen · er kommutativ (idet ringen M jo var forudsat kommutativ). Ligeledes ser man umiddelbart, at kompositionen er associativ. Endvidere er · distributiv med hensyn til +, thi man finder

$$\left(\frac{a}{b}\right)' \cdot \left[\left(\frac{c}{d}\right)' + \left(\frac{e}{f}\right)'\right] = \left(\frac{acf + ade}{bdf}\right)'$$

og

$$\left(\frac{a}{b}\right)' \cdot \left(\frac{c}{d}\right)' + \left(\frac{a}{b}\right)' \cdot \left(\frac{e}{f}\right)' = \left(\frac{acbf + aebd}{b^2df}\right)'$$

hvor højresiderne åbenbart er den samme ækvivalensklasse, da den sidste repræsentant kan fremgå af den første ved at forlænge og forkorte (f.eks. med henholdsvis b^2 og b). Der findes et etelement ved ·, nemlig klassen $\left(\frac{b}{b}\right)'$, og endvidere har enhver klasse $\left(\frac{a}{b}\right)'$, hvori $a \neq 0$, en invers klasse, nemlig $\left(\frac{b}{a}\right)'$; begge dele ses umiddelbart af definitionen.

Dermed har vi konstrueret et legeme (L,+,·). Det har ikke umiddelbart den givne ring (M,+,·) som delring, men det kan vi opnå, dersom vi identificerer visse af elementerne i L med elementerne i M, og viser, at for denne delmængde bliver restriktionen af legemskompositionerne + og · netop til ringkompositionerne + og ·. Vi identificerer $\left(\frac{ab}{b}\right)' \in L$ med $a \in M$ (det ses, at være ligegyldigt, hvilket element b vi her har benyttet). Ringsummen af elementerne a og c bliver a + c, medens legemssummen af de dermed identificerede bliver $\left(\frac{ab}{b}\right)' + \left(\frac{cb}{b}\right)' = \left(\frac{ab^2+cb^2}{b^2}\right)'$, og man ser, at den netop bliver identificeret med ringsummen a + c. Med multiplikationen går det analogt. Dermed har vi fået gjort legemet til et udvidelseslegeme for ringen. Og det er kvotientlegeme for ringen, thi man ser, at $\left(\frac{a}{b}\right)'$ netop er kvotienten mellem ringelementerne a og b, da $\left(\frac{a}{b}\right)' \cdot b = \left(\frac{a}{b}\right)' \cdot \left(\frac{bc}{c}\right)' = \left(\frac{abc}{bc}\right)' = a$. Dermed er sætningen bevist.

Dersom vi som ring (M,+,·) benytter $(\acute{Z},+,\cdot)$, bliver kvotientlegemet netop $(\acute{Q},+,\cdot)$.

Men det bør bemærkes, at i den foregående systematiske opbygning af matematikken i kursus AG (Mat.1), kapitlerne I og II, og i nærværende paragraf er der ikke på noget sted bygget

på kendskab til legemet af rationale tal $(\acute{Q},+,\cdot)$, og ejheller på kendskab til legemet $(\acute{R},+,\cdot)$ af de reelle tal eller legemet $(\acute{C},+,\cdot)$ af komplekse tal. De er kun på grund af deres tilvante karakter benyttet i (ganske visttalrige) illustrerende eksempler og øvelser. Ringen $(\acute{Z},+,\cdot)$ af hele tal er derimod benyttet fra et tidligt tidspunkt. Den foregående sætning om kvotientlegemets skabelse giver på grundlag af de hele tal en indførelse af de rationale tal, en indførelse, som naturligvis i princippet minder om regneundervisningens indførelse af brøker, men er betydelig kraftigere gennemtænkt.

Vedrørende mængden af reelle tal $\acute{R}$, skal vi bemærke, at de kan fås ud fra systemet af rationale tal ved en videreudbygning, hvorved man søger at nå frem til et system med egenskaber, der er motiveret ved, hvad der kan synes rimeligt for mængden af punkter på en ret linie (se AG III, §3). Vi skal ikke her foretage denne udbygning, men i det følgende antage systemet af reelle tal for bekendt, ligesom det jo også i kursus MA(Mat.1) lige fra første færd har været antaget bekendt. Lad os iøvrigt bemærke, at med begrebet "tallegeme" (i AG III,§2) menes dellegeme af $(\acute{R},+,\cdot)$ (evt. af $(\acute{C},+,\cdot)$.

Lad os endnu bemærke, at hele læren om determinanter og lineære ligningssystemer umiddelbart kan anvendes, når blot de indgående størrelser er elementer i et legeme.

Lad $(M,+,\cdot)$ være en ring, og I et ideal i denne; vi siger, at I er maximalideal i ringen, såfremt det ikke er ægte delideal af noget andet ideal end det trivielle ideal M. Hvis vi har en ring $(M,+,\cdot)$, som er kommutativ og har et etelement, og I er et maximalideal i ringen, da er faktorringen $(M,+,\cdot)/I$ et legeme.

Bevis: Lad f være en homomorfi, som fører $(M,+,\cdot)$ over i $L = (M,+,\cdot)/I$. Ifølge de almindelige resultater om homomorf afbildning (AT 1, 6) vil L også være kommutativ og have et etelement. Lad nu a være et fra nulelementet forskelligt element i L, da vil a frembringe et hovedideal I_a indenfor L, og I_a er kerne for en homomorf afbildning g af L; den sammensatte afbildning $g\circ f$ er en homomorf afbildning af $(M,+,\cdot)$, og dennes kerne er et ideal, som indeholder hele I og desuden indeholder mere, nemlig $f^{-1}(a)$, og ifølge definitionen af maximalideal er det derfor hele M, således at resultatet af $g\circ f$ bliver en (uegentlig) ring, kun bestående af et nulelement. Idealet I_a omfatter derfor hele L, men dermed er jo vist, at ethvert element i L er et multiplum af a, d.v.s. at division med a altid er mulig, og L er derfor et legeme.

Eksempel: Indenfor $(Ź,+,\cdot)$ gælder det for ethvert primtal p, at mængden $Ź_p$ af multipla af p er et maximalideal. Thi det er jo i hvert fald et ideal, og den tilsvarende faktorring $(Ź,+,\cdot)/Ź_p$ (altså restklasseringen modulo p) indeholder p elementer; for et ideal I, hvor $Ź_p \subsetneq I$ vil der ifølge beviset ovenfor findes en homomorf afbildning af $Ź/Ź_p$ på $Ź/I$, og ifølge et tidligere resultat (AT 1, side 10 øverst) må elementantallet for $Ź/I$ så gå op i p, d.v.s. enten være 1, i hvilket tilfælde I er det trivielle ideal Ź, eller være p, i hvilket tilfælde er lig $Ź_p$. Vi ser altså, at $Ź_p$ er et maximalideal, og at for ethvert primtal p findes der et legeme med p elementer, nemlig restklasseringen modulo p.

Lad $(M,+,\cdot)$ være et legeme, og lad etelementet hedde e. Da $(M,+)$ er en kommutativ gruppe, vil der indenfor $(M,+)$ findes en mindste undergruppe, der indeholder e, nemlig fællesmængden for samtlige undergrupper, der indeholder e. Denne undergruppe må i hvert fald for alle $n \in \dot{Z}$ indeholder elementet ne, idet dette for $n > 0$ defineres som e+e+...+e (n addender), og man endvidere definerer (-n)e som -(ne); man ser, at me+ne bliver lig (m+n)e, og undergruppen kan derfor fremgå af $(\acute{Z},+)$ ved en homomorfi.

Der kan nu indtræffe to muligheder: Enten er alle elementerne ne forskellige, således at undergruppen er isomorf med $(\acute{Z},+)$, og da man af definitionen på ne let ser, at $(me)\cdot(ne) = (mn)e$, vil undergruppens elementer endda udgøre en delring af $(M,+,\cdot)$ isomorf med $(\acute{Z},+,\cdot)$. Denne delring har indenfor $(M,+,\cdot)$ et kvotientlegeme som er isomorft med kvotientlegemet for $(\acute{Z},+,\cdot)$, d.v.s. med $(\acute{Q},+,\cdot)$, og dette ses at være primlegeme (d.v.s. det mindste ikke-trivielle dellegeme) for $(M,+,\cdot)$, da et ikke-trivielt dellegeme altid må indeholde etelementet. I dette tilfælde siger man, at $(M,+,\cdot)$ har karakteristik 0, og i så fald er dets primlegeme isomorft med $(\acute{Q},+,\cdot)$.

Eller man har ne = me, hvor n og m er forskellige; så er (n-m)e = 0, og der vil da findes et mindste positivt $p \in \acute{Z}$, så pe = 0, og undergruppen bliver isomorf med den additive restklassegruppe modulo p, og man ser som ovenfor, at dens elementer udgør en delring af $(M,+,\cdot)$ isomorf med restklasseringen modulo p. Da nulreglen gælder i $(M,+,\cdot)$, må p være et primtal, thi hvis p = ab (sædvanlige hele tal) vil $(ae)\cdot(be) = pe = 0$, og det er ovenfor omtalt, at restklasseringen så i sig udgør et legeme. I dette tilfælde siger man, at $(M,+,\cdot)$ har karakteristik p, og denne er et primtal, og legemets primlegeme er isomorft med legemet af restklasser modulo p.

Eksempel: Legemerne $(\acute{Q},+,\cdot)$, $(\acute{R},+,\cdot)$ og $(\acute{C},+,\cdot)$ har alle karakteristik 0.

Nogle trykfejl i AT § 1:

Side	5	Linie	1 f.o.	4)	læs	3)
-	6	-	8 f.n.	AG I	-	AG II
-	7	-	4 f.o.	(M,	-	(M',
-	8	-	14 f.n.	$	-	$'
-	12	-	9 f.o.	elementet	-	etelementet
-	12	-	2 f.n.	hovedelement	-	hovedideal
-	16	-	14 f.n.	L	-	L^*
øvelse	3			K betegner matricen		
øvelse	17			$\cup$	læs	$\cap$

Øvelser til § 1.

1) 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 $y \in M$.

2) Lad $(M,+,\cdot)$ være en vilkårlig ring. På $(\acute{Z} \times M)$ 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 $(\acute{Z} \times M, \oplus, \odot)$ er en ring med etelement, og at den har en med $(M,+,\cdot)$ isomorf delring.

3) Vis, at matricerne (med komplekse elementer)

$$\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix} \qquad a,b,c,d \in \acute{R}$$

med matrix addition og matrixmultiplikation udgør en ikke-kommutativ ring med etelement, og i hvilken ethvert elementforskelligt fra nulelementet har et inverst.
Bestem ringens centrum (definitionen af centrum nævnt i øv. 1). Idet K kan angives ved talsættet $(a,b,c,d) \in \acute{R}^4$, viser opgaven, at $\acute{R}^4$ på en ikke-triviel måde kan organiseres som ring ("kvaternionringen").

4) 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 har et med hensyn til \$ inverst element; et nilpotent element $a \in M$ er et element, til hvilket der findes et n så (med ringkompositionerne) $a^n = 0$.

5) 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 i 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 ind i 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: $(x,y) \to (x,y)$,

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

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

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

(tidligere undersøgt i AGI,6,øv.4); find antallet elementer i endomorfiringen for $(G,\$)$, og vis, at ringen ikke er kommutativ og at nulreglen ikke gælder.

6) Vis, at mængden af $n \times n$-matricer $\underline{\underline{A}}$, der har 0 under diagonalen, med matrixaddition og matrixmultiplikation som kompositioner udgør en ring $(M,+,\cdot)$.
Angiv samtlige nilpotente elementer i M(definitionen af nilpotent nævnt i øv.4). Gælder nulreglen i $(M,+,\cdot)$? Undersøg om afbildningerne $\underline{\underline{A}} \to \det\underline{\underline{A}}$ og $\underline{\underline{A}} \to \mathrm{tr}\underline{\underline{A}}$ er homomorfe afbildninger af $(M,+,\cdot)$ ind i $(\dot{R},+,\cdot)$. Angiv to forskellige homomorfier af $(M,+,\cdot)$ ind i $(\dot{R},+,\cdot)$.

7) Lad N være en normal undergruppe i gruppen $(G,\$)$. Vi definerer relationen $\equiv$ i G ved: $x \equiv y \iff x\$y^{-1} \in N$. Vis, at relationen $\equiv$ er en ækvivalensrelation harmonerende med $\$$.

8) Lad $(M,+,\cdot)$ være en (ikke-kommutativ) ring. Vis, at fællesmængden for (endelig eller uendelig mange) idealer i ringen atter er et ideal. Vis herved, 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/I bliver kommutativ.

9) Lad $(M,+,\cdot)$ være en kommutativ ring. Vis, at mængden af de nilpotente elementer udgør et ideal I (nilpotent defineret i øvelse 4). Vis, at faktorringen M/I ikke har andre nilpotente elementer end nulelementet.

10) Der betragtes ringen af de kontinuerte funktioner x(t), der afbilder $0 \leqq t \leqq 1$ ind i $\mathbb{R}$, idet ringsum og ringprodukt er definerede ved henholdsvis $x(t) + y(t)$ og $x(t)\cdot y(t)$. Vis, at følgende tre mængder er idealer, og undersøg hvilke af dem, der er hovedidealer:

$$I_1 = \{x(t) \mid x(t) = 0 \text{ for alle } t \text{ i en omegn af } t = 0\},$$
$$I_2 = \{x(t) \mid x(0) = 0\},$$
$$I_3 = \{x(t) \mid x(0) = 0 \wedge x(t) \text{ differentiabel i } t = 0\}.$$

11) Lad $(M,+,\cdot)$ være den i øvelse 10 betragtede ring, og $I = I_{t_0} = \{x(t) \mid x(t_0) = 0\}$.

I er et ideal; vis, at det er et maximalt ideal, hvormed menes, at M er det eneste ideal i hvilket I er en ægte delmængde.

Vis omvendt, at hvert maximalt ideal er af den nævnte form, idet ethvert ægte delideal af M er indeholdt i et I_{t_0} (til hjælp: vis ved hjælp af Borel's overdækningssætning, at hvis et ideal for ethvert t_0 indeholder et x(t) så $x(t_0) \neq 0$, så indeholder det et x(t) som er $\neq 0$ for alle t, $0 \leqq t \leqq 1$, hvoraf følger, at det indeholder hele M).

12) Lad $(M,+,\cdot)$ være ringen af vilkårlig ofte differentiable funktioner $x(t)$, som afbilder $0 \leqq t \leqq 1$ ind i $\mathbb{R}$; sædvanlig addition og multiplikation. Lad $I = \{x(t) \mid x(0) = 0\}$. Vis, at I er et ideal, og undersøg, om det er et hovedideal.
Idet "vilkårlig ofte differentiable" erstattes med "en gang differentiable" stilles de samme spørgsmål (det kan ved dette spørgsmål være fordelagtigt at bemærke, at hvis $k(t)$ betegner funktionen $t \sin \cdot \frac{1}{t}$ suppleret med værdien 0 for $t = 0$ (det kendte eksempel på en kontinuert, men ikke differentiabel funktion), så vil $a(t) \in I \Rightarrow a(t) \cdot k(t) \in I$.
Bemærk, at hvis der erstattes med "kontinuerte", er de samme spørgsmål stillet i øvelse 10, I_2.

13) $(M,+,\cdot)$ er ringen af $n \times n$-matricer 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.

14) 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 $I \subseteq M_1 \subseteq M$ og delringene af M/I, og enentydig forbindelse mellem idealerne I_1, hvor $I \subseteq I_1 \subseteq M$ og idealerne i M/I, og endda således, at vi med et "naturligt" valg af betegnelserne får $M/I_1 = (M/I)/(I_1/I)$ (hvormeget ligger der i glosen "naturligt"?).

15) 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.

16) Lad $(M,+,\cdot)$ være en kommutativ ring og I et ideal i ringen. Ved "radikalet" rad(I) forstås mængden $\bigcup_{n \in \acute{N}} \{a \mid a^n \in I\}$. Vis, at rad(I) er et ideal.
Vis endvidere, at $\mathrm{rad}(\mathrm{rad}(I)) = \mathrm{rad}(I)$ og at $\mathrm{rad}(I_1 \cap I_2) = \mathrm{rad}(I_1) \cap \mathrm{rad}(I_2)$.
Det er klart, at $I \subseteq \mathrm{rad}(I)$; giv et eksempel på et ideal I i ringen $(\acute{Z},+,\cdot)$, således at I er en ægte delmængde af sit radikal.

17) Lad $(M,+,\cdot)$ være en kommutativ ring og I_1 og I_2 to idealer i ringen. Vis, at mængden $\bigcup_{a_2 \in I_2} \{x \mid xa_2 \in I_1\}$ er et ideal i ringen ("idealkvotienten" $I_1 : I_2$).
Giv ved hjælp af idealer af formen $\acute{Z}_m$ i ringen $(\acute{Z},+,\cdot)$ eksempler 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.

18) Vis, at legemet af de rationale tal ikke indeholder noget ægte egentligt dellegeme.

19) Vis, at en endelig ring, hvori nulreglen gælder, er et legeme.

20) Vis, at i et vilkårligt legeme er centrum et dellegeme (smlgn. øv. 1 og øv. 3).

21) Vis, at mængden af komplekse tal $M = \{\frac{a + b\sqrt{-3}}{2}\}$, hvor $a,b \in \acute{Z}$ og a+b er lige, med sædvanlig addition og multiplikation udgør en ring. Vis, at $I = \{a + b\sqrt{-3}\}$, hvor $a,b \in \acute{Z}$ 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 (idet resultatet fra øv. 19 kan benyttes).
Bestem samtlige automorfier af M/I.
Vis, at ethvert legeme, som har samme elementantal som M/I er isomorft med M/I.

22) Lad (M,+,·) være en kommutativ ring, der kun har trivielle idealer. Vis, at enten er den et legeme, eller også er det en ring af den art, hvori alle produkter er 0 (omtalt i eks. 3, AT 1, side 4).

23) Lad (M,+,·) være en kommutativ ring med etelement.
Et ideal I i ringen kaldes et primideal, dersom nulreglen gælder i M/I. Vis, at I er primideal hvis, og kun hvis $a \cdot b \in I \Rightarrow a \in I \vee b \in I$.
Et ideal I i ringen kaldes maximalideal, dersom M/I er et (egentligt) legeme. Vis, at I er et maximalideal hvis, og kun hvis der ikke findes noget ægte delideal af M, som har I som ægte delmængde; ved beviset kan man med fordel anvende resultaterne fra øv. 14 og øv. 22. (Maximalidealet er tidligere omtalt i øv. 11; hvad bliver legemet M/I i denne øvelse?)
Sammenlign for en given ring mængden af primidealer og mængden af maximalidealer, og giv eventuelt et eksempel på at disse mængder kan være forskellige.

24) Lad $(M,+,\cdot)$ være et kommutativt legeme, i hvilket $1+1 = 2 \neq 0$. Lad f være en afbildning af M ind i sig selv, således at $f(x+y) = f(x) + f(y)$ og $f(x)\cdot f(\frac{1}{x}) = f(1) \neq 0$. Vis, at f er en isomorfi af $(M,+,\cdot)$ på et (ægte eller uægte) dellegeme af sig selv. (Benyt først formlen $\frac{1}{1-x} + \frac{1}{1+x} = \frac{2}{1-x^2}$ til at vise, at $f(x^2) = f(x)^2$, og benyt derefter den frade kvadratiske formers teori bekendte fremstilling af et produkt ved hjælp af kvadrater).

25) Lad $(M,+,\cdot)$ være et kommutativt legeme, i hvilket $1+1 = 2 \neq 0$. Lad G være en undergruppe i $(M,+)$ for hvilken det gælder, at de inverse af elementerne i $G \setminus \{0\}$ også, suppleret med $\{0\}$, udgør en undergruppe i $(M,+)$. Vis, at der findes et (ægte eller uægte) dellegeme L af $(M,+,\cdot)$, således at $G = \{a\cdot x \mid x \in L\}$, hvor a er et element fra $G\setminus\{0\}$. (Benyt først formlen $x^2y^{-1} = x+((x-y)^{-1}-x^{-1})^{-1}$ til at vise, at $x,y \in G \setminus\{0\} \Rightarrow x^2y^{-1} \in G \setminus \{0\}$, og slut heraf at $x,y,z \in G \setminus \{0\} \Rightarrow xyz^{-1} \in G \setminus \{0\}$).

26) Lad $(M,+,\cdot)$ være ringen af n × n-matricer af reelle tal og med 0 under diagonalen (omtalt i øv. 6). Vis, at delmængden M_j bestående af matricer hvori $a_{jj} = 0$, udgør et ideal i ringen, og vis, at dette er et maximalideal (se øv. 23). Eftervis, at der ikke findes andre maximalideale r end de nævnte ($1 \leqq j \leqq n$), og bestem derved samtlige homomorfier af $(M,+,\cdot)$ ind på $(\mathbb{R},+,\cdot)$.

27) Bestem samtlige automorfier og endomorfier af den i øv. 10 omtalte ring (vis først, at de konstante funktioner er fixelementer ved enhver ikke-triviel endomorfi (først betragtes rationale værdier), og at funktioner $\geqq 0$ afbildes i funktioner $\geqq 0$. Vis dernæst, at ligelig konvergentfølge afbildes i ligelig konvergent følge, og udnyt Weierstrass' approximationssætning).

28) 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.

29) 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 $a \cdot x = e$.

30) Lad M være mængden af kontinuerte funktioner $x(t)$, som afbilder $\mathbb{R}$ ind i $\mathbb{R}$ 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).

§2. Polynomier. Hele tal.

Lad $(M,+,\cdot)$ være en ring, om hvilken vi for simpelheds skyld antager, at den er kommutativ, har et etelement og, at nulreglen gælder (en sådan ring kaldes ofte "integritetsområde"; prototypen er de hele tals ring $(Ź,+,\cdot)$). Mængden af følger $a = (a_0,a_1,a_2,\ldots)$ af elementer fra M vil vi organisere som en ring, idet vi definerer kompositioner + og · indenfor mængden (det vil ikke volde besvær, at vi vælger de samme tegn + og · som for kompositionerne i M).

Additionen defineres, idet vi sætter følgesummen a + b lig følgen $c = (c_0,c_1,c_2,\ldots)$, hvor $c_n = a_n+b_n$. Man ser let, at følgerne med denne komposition udgør en kommutativ gruppe, hvis neutrale element (følgeringens nulelement) bliver nulfølgen $(0,0,0,\ldots)$. Multiplikationen defineres, idet vi sætter følgeproduktet a·b lig følgen $c = (c_0,c_1,\ldots)$, hvor $c_n = \sum_{j=0}^{n} a_j b_{n-j}$.

Multiplikationen bliver kommutativ (fordi ringen M var kommutativ), og endvidere bliver den associativ, idet man finder

$$a \cdot b \cdot c = d = (d_0,d_1,\ldots), \text{ hvor } d_n = \sum_{j+k+l=n} a_j b_k c_l,$$

uanset hvorledes man sætter parenteser i produktet a·b·c. Endvidere bliver den distributiv m.h.t. additionen, hvilket let ses (fordi udtrykket for c_n ovenfor åbenbart er lineært i a_j og ligeledes lineært i b_{n-j}). Der findes et etelement (neutralt element ved multiplikationen), nemlig følgen $(1,0,0,\ldots)$, hvor 1 er etelementet i ringen $(M,+,\cdot)$. Endelig gælder nulreglen, thi dersom a og b ikke er nulfølger, findes der i følgen a et første element $a_k \neq 0$ og i følgen b et første element $b_m \neq 0$, og af produktfølgens definition finder man så $c_{k+m} = a_k b_m \neq 0$.

Mængden af følger er altså hermed organiseret som et integritetsområde. Som mnemoteknisk regel for følgemængdens organisation kan man opfatte a som koefficientfølge i en "formel potensrække" $a(X) = \sum_{n=0}^{\infty} a_n X^n$, og så fås summen c = a + b som følgen af koefficienter til den formelle sum af potensrækkerne a(X) og b(X), og produktet c = a·b som følgen af koefficienter til det formelle produkt af a(X) og b(X), idet man i produktudregningen sætter $X^j \cdot X^{n-j} = X^n$. Den hermed organiserede ring af følger kaldes derfor ofte potensrækkeringen over ringen (M,+,·), og betegnes hyppigt M[[X]]. Det turde være overflødigt at anføre, at det her omtalte intet har at gøre (umiddelbart i hvert fald) med spørgsmål om konvergente rækker.

Til $a_0 \in M$ kan vi lade svare følgen $(a_0,0,0,\ldots) \in M[[X]]$, og man ser let af definitionerne af addition og multiplikation, at vi derved har fået en isomorf afbildning af ringen (M,+,·) på "konstanterne" i potensrækkeringen M[[X]]. Vi kan derfor, om vi vil, udskifte betegnelserne og i stedet for $(a_0,0,0,\ldots)$ blot skrive a_0, og kan opfatte M[[X]] som en nyskabt udvidelsesring for (M,+,·).

Hvis man i potensrækkeringen betragter mængden af følger $(a_0,a_1,a_2,\ldots)$, hvori kun endelig mange elementer er ulig 0, så udgør disse følger en delring, thi man ser, at de med hensyn til kompositionen + udgør en gruppe, og at produktet af sådan to følger er en følge af samme art. Delringen indeholder etelementet, og endvidere er den kommutativ, og nulreglen gælder (fordi potensrækkeringen har disse egenskaber), den er altså et integritetsområde. Den kaldes integritetsområdet af polynomier over (M,+,·), og betegnes hyppigt M[X].

M[X] indeholder specielt følgen $(0,1,0,0,\ldots)$ som vi vil betegne X. Udregner vi de sukcessive potenser af X finder vi

$$X = (0,1,0,0,\ldots)$$
$$X^2 = (0,0,1,0,\ldots)$$
$$X^3 = (0,0,0,1,0..)$$
$$\text{o.s.v.}$$

og da vi endvidere har sat $a_k = (a_k,0,0,\ldots)$ finder vi af den ovennævnte mnemotekniske regel for følgemængdens kompositioner, at det vilkårlige element $(a_0,a_1,\ldots,a_n,0,0,\ldots)$ indenfor integritetsområdet af polynomier M[X] kan skrives på formen

$$a = a_0 + a_1X + \ldots + a_nX^n,$$

hvor lighedstegnet er et sædvanligt lighedstegn, og ikke blot en formel skrivemåde. Når vi fremtidig taler om et polynomium a vil vi tænke os det skrevet på denne form, og for at understrege dette ofte kalde det a(X). Addition og multiplikation af polynomier bliver derved reduceret til simple (og fra skolen velkendte) regninger. Vi skal her kun betragte "polynomier i en variabel", men "polynomier i to variable" kunne på analog måde defineret ved hjælp af sæt af elementer a_{jk}, hvor $j,k \in \{0\} \cup \dot{N}$, og tilsvarende for "flere variable".

Ved graden af det ovenfor opskrevne polynomium a vil vi, såfremt $a \neq 0$, forstå det største index k, for hvilket $a_k \neq 0$, medens vi vil tilskrive nulpolynomiet $a = 0$ en grad $-\infty$. Vi finder så, at graden af en sum af to polynomier er mindre end eller lig den maximale af addendernes grader, og at graden af et produkt af to polynomier er lig summen af faktorernes grader (idet vi på en selvfølgelig måde regner med $-\infty$).

Et kommutativt legeme er automatisk et integritetsområde, da det har et etelement og nulreglen gælder. Lad os antage, at $(M,+,\cdot)$ er et kommutativt legeme. For to givne polynomier D(X)

("dividend") og d(X) ("divisor"), hvor d(X) $\neq 0$, fra M[X] kan vi for ethvert q(X) $\in$ M[X] opskrive

$$r(X) = D(X) - d(X)\cdot q(X),$$

og det er her muligt ved en velkendt divisionsalgoritme - ved hvilken man benytter at (M,+,·) er et legeme, idet man dividerer koefficienten til højestegradsleddet i d(X) op i visse andre elementer fra M - at bestemme q(X) således at graden af r(X) bliver mindre end graden af d(X).

Inden vi går videre skal vi minde om begrebet hovedideal. Derved forstod vi det mindste ideal I indenfor en given ring som indeholder et givet element a. Hvis ringen er et integritetsområde (L,+,·), så er hovedidealet netop $I = \{q\cdot a \mid q \in L\}$ (se AT 1, 12). Indenfor integritetsområdet M[X] af polynomier over et legeme (M,+,·) er det af polynomiet a(X) frembragte hovedideal altså netop mængden af polynomier $\{a(X)\cdot q(X)\}$, hvor q(X) gennemløber M[X].

I ringen M[X] af polynomier over et legeme (M,+,·) er ethvert ideal et hovedideal. Bevis: For nulidealet {0} er påstanden triviel, idet det åbenbart er det af 0 frembragte hovedideal, og iøvrigt kan skrives som $\{0\cdot q(X) \mid q(X) \in M[X]\}$. Ellers indeholder idealet egentlige polynomier, og lad os fra idealet tage et d(X) $\neq 0$ af lavest forekommende grad. For et vilkårligt D(X) fra idealet kan vi ved divisionsligningen ovenfor bestemme et r(X) af lavere grad end d(X), og af idealbetingelserne Id 1 og Id 2 (se AT 1,10) ser vi, at r(X) tilhører idealet; det må da have graden $-\infty$, altså være 0, og $D(X) = d(X)\cdot q(X)$. Idealet er følgelig netop det af d(X) frembragte hovedideal.

Lad os på dette sted bemærke, at vi ved et ganske lignende bevis kan indse, at i integritetsområdet (Ź,+,·) er ethvert ideal et hovedideal. Thi for to givne hele tal D og d, hvor d $\neq 0$

kan vi for ethvert $q \in \acute{Z}$ opskrive en divisionsligning

$$r = D - d \cdot q,$$

og det er her muligt at bestemme q således at $|r|<|d|$. Derefter kan vi kopiere det foregående bevis: For nulidealet $\{0\}$ er påstanden triviel, idet det åbenbart er det af 0 frembragte hovedideal. Ellers indeholder idealet hele tal forskellige fra0, og lad os fra idealet tage et $d \neq 0$, som har den lavest forekommende værdi af $|d|$. For et vilkårligt D fra idealet kan vi ved divisionsligningen bestemme et r, så $|r|<|d|$, og af idealbetingelserne ser vi, at r tilhører idealet: vi har da $r = 0$, og $D = d \cdot q$, så idealet er det af d frembragte hovedideal. Iøvrigt følger sætningen også af at idealet er en undergruppe i $(\acute{Z},+)$ (se AG II,2,11).

For et integritetsområde, hvori ethvert ideal er et hovedideal, skal vi se at man kan bevise nogle betydningsfulde sætninger; man har derfor indført en særlig betegnelse for et sådant integritetsområde, nemlig <u>hovedidealring</u>. Og vi har altså vist, at ringen af polynomier over et kommutativt legeme er en hovedidealring, og at $(\acute{Z},+,\cdot)$ er en hovedidealring.

Som eksempel på et ideal i $M[X]$ kan vi betragte mængden af polynomier hvori $a_0=a_1=0$, altså $I = \{a_2X^2+a_3X^3+\ldots+a_nX^n\}$; det er åbenbart netop hovedidealet bestående af alle multipla af X^2. Hvis vi nu i $M[X]$ tager delmængden L bestående af polynomier hvori $a_1 = 0$, så vil $M[X] \supset L \supset I$, og L ses at være et integritetsområde, der også indeholder I som ideal; men I er ikke noget hovedideal i L (fordi $X^2 \in I$ og $X^3 \in I$, og der let ses at komme en modstrid, når man forsøger at skrive disse elementer på formen $a(X)\cdot q(X)$ med $q(X) \in L$ og et fælles $a(X) \in I$). Altså er L et eksempel på et integritetsområde, der ikke er en

hovedidealring.

Lad nu $(M,+,\cdot)$ være en hovedidealring, hvilket altså betyder, at det er et integritetsområde, hvori ethvert ideal er af formen $I_c = \{\text{multipla af } c\}$; omvendt vil ethvert c frembringe et ideal I_c, og vi har $c \in I_c$. Vi skal nedenfor komme tilbage til det fænomen, at det samme ideal I_c kan frembringes af forskellige c, det er f.eks. klart at $I_c = I_{-c}$. Vi ser, at $\underline{I_d \subseteq I_c} \Rightarrow \underline{d \in I_c} \Rightarrow \underline{d = \text{multiplum af } c} \Rightarrow \underline{\text{ethvert multiplum af } d = \text{multiplum af } c} \Rightarrow \underline{I_d \subseteq I_c}$, således at alle de her understregede relationer udtrykker det samme, nemlig at d er et multiplum af c. At d er et multiplum af c skrives kort med betegnelsen $c|d$ (læses: "c går op i d").

En hovedidealring har to vigtige egenskaber: fællesmålegenskaben og den opstigende kædes egenskab.

Fællesmålsegenskaben: Til to elementer a og b findes altid et d (kaldet "største fælles mål for a og b"), så for alle c er

$$c|a \wedge c|b \iff c|d.$$

Egenskaben udsiger altså, at mængden af fælles divisorer ("mål", et udtryk fra Euklid) for a og b netop er samtlige divisorer i et største fælles mål d(blandt disse er d selv; glosen "største" i "største fælles mål" skal vi ikke udlægge, vi har ikke nogen størrelsesordning i M).

Beviset klares let, idet vi udtrykker påstanden på idealform $a \in I_c \wedge b \in I_c \iff d \in I_c$. Endvidere benytter vi, at fællesmængden for (endelig eller uendelig mange) idealer i en ring igen er et ideal i ringen; dette kan bevises med idealkarakteriseringen Id1 og Id2 (se AT 1,10) ganske som de tilsvarende sætninger om fællesmængder for delringe og for undergrupper (se

AT 1,5-6). Thi så er fællesmængden for de idealer, som indeholder elementerne a og b netop et ideal, og når vi er i en hovedidealring kan dette skrives på formen I_d, og så er både venstre- og højresiden i påstandens formel (på idealformen) opfyldt netop når $I_d \subseteq I_c$.

Den opstigende kædes egenskab: Har vi en følge af idealer $I' \subseteq I'' \subseteq \ldots \subseteq I^{(n)} \subseteq \ldots$, så er alle $I^{(j)}$ ens fra et vist trin.

Bevis: Vi skal først vise, at foreningsmængden $\bigcup_j I^{(j)}$ er et ideal I, og det ses let ved at vise, at den opfylder egenskaberne Id1 og Id2; for at vise, at $x,y \in I$ medfører $x+y \in I$ benytter vi, at idealerne er indeholdt i hinanden på den anførte måde; der må da findes et fælles n så $x,y \in I^{(n)}$ og derfor $x+y \in I^{(n)} \subseteq I$; sammenlignet hermed er de øvrige dele af beviset simple. Når vi nu er i en hovedidealring kan idealet I skrives på formen I_d, hvor $d \in I$, men det vil jo sige, at der findes et k så $d \in I^{(k)}$, og derfor $I = I_d \subseteq I^{(k)}$, og altså $I' \subseteq I'' \subseteq \ldots \subseteq I = I^{(k)}$, og alle idealerne i kæden er derfor ens fra og med $I^{(k)}$.

Begge de to egenskaber omhandler i realiteten hovedidealringens multiplikative struktur, og det er denne struktur vi skal se nærmere på; nulelementet er uden interesse i denne forbindelse, så det vi vil betragte er $(M\setminus\{0\},\cdot)$. Dette er en mængde med en komposition, der er associativ og kommutativ, med et etelement, og således at division er højst entydig (men ikke altid mulig).

Et regulært element r er et element, som har et inverst r^{-1}. De regulære elementer kan derfor karakteriseres som de elementer, med hvilke det altid er muligt at dividere. Lad mængden af de regulære elementer hedde E; man ser, at $(E,\cdot)$ udgør en gruppe (for-

di etelementet $\in E$, og endvidere $r \in E \Rightarrow r^{-1} \Rightarrow E$ idet $(r^{-1})^{-1} = r$, og endelig $r_1, r_2 \in E \Rightarrow r_1 r_2 \in E$ idet $(r_1 r_2)^{-1} = r_1^{-1} \cdot r_2^{-1}$). Iøvrigt ser man, at E er den største delmængde af $M \setminus \{0\}$, som med multiplikationen udgør en gruppe.

Division med et regulært element er en triviel mulighed, som vi gerne vil se bort fra ved undersøgelsen af den multiplikative struktur. Det opnås således: Vi sætter $x \equiv y$ dersom $x = ry$, hvor $r \in E$; man ser, at $\equiv$ er en ækvivalensrelation indenfor $M \setminus \{0\}$, og at den er harmonerende med multiplikationen, d.v.s. $x \equiv y \wedge x_1 \equiv y_1 \Rightarrow xx_1 \equiv yy_1$. Ifølge den almindelige homomorfisætning (AT 1,9) findes der så en afbildning $x \to x'$, hvorved $(M \setminus \{0\}, \cdot)$ afbildes homomorft på en mængde med komposition $(M', \odot)$. Som elementer $x' \in M'$ kan vi tage ækvivalensklasserne, d.v.s. klasser af elementer fra $M \setminus \{0\}$, som indbyrdes kun afviger med en regulær faktor. Billedet $(M', \odot)$ er en mængde med en komposition, som er associativ og kommutativ og med etelement, og $x|y \Rightarrow x'|y'$ (idet vi for simpelheds skyld benytter det samme gå-op-tegn ved $\odot$ som ved $\cdot$). Lad os omvendt antage, at $x'|y'$, der findes da et z' så $x' \odot z' = y'$, og i denne ligning er venstresiden billede af $x \cdot z$ og højresiden er billede af y, og vi har derfor $x \cdot z \equiv y$, eller $x \cdot z \cdot r = y$, hvoraf ses, at $x|y$; endvidere ses af denne sidste ligning, at $z = r^{-1} \cdot \frac{y}{x}$ for ethvert z der har et billede z' som passer i ligningen $x' \odot z' = y'$, og denne ligning bestemmer derfor z pånær en regulær faktor, og dermed z' entydigt. Vi har dermed vist, at $x|y \iff x'|y'$ og at der er højst endtydig (men ikke altid mulig) division i $(M', \odot)$. I analogi med tidligere betegnelser kan vi sige, at strukturen $(M', \odot)$ er faktorstrukturen $(M \setminus \{0\}, \cdot)/E$.

Eksempler: I integritetsområdet af hele tal er de regulære elementer +1 og -1, og det foregående udtrykker blot, at vi

ved en undersøgelse af den multiplikative struktur af de fra 0 forskellige hele tal vil "se bort fra fortegnet"; faktorstrukturen $(\acute{Z}\setminus\{0\},\cdot)/\{+1,-1\}$ bliver isomorf med $(\acute{N},\cdot)$, altså den multiplikative struktur af de naturlige tal. I integritetsområdet M[X] af polynomier over legemet M er de regulære elementer netop de fra 0 forskellige konstanter, og det foregående udtrykker blot, at vi ved en undersøgelse af den multiplikative struktur af mængden af de fra 0 forskellige polynomier vil "se bort fra konstante faktorer".

$I(M',\odot)$ er etelementet e' det eneste regulære element, thi efter det foregående vil $r'|e' \Rightarrow r|e$, så at r er regulær og dets billede r' derfor e'. Heraf følger let, at $d'|c' \wedge c'|d'$ er ensbetydende med at $c' = d'$, thi relationen udsiger jo, at $\frac{c'}{d'}$ eksisterer $\in M'$ og har en invers $\in M'$ og derfor må være lig e'. Betragter vi idealer har vi $I_c = I_d \iff I_c \subseteq I_d \wedge I_d \subseteq I_c \iff d|c \wedge c|d \iff d'|c' \wedge c'|d' \iff c' = d' \iff c \equiv d$; vi har derfor at et ideal I_c bestemmer sit frembringerelement c entydigt på nær en regulær faktor, og endvidere at der er enentydig forbindelse mellem idealerne og elementerne $c' \in M'$, og ved denne forbindelse vil $I_d \subseteq I_c$ svare til $c'|d'$.

Udtrykt ved elementerne fra M' bliver fællesmålsegenskaben: Til to elementer a' og b' findes altid et entydigt bestemt d' således at $c'|a' \wedge c'|b' \iff c'|d'$. Ved at operere i M' har vi opnået den fordel, at d' er entydigt bestemt, tidligere var det kun idealet I_d som var entydigt bestemt. Vi vil betegne d' som <u>det største fælles mål for a' og b', og benytte betegnelsen (a',b')</u>. Vi kan opfatte det som fremgået af a' og b' ved en kompositionsforskrift, for hvilken vi altså benytter tegnet (,); kompositionen er åbenbart kommutativ og associativ (men der gælder ikke forkortningsregel eller findes neutralt element, smlgn.

AG II,1, øv. 1,d)). Vi vil lejlighedsvis også tillade os at undlade indførelsen af M' og nøjes med betegnelser fra M\{0}, og (a,b) skal så betyde et (på nær en regulær faktor entydigt bestemt) største fælles mål d for a og b.

Multiplikationen er distributiv m.h.t. største-fælles-måls-dannelse, idet $(m'\odot a', m'\odot b') = m'\odot(a',b')$, eller med den løse skrivemåde $(ma,mb) = m(a,b)$. Beviset benytter gentagne gange, at $p|q \iff mp|mq$. Det forløber iøvrigt således: Vi sætter $(a,b) = d$ og $(ma,mb) = D$; vi har $d|a \wedge d|b \Rightarrow md|ma \wedge md|mb \Rightarrow md|D$, og vi kan derfor skrive D på formen $D = mx$, hvor $d|x$; så er $D|ma \wedge D|mb \iff mx|ma \wedge mx|mb \Rightarrow x|a \Rightarrow x|b \Rightarrow x|d$, og denne sidste kombineret med $d|x$ giver, at $d \equiv x$ (idet $I_d = I_x$, smlgn. forrige side), eller altså $D = mx = md$ på nær den løse formulerings uundgåelige ubestemthed med en regulær faktor (for valgt d kan vi sige, at $D = md$ er en brugbar værdi for (ma,mb)).

Fællesmålsegenskaben medfører, at dersom $c|ab$, da kan c skrives på formen $c = c_1c_2$, hvor $c_1|a$ og $c_2|b$. Bevis: Vi vælger c_1 som en af værdierne for (a,c), hvormed vi har opnået, at $c_1|a$ og endvidere, at $c_1|c$, så at $c = c_1c_2$ med et vist c_2; det er evident, at $c|cb$, og derfor $c|ab \wedge c|cb \Rightarrow c|(a,c)b$ eller $c_1c_2|c_1b \Rightarrow c_2|b$. Ved successiv anvendelse heraf ses, at hvis $c|a_1a_2\ldots a_s$, så er $c = c_1c_2\ldots c_s$, hvor $c_j|a_j$ for $j = 1,2,\ldots,s$, eller med andre ord, det er muligt at opløse c og $a_1,a_2,\ldots,a_s$ i faktorer, således at alle de faktorer, der står foran gå-op-tegnet også står efter gå-op-tegnet. Ved succesiv anvendelse heraf ses, idet man undervejs bortdividerer de fælles faktorer, at den understregede påstand også er gyldig, hvis man har en situation $c_1c_2\ldots c_t|a_1a_2\ldots a_s$.

Dersom specielt $c_1c_2\ldots c_t = a_1a_2\ldots a_s$ er det muligt at foretage en videreopløsning i faktorer på begge sider af lig-

hedstegnet, således at man får den samme mængde faktorer (gentagelser medregnet) på begge sider af lighedstegnet. Thi ifølge det foregående kan vi opnå, at alle faktorer på venstre side også findes på højre side, og de overskydende på højre side har produktet 1, og kan derfor fås ved at trække en faktor 1 ud på venstre side og opløse den. Af homomorfien $(M\setminus\{0\},\cdot) \to (M',\odot)$ er det klart, at ordret det samme resultat gælder i $(M',\odot)$.

Inden vi udnytter den opstigende kædes egenskab skal vi give et par definitioner.

Et element $p' \in M'$ kaldes reducibelt, dersom det kan skrives som et produkt $a'\odot b'$, hvori ingen af faktorerne er etelementet. Et element $p \in M\setminus\{0\}$ kaldes reducibelt, dersom p' er reducibel, eller med andre ord: p er reducibel, dersom det kan skrives som produkt af to ikke-regulære faktorer. Hvis $p' \in M'$ ikke er etelementet og ikke er reducibelt, kaldes det irreducibelt. Et element $p \in M\setminus\{0\}$ kaldes irreducibelt, dersom p' er irreducibel, eller med andre ord: p er irreducibel, dersom det for enhver produktfremstilling $p = ab$ gælder, at en af faktorerne, men ikke dem begge, er regulær.

Eksempler: Som nævnt vil integritetsområdet $(\acute{Z},+,\cdot)$ give en struktur $(M',\odot)$, der kan repræsenteres ved $(\acute{N},\cdot)$; heri vil de reducible elementer netop være de sammensatte tal, og de irreducible vil være primtallene. Indenfor en polynomiumsring er et polynomium reducibelt, dersom det kan skrives som produkt af to polynomier fra ringen, ikke konstanter; hvis dette ikke er muligt, og polynomiet ikke selv er en konstant, så er det irreducibelt. F.eks. er $8(X^2-2)$ reducibelt i $\acute{R}[X]$, medens det samme polynomium er irreducibelt i $\acute{Q}[X]$; polynomier af første grad er altid irreducible.

Den opstigende kædes egenskab udsagde, at har man idealer,

hvor $I' \subsetneqq I'' \subsetneqq \ldots$, så er de alle ens fra et vist trin. I en hovedidealring kan man skrive $I^{(n)}$ på formen I_{a_n}, og betingelsen $I^{(n)} \subsetneqq I^{(n+1)}$ betyder, at a_n er et multiplum af a_{n+1}, altså at $a_n = a_{n+1}q_n$, og ifølge det tidligere vil de to idealer være lige store, hvis, og kun hvis q_n er regulær. Den opstigende kædes egenskab udsiger altså, at hvis $a_1 = a_2q_1, \ldots, a_n = a_{n+1}q_n, \ldots$, så er alle q_n regulære fra et vist trin.

Vi ser nu, at dersom $M\setminus\{0\}$ overhovedet indeholder ikke-regulære elementer, så eksisterer der irreducible elementer; thi ellers kunne vi tage et ikke-regulært element a_1, skrive det som produkt a_2q_1 af to ikke-regulære, igen skrive a_2 som produkt a_3q_2 af to ikke-regulære o.s.v., og derved ville vi få en modstrid med den opstigende kædes egenskab. Men ræsonnementet giver endda mere, thi det viser jo, at et vilkårligt ikke-regulært element a_1 er deleligt med et irreducibelt element. Og så viser det endda endnu mere, nemlig at <u>i en hovedidealring kan ethvert ikke-regulært element skrives som produkt af irreducible elementer</u>. For enten er a_1 irreducibel, og så er det i orden, eller også kan vi skrive a_1 som produkt a_2q_1, hvor q_1 er irreducibel og a_2 er ikke-regulær; enten er a_2 irreducibel, og så er det i orden, eller også kan vi skrive a_2 som produkt a_3q_2, hvor q_2 er irreducibel og a_3 er ikke-regulær; således fortsættes, men ifølge det foregående skal processen standse, hvilket sker ved at vi møder et irreducibelt a_n, og så har vi den ønskede produktfremstilling $q_1q_2\ldots q_{n-1}a_n$. Det er klart, at resultatet umiddelbart kan overføres til strukturen $(M',\odot)$.

Vi kombinerer nu med resultatet fra fællesmålsegenskaben, og opnår følgende hovedsætning: <u>Lad $(M,+,.)$ være en hovedidealring, og E mængden af dens regulære elementer. I faktorstrukturen</u>

$(M',\odot) = (M\setminus\{0\},\cdot)/E$ gælder det, at ethvert fra etelementet forskelligt element på en og (bortset fra faktorernes rækkefølge) kun een måde kan skrives som produkt af irreducible.

Formulerer vi sætningen for selve hovedidealringen $(M,+,\cdot)$, kommer der den uundgåelige ubestemthed i entydigheden, som skyldes de regulære faktorer, så sætningen bliver: I en hovedidealring kan ethvert fra 0 forskelligt ikke-regulært element a skrives som produkt af irreducible elementer $a = a_1 a_2 \ldots a_s$, og hvis man har to sådanne fremstillinger af a, f.eks. $a_1 \ldots a_s$ og $c_1 \ldots c_t$, så indeholder de lige mange faktorer ($s=t$), og ethvert a_j er pånær en regulær faktor lig et c_j. Sætningens rigtighed følger af det foregående, idet den opstigende kædes egenskab giver produktfremstillingens mulighed, medens fællesmålsegenskaben giver dens entydighed (når $c_1 \ldots c_t = a_1 \ldots a_s$ kan vi videreopløse produkterne indtil de to sider bliver identiske, se side 10, men for en irreducibel faktor findes kun den trivielle opløsning, der består i at udtrække en **regulær faktor**).

Anvendes sætningen på hovedidealringen $(Z,+,\cdot)$ får vi for dens faktorstruktur $(N,\cdot)$: Ethvert naturligt tal større end 1 kan på en og kun een måde skrives som produkt af primtal (talteoriens hovedsætning om den entydige primopløsning).

Anvendes sætningen på hovedidealringen af polynomier over et legeme M får vi: Ethvert polynomium af grad større end 0 kan på en og kun een måde skrives som produkt af irreducible polynomier fra $M[X]$ (idet disse dog kun er bestemt pånær konstante faktorer).

Eksempel: I $R[X]$ kan polynomiet $3(X^4-4)$ skrives som produkt af irreducible, nemlig som $(3X-3\sqrt{2})(X+\sqrt{2})(X^2+2)$, (idet dog den konstante faktor 3 også på andre måder kan "fordeles" på de tre parenteser). Den såkaldte "algebraens fundamentalsætning" - som vi ikke skal bevise her, da den er en sætning fra den matematiske

analyse - udsiger i det væsentlige, at ethvert irreducibelt polynomium i $\check{R}[X]$ er af første eller anden grad.

Vi betragter igen polynomiumsintegritetsområdet $M[X]$ over et legeme $(M,+,\cdot)$; vi antager, at M består af mere end nulelementet, for ellers ville alt blive trivielt. Lad endvidere $(M,+,\cdot)$ være indeholdt i et integritetsområde $(L,+,\cdot)$, og lad c være et vilkårligt element fra L.

Der findes netop een 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 den ikke kan være anderledes. Vi beskriver afbildningen kort ved at sige, at vi <u>sætter X lig c i polynomiet</u>, 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 integritetsområdet L, vil nulreglen gælde for billedet; dette er derfor et integritetsområde, og vi betegner det $M[c]$, og kalder det for <u>integritetsområdet fremgået af M ved adjunktion af c</u>; dets 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, altså ikke tilhører kernen. Integritetsområdet $M[c]$ 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 afbildningen er enentydig, 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 $q_0+q_1X+\ldots q_nX^n \leftrightarrow q_0+q_1\pi+\ldots+q_n\pi^n$, 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 et hovedideal I_d frembragt af et egentligt polynomium $d(X) \in M[X]$, og da I er en ægte del af $M[X]$, må d(X) have en grad større end 0 (ellers var d(X) en konstant, d.v.s. et regulært element, og I blev lig hele $M[X]$). Idealet I består netop af mængden af multipla af d(X), og vi får derfor, at nødvendigt og tilstrækkeligt for at c er rod i et polynomium a(X) er, at a(X) er delig med d(X). Dette d(X) er ikke bestemt entydigt, men kun pånær en konstant faktor.

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-

gritetsområdet $(L,+,\cdot)$ indeholde dellegemet $(M,+,\cdot)$; 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 $d(X)$.

Lad os igen et øjeblik betragte en vilkårlig hovedidealring $(K,+,\cdot)$, og lad d være et irreducibelt element i denne. K er lig $I_1 = I_r$ for ethvert regulært r, medens I_d er en ægte delmængde af K, fordi d ikke er regulær. Lad os omvendt antage, at I_d er ægte delmængde af et ideal I_s, så vil $s \mid d$, hvoraf følger, at enten er s regulær, eller også vil s afvige fra d med en regulær faktor; det sidste tilfælde kan ikke indtræffe, for så var $I_s = I_d$, og s er derfor regulær, således at $I_s = K$. Vi har altså, at i en hovedidealring er et af et irreducibelt element d frembragt ideal I_d maximalt, i den forstand at det ikke er indeholdt i noget andet ideal end hele ringen. Man ser iøvrigt let, at dersom d er reducibel, så er idealet I_d ikke maximalt.

Lad nu I_d være maximalt ideal i en hovedidealring $(K,+,\cdot)$. Det er kerne ved en homomorfi f, ved hvilken $(K,+,\cdot)$ afbildes i en ring $(L,+,\cdot)$. Ifølge de almindelige resultater om homomorf afbildning af en ring (se AT 1, side 6) vil $(L,+,\cdot)$ være en kommutativ ring med etelement, fordi $(K,+,\cdot)$ har disse egenskaber, hvorimod nulreglens gyldighed jo ikke umiddelbart kan overføres; men vi vil faktisk vise et endnu stærkere resultat nemlig at $(L,+,\cdot)$ er et legeme. Lad a være et fra 0 forskelligt element i L, mængden af multipla af a udgør et hovedideal $I_a \subseteq L$. Der findes da en homomorfi g, med I_a som kerne, ved

hvilken $(L,+,\cdot)$ overføres i en ny ring, og denne ses at være fremgået af $(K,+,\cdot)$ ved anvendelse af den sammensatte afbildning $g \circ f$, der selv er en homomorfi, fordi den er sammensat af to homomorfier. Kernen for $g \circ f$ er et ideal i K, og det indeholder I_d, og det indeholder desuden mere, nemlig også $f^{-1}(a)$; det må derfor være hele K, fordi I_d var et maximalt ideal. Den sidste billedring består derfor kun af et nulelement, og I_a, som var kernen ved g, omfatter derfor hele L, d.v.s. at ethvert element i L er et multiplum af a; indenfor L er det altså altid muligt at dividere med det vilkårlige, blot fra 0 forskellige, element a. Dermed har vi vist: Hvis d er et irreducibelt element i en hovedidealring $(K,+,\cdot)$, så er faktorringen $(K,+,\cdot)/I_d$ et legeme.

Første anvendelse: I hovedidealringen $(\acute{Z},+,\cdot)$ er de irreducible elementer +p og -p, hvor p er et primtal; de giver anledning til idealerne $\acute{Z}_p$ = mængden af multipla af p, og faktorringen $(\acute{Z},+,\cdot)/\acute{Z}_p$ er den ofte tidligere omtalte restklassering modulo p. Sætningen viser nu, at restklasseringen af de hele tal modulo p (p=primtal) er et legeme. Dette har p elementer, og vi ser altså specielt, at for ethvert primtal p eksisterer der et legeme med p elementer.

Anden anvendelse: Når c er algebraisk over M, så er kernen ved homomorfien $M[X] \to M[c]$ netop idealet I_d, hvor d er et irreducibelt polynomium $\in M[X]$, og vi har derfor at integritetsområdet M[c] er et legeme, når c er algebraisk over legemet M.

Hvis man indenfor et integritetsområde $(L,+,\cdot)$ har et delintegritetsområde M og et element c, så betegner man almindeligt med M[c] det mindste integritetsområde indenfor $(L,+,\cdot)$, for hvilket $M \subsetneq M[c]$ og $c \in M[c]$. Vi siger, at

M[c] er integritetsområdet fremgået af M ved adjunktion af c (indenfor L). Benævnelsen ses at stemme overens med alt det foregående, og specielt bemærkes, at M[X] er det mindste integritetsområde, der indeholder X = (0,1,0,...). For legemer benyttes analoge betegnelser med runde parenteser: Hvis man indenfor et legeme (L,+,·) har et dellegeme M og et element c, så betegner man almindeligt med M(c) det mindste legeme indenfor (M,+,·) 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). Vi ser, at M(c) er kvotientlegemet for M[c]. Specielt ses, at M(X) er mængden af "polynomiumsbrøker"

$$\frac{a_o+a_1X+\ldots+a_nX^n}{b_o+b_1X+\ldots+b_mX^m} \quad ,$$

og at M[X] er en ægte del af M(X), fordi f.eks. $\frac{1}{X} \notin M[X]$. Hvis c er algebraisk over M, så er M(c) = M[c].

Når c er rod i polynomiet d(X), så er d(c) = 0. For et vilkårligt polynomium a(X) kan vi opskrive en divisionsligning $a(X) = d(X)\cdot q(X) + r(X)$, og homomorfien $X \to c$ giver så at $a(c) = d(c)\cdot q(c)+r(c) = r(c)$ og her kan vi i divisionsligningen altid vælge r(X) af lavere grad end d(X). Vi kan nu sammenfatte nogle af de foregående resultater i følgende sætning:

Lad c være et element, der er indeholdt i et integritetsområde, der også indeholder et dellegeme (M,+,·). Enten er c transcendent over M, og dette indtræffer specielt for X = (0,1,0,...); så er integritetsområderne M[c] indbyrdes isomorfe (for forskellige c), og specielt alle isomorfe med polynomiumsringen M[X], og M[c] er ikke noget legeme; dets kvotientlegeme M(c) er isomorft med legemet M(X) af "polynomiumsbrøker". Eller også er c algebraisk over M; så er integritetsområdet M[c] et

legeme, altså sit eget kvotientlegeme og $M[c] = M(c)$; som fremstilling af elementerne i $M[c]$ kan vi tage alle udtryk af formen $a_0+a_1c+\ldots+a_{n-1}c^{n-1}$, hvor alle $a_j \in M$ og hvor n er graden af det irreducible polynomium, der har c som rod.

Eksempel: Indenfor $(\dot{R},+,\cdot)$ er $\sqrt[3]{2}$ algebraisk over $(\dot{Q},+,\cdot)$; det er rod i det irreducible polynomium X^3-2, og mængden $\{q_0 + q_1\sqrt[3]{2} + q_2\sqrt[3]{2^2} \mid q_0,q_1,q_2 \in \dot{Q}\}$ udgør derfor $\dot{Q}[\sqrt[3]{2}] = Q(\sqrt[3]{2})$; da det er et legeme, er det altid mulig 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, at førstegradspolynomier er irreducible, og sætningen om den entydige faktoropløsning).

Hvis $a(X) \in M[X]$ og $c \in M$, så vil $c \to a(c)$ være en 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. Lad os blot bemærke, at for endelige legemer M vil nulfunktionen: $c \to 0$ for alle $c \in M$

fremkomme for uendelig mange a(X), nemlig for alle delelige med $(X-c_1)(X-c_2)\ldots(X-c_m)$, hvor $c_1,c_2,\ldots,c_m$ er elementerne i M. For uendelige legemer M kan noget sådant ikke indtræffe, da et egentligt polynomium ikke kan have uendelig mange rødder (men for uendelige M findes til gengæld afbildninger af M ind i M, som ikke er polynomiumsfunktioner, f.eks. den afbildning, hvorved $c \to 0$ for alle $c \neq 0$, medens $0 \to 1$).

Vi har hidtil betragtet polynomier d(X) i M[X] og et legeme $(L,+,\cdot)$ med M som dellegeme, og så mødt muligheden af, at et c indeholdt i L kunne være rod i d(X). Dersom der findes en sådan rod c, så er strukturen af legemet M(c) givet, idet legemet er bestemt paanær isomorfi, nemlig som en faktorring $(M[X],+,\cdot)/I_d$. Men selvom vi kun har <u>givet 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 c i d(X)</u>, nemlig løst sagt: den nævnte faktorring. Udførligere: d(X) frembringer et ideal $I_d \subset M[X]$, og ifølge den almindelige homomorfisætning findes der da en homomorf afbildning $a = a(X) \to a'$ af M[X], ved hvilken I_d er kerne; billedet er en faktorring $(M[X],+,\cdot)/I_d$, og da d er irreducibel bliver det et legeme $(L,+,\cdot)$; for mængden af M's elementer er afbildningen enentydig, 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 X' af X vil vi kalde for c, og det vil netop have den ønskede egenskab, thi da vi har opnået at 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 afbildningens kerne er $d(c) = 0$.

Eksempel: Polynomiet X^2+1 er irreducibelt over de reelle

tals legeme $(\acute{R},+,\cdot)$; legemet kan udvides til etlegeme, der indeholder en rod i polynomiet, og en sådan rod kaldes sædvanligvis i, og $\acute{R}[i] = \grave{R}(i)$ er da de komplekse tals legeme $(\acute{C},+,\cdot)$. I den foregående systematiske opbygning af matematikken er kendskab til de komplekse tal intetsteds benyttet, og det ovenstående viser nu, hvorledes man på grundlag af de reelle tal kan indføre de komplekse tal (sammenlign slutningen af forrige §).

I eksemplet gav adjunktion af en rod legemet $\acute{R}(i)$, som også indeholder den anden rod -i. Derimod X^3-2 er irreducibel over $(\acute{Q},+,\cdot)$; legemet $\acute{Q}(\sqrt[3]{2})$ vil kun indeholde een rod til polynomiet, men hvis man til dette legeme dernæst adjungerer en af de komplekse rødder, fås et legeme, der indeholder alle tre rødder til X^3-2.

Øvelser til § 2.

1) Potensrækkeringen $M[[X]]$ over et integritetsområde M betragtes. Vis, at de regulære elementer netop er følgerne $(a_0, a_1, \ldots)$, hvor a_0 er regulær i M.

2) Undersøg kvotientlegemet for potensrækkeringen $M[[X]]$ over et legeme M.

3) Bestem samtlige idealer i potensrækkeringen $M[[X]]$ over et legeme M, og vis, at de kan ordnes i en "nedstigende kæde" $I^{(o)} \supseteq I' \supseteq I'' \supseteq \ldots$; vis, at den er en hovedidealring; angiv (paanær isomorfi i billedet) samtlige homomorfe afbildninger af $M[[X]]$.

4) Bestem samtlige endomorfier, ved hvilke M's elementer er fixe, af polynomiumsringen $M[X]$ over et legeme M, og angiv specielt samtlige automorfier.

5) Bestem samtlige endomorfier, ved hvilke M's elementer er fixe, af potensrækkeringen $M[[X]]$ over et legeme M, og angiv specielt samtlige automorfier.

7) Lad $(M,+,\cdot)$ være en kommutativ ring, i hvilken nulreglen gælder, og med et etelement (altså et integritetsområde), og således, at der eksisterer en funktion $g(x)$ som afbilder M over i de hele, ikke negative tal, og for hvilken

   1) $g(xy) \geq g(x)$ for alle $x,y \in M \wedge y \neq 0$,

   2) for ethvert $d \neq 0$ og ethvert D findes et q så $g(r) = g(D-dq) < g(d)$.

Vis, at $(M,+,\cdot)$ er en hovedidealring. Vis, at den med $=\!=$ understregede forudsætning følger af de øvrige. Opgaven generaliserer beviset på side 4-5 i teksten for $(\acute{Z},+,\cdot)$, idet $g(x) = |x|$ brugbar; vis, at den også generaliserer beviset samme sted for $M[X]$. Idet de nævnte beviser på en måde beror på muligheden af at gennemføre den såkaldte "Euklids algoritme", kalder man ofte en ring, som opfylder opgavens betingelser for en "euklidisk ring", og en sådan er altså altid en hovedidealring.

8) Lad $\acute{Z}[i]$ betegne mængden af komplekse tal $a+bi$, hvor $a,b \in \acute{Z}$. Vis, at $\acute{Z}[i]$ med sædvanlig addition og multiplikation udgør en "euklidisk ring" (se forrige øvelse), idet man som funktion $g(a+bi)$ kan benytte a^2+b^2 (benyt eventuelt en figurbetragtning i den komplekse plan).

Angiv mængden E af regulære elementer i $\acute{Z}[i]$. Undersøg hvilke af tallene 2, 2+i, 3 og 3+i der er reducible. Vis, at afbildningen $a+bi \to a^2+b^2$ er en homomorf afbildning af $(\acute{Z}[i]\setminus\{0\},\cdot)$ ind i $(\acute{N},\cdot)$, og at herved vil et regulært element afbildes i 1, og et reducibelt element afbildes i et sammensat tal; hvad kan man sige om billedet af et irreducibelt element.

Bestem et frembringerelement for det mindste ideal, der indeholder 2 og 3+i.

Vis, at $40049 \cdot 964 = 38607236$ kan skrives som en sum x^2+y^2 af to sædvanlige kvadrattal $(x,y \in \acute{N})$.

9) 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 fællesmul-

tiplumsegenskaben forstår vi: Til to elementer a og b findes altid et m, (kaldet "mindste fælles multiplum for a og b"), så $a|g \wedge b|g \Leftrightarrow m|g$ 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-multiplums-dannelsen.

10) 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.

11) 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. Find samtlige irreducible elementer.

12) Vis, at dersom der for et integritetsområde gælder hovedsætningen om den entydige og altid mulige fremstilling som produkt af irreducible (side 13), så har integritetsområdet både fællesmålsegenskaben og den opstigende kædes egenskab (men det behøver ikke at være en hovedidealring, se øv. 14).

13) Indenfor M[[X]] (M et legeme), betragtes mængden L af potensrækker, hvori $a_1 = 0$. Bestem de irreducible elementer i (L,+,·). Vis, at der findes hovedidealer I_d frembragt af irreducible elementer d, således at nulreglen ikke gælder i faktorringen $(L,+,\cdot)/I_d$. Bestem samtlige idealer i (L,+,·), 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.

14) Vis, at en homomorfi af et integritetsområde (M,+,·) på et integritetsområde $(M^*,+,\cdot)$ kan udvides til en homomorfi af M[X] på $M^*[X]$, ved hvilken $X \in M[X]$ afbildes i $X \in M^*[X]$. De fra 0 forskellige polynomier $a(X) \in Ź[X]$ kan opdeles i ækvivalensklasser $(a(X))'$ af indbyrdes proportionale. Vis,

at dersom a(X) kan skrives som produkt b(X)·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 $(\acute{Z},+,\cdot) \to (\acute{Z}(\text{mod.}p),+,\cdot)$, at hvis alle koefficienterne 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',·) gælder, at ethvert element på en og kun een måde kan skrives som produkt af irreducible (for ækvivalensklasserne fra $\hat{Q}[X]$ er den tilsvarende påstand gyldig ifølge §2).

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 $\acute{Z}[X]$.

Eftervis, at $\acute{Z}[X]$ ikke er en hovedidealring.

15) Vis, at polynomiet $a(X) = (X-1)(X-2)\ldots(X-n) \quad 1$ er irreducibelt indenfor $\acute{Z}[X]$ (og dermed ifølge øv. 1 indenfor $\acute{Q}[X]$).

16) 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.

17. Lad $(M,+,\cdot)$ være et legeme med to elementer, f.eks. legemet af restklasser modulo 2. Undersøg, om $a(X) = X^2 + X + 1$ 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, og nu $a(X) = X^2 + X + 1 \in N[X]$, ønskes de samme spørgsmål besvaret.

18. Bevis, 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).

19. Lad $(M,+,\cdot)$ være en hovedidealring med etelementet e, og lad I være en ideal i ringen; med $\equiv$ betegnes den til I svarende kongruensrelation, d.v.s. at $x \equiv y$ er ensbetydende med at $x-y \in I$. Der defineres en ny relation $\sim$ i mængden M, ved at $x \sim y$ hvis, og kun hvis $x^2 \equiv y^2$. Lad endvidere I_4 betegne det af elementet 4e frembragte hovedideal.
Vis, at $\sim$ er en ækvivalensrelation, og at den er harmonerende med multiplikationen.
Vis, at dersom $\sim$ desuden er harmonerende med additionen, så er $2e \sim 0$ og $I_4 \subseteq I$.
Vis, at mængden K af elementer, hvis kvadrat tilhører I, er et ideal. Vis endelig, at dersom $(M,+,\cdot)$ er ringen af hele tal $(\mathbb{Z},+,\cdot)$, og $I_4 \subseteq I$, så er $\sim$ netop den til idealet K svarende kongruensrelation.

20. 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 $\mathbb{Q}[X]$ er $p(X)$ irreducibel. Hvad kan man sige om $p(X)$ betragtet som element i $\mathbb{Z}[X]$?

Vis, at betragtet som element i potensrækkeringen $\mathbb{Q}[[X]]$ er $p(X)$ regulær.

Undersøg for $a = -2$, $a = 1$ og $a = 5$ om $p(X)$ betragtes som element i $\mathbb{Z}[[X]]$ 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.

21. Lad M være mængden bestående af de rationale tal, der kan 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 de rationale tals ring $(\mathbb{Q},+,\cdot)$.

Bestem samtlige regulære elementer i $(M,+,\cdot)$. Bevis, at $(M,+,\cdot)$ er en hovedidealring med en numerabel mængde af idealer, og angiv idealerne. Angiv sluttelig, hvilke elementer i $(M,+,\cdot)$ der er irreducible, og hvilke der er reducible.

22. Lad $(M,+,\cdot)$ være et integritetsområde, og lad K være mængden af de ikke-regulære elementer i dette. Vis, at K netop er foreningsmængden af alle de fra M forskellige idealer i $(M,+,\cdot)$.

Vis, at dersom K er en delring af $(M,+,\cdot)$, så er K et ideal, og gør rede for at i dette tilfælde er faktorringen $(M,+,\cdot)/K$ et legeme.

Giv eksempel på et integritetsområde, hvori K ikke er noget ideal, og på et integritetsområde, hvori K er et ikke-trivielt ideal.

23. I potensrækkeringen $\mathbb{Z}[[X]]$ over de hele tals integritetsområde skal I betyde det af potensrækken $(2,0,0,\ldots)$ frembragte hovedideal.

Vis, at faktorringen $(M,+,\cdot) = \mathbb{Z}[[X]]/I$ indeholder uendelig mange elementer, og angiv de potensrækker $a = (a_0,a_1,a_2,\ldots) \in \mathbb{Z}[[X]]$ som ved homomorfien med I som kerne afbildes over i regulære elementer i $(M,+,\cdot)$. Vis, at $(M,+,\cdot)$ er et integritetsområde.

Lad $(M_1,+,\cdot)$ være faktorringen $\mathbb{Z}[[X]]/I_1$, hvor I_1 er det af potensrækken $(2,-1,0,0,\ldots) = 2 - X$ frembragte hovedideal.

Det ønskes vist, at $(M,+,\cdot)$ og $(M_1,+,\cdot)$ ikke er isomorfe.