

Om ringe og moduler

1. Nogle grundbegreber.

(1.1). I det følgende betegner R en ring. Her, som overalt i dette kursus, forudsættes, at ringen er *kommutativ*, dvs at multiplikationen er kommutativ: $rs = sr$ for alle elementer r, s i ringen. Videre forudsættes overalt, at ringen har et *et-element*, dvs at der findes et element 1 i ringen, så at $1r = r$ for alle elementer r i ringen. Et-elementet er med andre ord neutralt element for multiplikationen. Ringens *nul-element* er det neutrale element for additionen. Det betegnes 0 , og det er karakteriseret ved $r + 0 = r$. Hvert element r i R har et inverst med hensyn til additionen: det er det *modsatte element*, betegnet $-r$. Det er ikke udelukket, at nul-elementet og et-elementet i R er det samme element. Hvis $0 = 1$, så sluttes imidlertid, at $r = 1r = 0r = 0$; ringen indeholder altså så kun ét element, nemlig nul-elementet, og den kaldes også *nul-ringen* og betegnes 0 .

Et element i R , der har et inverst med hensyn til multiplikationen, siges blot at være et *invertibelt* i R . Et sådant element kaldes også en *enhed* i R . At r er invertibelt i R betyder, at der findes et element r' i R , således at $rr' = 1$. Elementet r' er det *inverse element*, betegnet r^{-1} . De invertible elementer i R udgør, med multiplikation som komposition, en gruppe betegnet R^* .

Et element r i R kaldes *nilpotent*, hvis der findes en eksponent n således at $r^n = 0$, det kaldes *idempotent*, hvis $r^2 = r$, og det kaldes *involutorisk*, hvis $r^2 = 1$.

(1.2) Definition. Et element r i R kaldes en *nuldivisor*, hvis der findes et element $a \neq 0$ i R , således at $ra = 0$, og det kaldes *regulært*, hvis det ikke er en nuldivisor. Bemærk, at der ikke findes nogen nuldivisorer i nul-ringen. I alle andre ringe er nulelementet en nul-divisor. Ringen kaldes et *integritetsområde*, hvis ringen ikke er nul-ringen og den eneste nuldivisor er nul-elementet. Den sidste betingelse kan udtrykkes ved *nul-reglen*: af $ra = 0$ følger at $r = 0$ eller at $a = 0$.

Ringen R kaldes et *legeme*, hvis R ikke er nul-ringen og hvis alle elementer forskellige fra 0 er invertible i R . Bemærk, at et legeme er et integritetsområde. Af en ligning $ra = 0$, hvor $r \neq 0$, fås nemlig ved multiplikation med r^{-1} at $a = 0$.

Ringene \mathbb{Z} af hele tal er et integritetsområde. Ringene \mathbb{Q} , \mathbb{R} og \mathbb{C} af henholdsvis rationale, reelle og komplekse tal er legemer.

(1.3) Karakteristik. Lad 1 være et-elementet i R . Det er ikke udelukket, at der findes naturlige tal n således at

$$\underbrace{1 + \dots + 1}_n = 0. \quad (1.3.1)$$

Hvis der findes sådanne tal n , så kaldes det mindste af disse også for ringens *karakteristik*. Alle tal n , for hvilke (1.3.1) er opfyldt, vil så være multipla af karakteristikkens. Hvis ligningen (1.3.1) ikke er opfyldt for noget tal n , siges ringen at have karakteristik 0.

(1.4) Ringhomomorfi. En afbildning $\theta: S \rightarrow R$ mellem ringe kaldes en (*ring-*)*homomorfi*, hvis θ bevarer addition og multiplikation og afbilder et-elementet i S over i et-elementet i R . Betingelserne kan udtrykkes ved ligningerne $\varphi(s + t) = \varphi(s) + \varphi(t)$, $\varphi(st) = \varphi(s)\varphi(t)$ og $\varphi(1) = 1$. Homomorfin kaldes en *isomorfi*, hvis den er bijektiv.

En delmængde R' af R , som er stabil under addition og multiplikation, og som selv er en ring med samme et-element som R , kaldes en *delring* af R . Bemærk, at den sidste betingelse er nødvendig for at sikre, at inklusionsafbildningen $s \mapsto s$ er en ringhomomorfi $R' \rightarrow R$.

(1.5) Ideal. En delmængde \mathfrak{a} af R kaldes et *ideal*, hvis \mathfrak{a} er en undergruppe i ringens additive gruppe og \mathfrak{a} desuden er stabil med hensyn til multiplikation med et vilkårligt element fra R . Den sidste betingelse betyder, at der for alle elementer a i \mathfrak{a} og r i R gælder, at produktet ra tilhører \mathfrak{a} .

De *trivielle idealer* er delmængderne $\{0\}$ og R . Idealer, der er forskellige fra R , kaldes også *ægte idealer*. Bemærk, at et ideal \mathfrak{a} i R er et ægte ideal, hvis og kun hvis et-elementet 1 ikke tilhører \mathfrak{a} . Er nemlig $1 \in \mathfrak{a}$, så følger for hvert element r i R , at $r = r1 \in \mathfrak{a}$.

Et ideal \mathfrak{a} kaldes et *hovedideal*, hvis der i \mathfrak{a} findes et element a , således at \mathfrak{a} består af alle *multipla* af a , dvs $\mathfrak{a} = Ra = \{ra \mid r \in R\}$. Idealet siges da at være frembragt af a , og det betegnes også (a) . Ringen kaldes en *hovedidealring*, hvis alle idealer er hovedideal, og et *hovedidealområde* (eller et *PID*), hvis den desuden er et integritetsområde.

De trivielle idealer er hovedideal: hovedidealet (0) består kun af nul-elementet, og hovedidealet (1) består af alle elementer i R . Bemærk videre, at hovedidealet (a) er et ægte ideal, hvis og kun hvis a ikke er et invertibelt element. Er nemlig $(a) = R$, så er specielt 1 element i (a) . Følgelig er $1 = sa$, hvor $s \in R$, og så er a invertibel. Antag omvendt, at a er invertibel, altså at der findes s i R så at $sa = 1$. Da gælder for hvert element r , at $r = rsa$ tilhører (a) .

(1.6) Faktorielle ringe. Antag, at R er et integritetsområde. Et element p i R , som ikke er 0 og ikke er en enhed, kaldes *irreducibelt*, hvis det kun på triviell måde kan skrives som et produkt $p = rs$. Det kaldes et *primelement*, hvis det opfylder følgende: hvis p går op i et produkt rs , så går p op i en af faktorerne r og s . Det er let at vise, at et primelement er irreducibelt.

Ringens R siges at være *faktoriel* (eller et *UFD*), hvis hvert element i R , der ikke er 0 og ikke er en enhed, kan skrives som produkt af primelementer. Ækvivalent er betingelsen, at hvert element, som ikke er 0 og ikke er en enhed, entydigt kan skrives som produkt af irreducible elementer. En faktoriel ring siges også at være en ring med *entydig primopløsning*. Det er velkendt, at et hovedidealområde er en faktoriel ring („Et PID er et UFD“). To elementer i en faktoriel ring kaldes *primiske*, hvis deres fælles divisorer kun er enhederne.

(1.7) Idealoperationerne. Lad \mathfrak{a} og \mathfrak{b} være idealer i R . Det er klart, at fællesmængden $\mathfrak{a} \cap \mathfrak{b}$ igen er et ideal. Ved *summen* $\mathfrak{a} + \mathfrak{b}$ forstås idealet bestående af summer $a + b$, hvor $a \in \mathfrak{a}$ og $b \in \mathfrak{b}$. Ved *produktet* $\mathfrak{a}\mathfrak{b}$ forstås idealet bestående af alle endelige summer af produkter ab ,

hvor $a \in \mathfrak{a}$ og $b \in \mathfrak{b}$. Ved *radikalet* $\text{Rad } \mathfrak{a}$ forstås idealet bestående af de elementer r i R , der har en potens r^n , som tilhører \mathfrak{a} .

Bemærk, at produktet $\mathfrak{a}\mathfrak{b}$ er indeholdt i fællesmængden $\mathfrak{a} \cap \mathfrak{b}$. Bemærk videre, at radikalet $\text{Rad}(0)$ af det trivielle ideal (0) består af de nilpotente elementer i R .

(1.8) Kvotientring. Til hvert ideal \mathfrak{a} i R hører som bekendt en kongruensrelation: To elementer r og r' er *kongruente modulo* \mathfrak{a} , hvis differensen $r' - r$ tilhører \mathfrak{a} . Kongruens modulo \mathfrak{a} er en ækvivalensrelation, og ækvivalensklasserne kaldes også *restklasser* (eller *sideklasser*). Den tilhørende *kvotientring*, dvs mængden af restklasser, betegnes R/\mathfrak{a} . Restklasser komponeres ved regning med *repræsentanter*.

Ringhomomorfien $R \rightarrow R/\mathfrak{a}$, der afbilder et element r i R over i den ækvivalensklasse, der indeholder r , kaldes den *kanoniske* homomorfi, og den betegnes $r \mapsto \hat{r}$.

Lad $\theta: R \rightarrow S$ være en ringhomomorfi. Da udsiger *Isomorfisætning for ringe* som bekendt følgende: *Kernen for* θ , dvs *originalmængden* $\theta^{-1}(0)$, er et ideal i R , billedet $\theta(R)$ er en delring af S , og θ inducerer en naturlig isomorfi fra kvotientringen $R/\theta^{-1}(0)$ på billedringen $\theta(R)$.

(1.9) Polynomiumsringen. Med $R[X]$ betegnes ringen af *polynomier* med koefficienter i R . Elementerne i $R[X]$ er endelige summer,

$$f = r_0 + r_1X + \cdots + r_nX^n.$$

Hvis polynomiet ikke er *nul-polynomiet*, dvs hvis et af r_i 'erne er forskelligt fra 0, defineres polynomiets *grad* som det største i for hvilket $r_i \neq 0$. Den tilsvarende koefficient r_i kaldes *højstegradskoefficienten* eller den *ledende koefficient*. Hvis den er lig med 1, siges polynomiet at være et *normeret polynomium* (eller et *monisk polynomium*). Når nul-polynomiet tillægges en grad, forudsættes altid, at denne grad er mindre end alle andre grader, og specielt, at denne grad er mindre end 0. Graden af et polynomium f betegnes $\deg(f)$. Polynomierne af grad mindre end eller lig med 0 kaldes *konstante polynomier*. De udgør i $R[X]$ en delring, der er isomorf med R .

Ved multiplikation af polynomier multipliceres specielt højstegradskoefficienterne. Det ses specielt, at *hvis* R er et *integritetsområde*, så er også *polynomiumsringen* $R[X]$ et *integritetsområde*, og *graden af et produkt er summen af graderne*.

(1.10) Division med rest. Lad der i $R[X]$ være givet et normeret polynomium d af grad n . Sætningen om *division med rest* udsiger da, at hvert polynomium f har en entydig fremstilling,

$$f = qd + r,$$

hvor polynomiet r er af lavere grad end d , dvs af grad højst $n - 1$.

Polynomier af formen qd udgør hovedidealet (d) . Alternativt udtrykker sætningen derfor, at hvert polynomium f modulo (d) er kongruent med et entydigt bestemt polynomium af formen,

$$r_0 + r_1X + \cdots + r_{n-1}X^{n-1}.$$

Elementerne i kvotientringen $R[X]/(d)$ er restklasser \hat{f} af polynomier f . Sættes $\xi := \hat{X}$, er sætningen ækvivalent med følgende resultat: *Hver restklasse i $R[X]/(d)$ har en fremstilling,*

$$r_0 + r_1\xi + \cdots + r_{n-1}\xi^{n-1},$$

hvor r_i 'erne er entydigt bestemte elementer i R .

(1.11) Rødder. Et element a i R siges at være *rod* i polynomiet f , hvis $f(a) = 0$. For et givet element a i R kan sætningen om division med rest anvendes på førstegradspolynomiet $X - a$. Som resultat fås en fremstilling, $f = q(X - a) + r$, hvor graden af restpolynomiet r er mindre end 1. Restpolynomiet r er altså et konstant polynomium. Ved indsættelse af a ses, at konstanten er $f(a)$. Fremstillingen har altså formen,

$$f = q(X - a) + f(a).$$

Specielt aflæses heraf, at a er rod i f , hvis og kun hvis f er delelig med førstegradspolynomiet $X - a$.

Hvis polynomiet q har en rod kan processen gentages. Det er let herved at indse følgende: *Hvis R er et integritetsområde, så har hvert polynomium $f \neq 0$ en entydig fremstilling af formen,*

$$f = q(X - a_1)^{n_1} \cdots (X - a_r)^{n_r}, \quad (1.11.1)$$

hvor q er et polynomium uden rødder i R .

(1.12). Det er velkendt, at polynomiumsringen $k[X]$, med koefficienter i et legeme k , er et hovedidealområde. Specielt er $k[X]$ en faktoriel ring. Ethvert ikke-konstant polynomium kan altså skrives entydigt som produkt af irreducible polynomier. Enhederne er de konstante polynomier forskellige fra 0, og ofte antages (implicit), at irreducible polynomier er normerede.

Legemet k siges at være et *algebraisk afsluttet legeme*, hvis hvert ikke-konstant polynomium i $k[X]$ har en rod i k . En ækvivalent betingelse er, at de irreducible polynomier (på nær multiplikation med en konstant) netop er førstegradspolynomierne $X - a$ for $a \in k$ (dette følger fx ved at betragte fremstillingen (1.11.1)). Yderligere gælder følgende resultat:

Antag, at k er et algebraisk afsluttet legeme. Lad K være et legeme, som indeholder k , og antag at K er af endelig dimension som vektorrum over k . Da er $k = K$.

Bevis. Lad α være et element i K . Det skal vises, at α tilhører k . Betragt hertil potenserne $1, \alpha, \alpha^2, \dots$ i K . Da K er af endelig dimension over k , findes blandt disse uendelig mange potenser en ikke-triviel lineær relation, dvs en ligning af formen $a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$, hvor $a_i \in k$ og ikke alle a_i er lig med nul. Elementet α er med andre ord rod i et ikke-trivielt polynomium f i $k[X]$. Skriv nu f som produkt af irreducible polynomier, $f = p_1 \cdots p_r$. Ved indsættelse af α fås ligningen $0 = f(\alpha) = p_1(\alpha) \cdots p_r(\alpha)$. Da K er et legeme, og specielt et integritetsområde, følger det af ligningen, at en af faktorerne $p_i(\alpha)$ er lig med 0. Elementet α er således rod i et (normeret) irreducibelt polynomium. Da k er algebraisk afsluttet, er dette irreducible polynomium af formen $X - a$, hvor $a \in k$. At α er rod i $X - a$ betyder, at $\alpha = a$. Altså er α element i k , som ønsket. \square

30. marts 2007

(1.13) Algebraens fundamentalsætning. udsiger, at legemet \mathbb{C} af komplekse tal er et algebraisk afsluttet legeme. De irreducible (normerede) polynomier i $\mathbb{C}[X]$ er altså netop førstegradspolynomierne $X - a$ for $a \in \mathbb{C}$. Som konsekvens fås følgende resultat om ringen af polynomier $\mathbb{R}[X]$ med reelle koefficienter:

De irreducible (normerede) polynomier i $\mathbb{R}[X]$ er netop polynomierne $X - a$ for $a \in \mathbb{R}$ og andengradspolynomierne uden (reelle) rødder, dvs polynomierne af formen $(X - a)^2 + b^2$, hvor $b \neq 0$.

Bevis. Antag nemlig, at f er et irreducibelt (normeret) polynomium i $\mathbb{R}[X]$. Hvis f har en reel rod a , så er f delelig med $X - a$, jfr (1.11), og følgelig er $f = X - a$, da f er irreducibel. Antag derfor, at f ikke har reelle rødder. Da har f en kompleks rod α , og med α er også det komplekst konjugerede tal $\bar{\alpha}$ rod i f . Disse tal er forskellige, så inden for $\mathbb{C}[X]$ er f delelig med produktet $p = (X - \alpha)(X - \bar{\alpha})$. Polynomiet p har reelle koefficienter, og er af den ønskede form. I ringen $\mathbb{C}[X]$ går p op i f ; det følger så, fx af Sætningen om division med rest, at p også i ringen $\mathbb{R}[X]$ går op i f . Da f er irreducibelt, følger det endeligt at $f = p$, som ønsket. \square

Yderligere fås følgende resultat: *Lad K være et legeme, som indeholder \mathbb{R} , og antag at K har endelig dimension som vektorrum over \mathbb{R} . Da er enten $K = \mathbb{R}$ eller K er isomorf med \mathbb{C}*

Bevis. Antag, at $\mathbb{R} \subset K$, og betragt et element α i overskudsmængden. Som i (1.12) indses, at α er rod i et irreducibelt polynomium p i $\mathbb{R}[X]$. Da $\alpha \notin \mathbb{R}$, kan p ikke være et førstegrads-polynomium. Af det foregående resultat følger derfor, at p er et andengrads-polynomium $p = (X - a)^2 + b^2$, hvor a, b er reelle og $b \neq 0$. Sæt nu $j := (\alpha - a)/b$. Af ligningen $p(\alpha) = 0$ følger da, at $j^2 + 1 = 0$. Det er herefter klart, at elementerne i K af formen $x + yj$, hvor $x, y \in \mathbb{R}$, udgør et med \mathbb{C} isomorft dellegeme af K . Af resultatet i (1.12), anvendt for $k = \mathbb{C}$, følger nu, at K er lig med dette dellegeme. Hermed er resultatet bevist. \square

(1.14) Flere variable. Polynomiumsringen $R[X_1, \dots, X_n]$ i n variable defineres ganske som for én variabel. Elementerne i $R[X_1, \dots, X_n]$ er endelige summer,

$$F = \sum_{i_1, \dots, i_n} r_{i_1, \dots, i_n} X_1^{i_1} \cdots X_n^{i_n}, \quad (1.14.1)$$

altså en sum af endelige mange led af formen $r X_1^{i_1} \cdots X_n^{i_n}$. De specielle polynomier af formen $X_1^{i_1} \cdots X_n^{i_n}$ kaldes *monomier*, og summen $i_1 + \cdots + i_n$ er monomiets grad. Monomiet $X_1^{i_1} \cdots X_n^{i_n}$ siges at *forekomme* i polynomiet F , hvis den tilhørende koefficient r_{i_1, \dots, i_n} er forskellig fra 0. Hvis F ikke er nul-polynomiet, defineres *graden* af F som den største grad af et monomium, der forekommer i F .

Et polynomium H kaldes *homogent*, hvis alle monomier, der forekommer i H , har samme grad. Ethvert polynomium F kan fremstilles som en sum af *homogene led* F_h : Leddet F_h er summen af de led $r_{i_1, \dots, i_n} X_1^{i_1} \cdots X_n^{i_n}$, der har graden h .

Et polynomium F kan „ordnes“ efter en af de variable, fx efter X_n : Hermed menes, at man omordner summen (1.14.1) således:

$$F = \sum_i \left(\sum_{i_1, \dots, i_{n-1}} r_{i_1, \dots, i_{n-1}, i} X_1^{i_1} \cdots X_{n-1}^{i_{n-1}} \right) X_n^i$$

den indre sum, for en fastværdi af $i = 0, 1, \dots$, har formen $f_i X_n^i$, så via omformningen bliver F et polynomium i den ene variable X_n , med koefficienter f_i , der er polynomier i de resterende variable X_1, \dots, X_{n-1} . Specielt fås følgende induktive definition af polynomier:

$$R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}][X_n]. \quad (1.14.2)$$

Gauss' Sætning udsiger, at hvis R er en faktoriel ring, så er også polynomiumsringen $R[X]$ en faktoriel ring. Ved induktion følger så, at når R er faktoriel, så er også polynomiumsringen $R[X_1, \dots, X_n]$ i n variable en faktoriel ring. Specielt følger det ved induktion, at polynomiumsringen $k[X_1, \dots, X_n]$ med koefficienter i et legeme k er en faktoriel ring. [Induktionsstarten er her, at polynomiumsringen $k[X]$ er faktoriel, jfr (1.12).]

Over en faktoriel ring R kan man, også i flere variable via (1.14.2), bruge

Eisenstein's Irreducibilitetskriterium. Antag om $f = a_0 X^n + a_1 X^{n-1} + \dots + a_n \in R[X]$, at f er primitivt (dvs intet primelement fra R går op i alle a_i) og at der findes et primelement $p \in R$ således, at $p \mid a_i$ for $i = 1, \dots, n$ og $p^2 \nmid a_n$. Da er f irreducibel i $R[X]$.

(1.15) Moduler. Ved en *modul* M over ringen R (også kaldet en *R-modul*) forstås en kommutativ (additivt skrevet) gruppe M , i hvilken der yderligere er givet en *multiplikation med elementer fra R*, dvs en afbildning $R \times M \rightarrow M$ betegnet $(r, x) \mapsto rx$, som opfylder de linearitetskrav, der kendes fra vektorrum. Disse krav er følgende, for elementer $r, s \in R$ og $x, y \in M$:

$$r(x + y) = rx + ry, \quad (r + s)x = rx + sx, \quad (rs)x = r(sx), \quad 1x = x.$$

I denne forbindelse kaldes elementerne i ringen ofte *skalarer*. Modulen, der har netop ét element, kaldes *nul-modulen*, og den betegnes 0 .

For moduler kan det af og til være bekvemt at bruge en udførlig notation af formen $(M, +, R)$, som indikerer navnet, additionen, og multiplikationen med skalarer fra R .

(1.16) Eksempler. Moduler over et legeme er blot vektorrum over dette legeme; specielt er moduler over \mathbb{C} (eller \mathbb{R}) er blot komplekse (eller reelle) vektorrum.

Moduler over \mathbb{Z} er blot kommutative grupper i den forstand, er der for en givet kommutativ gruppe M er en entydig måde hvorpå man kan definere multiplikation med skalarer fra \mathbb{Z} : Er der nemlig givet en sådan multiplikation, så følger af den den anden og den sidste ligning ovenfor, for $n \in \mathbb{Z}$, $n \geq 1$, at

$$nx = \overbrace{(1 + \dots + 1)}^n x = \overbrace{(x + \dots + x)}^n;$$

multiplikationen af x med n er altså den n 'te (additive) potens af x i gruppen M . Heraf følger let, at også multiplikation med negative tal er bestemt ved den additive potens. Omvendt følger det af de tre potensregler, for en given kommutativ gruppe M , at med additiv potens som multiplikation med skalarer er M en \mathbb{Z} -modul.

For en vilkårlig givet ring R er det mest oplagte eksempel på en R -modul mængden R^n af søjler af n -sæt med koefficienter i R . Additionen og multiplikation med skalarer fra R

30. marts 2007

er koordinatvise. For $n = 1$ fås specielt ringen R opfattet som modul over sig selv. Hvis M_1, \dots, M_n er givne R -moduler, defineres mere generelt den *direkte sum*,

$$M_1 \oplus \cdots \oplus M_n,$$

som mængden af alle søjler af n -sæt $x = (x_1, \dots, x_n)^{\text{tr}}$, hvor $x_i \in M_i$. Addition og multiplikation med skalarer fra R defineres koordinatvis.

(1.17) Definition. En afbildning $\varphi: M \rightarrow N$ mellem moduler kaldes en (*modul-*) *homomorfi* eller en *R -lineær* afbildning, hvis den bevarer addition og multiplikation med skalar. Betingelsen kan udtrykkes ved ligningerne $\varphi(x + y) = \varphi(x) + \varphi(y)$ og $\varphi(rx) = r\varphi(x)$. Homomorfien kaldes en *isomorfi*, hvis den er bijektiv.

En modul M siges at være *endeligt frembragt*, hvis der i M findes endelig mange elementer e_1, \dots, e_n således, at hvert element x i M kan skrives som en *linearkombination*,

$$x = r_1 e_1 + \cdots + r_n e_n,$$

hvor r_i 'erne tilhører R . Hvis sådanne fremstillinger er entydige, siges modulen M at være en *fri modul*, og sættet e_1, \dots, e_n kaldes en *basis* for modulen. Det er let at se, at M er endeligt frembragt, hvis og kun hvis der findes en surjektiv homomorfi $R^n \rightarrow M$, og at M er fri, hvis og kun hvis der findes en isomorfi $R^n \rightarrow M$.

(1.18) Undermodul. Lad M være en R -modul. En *undermodul* N er da en delmængde N af M , som er stabil over for addition og multiplikation med skalarer fra R , og indeholder modulens nul-element. De *trivielle undermoduler* er hele M og undermodulen bestående alene af nul-elementet i M ; den sidste undermodul betegnes 0 eller (0) .

For givne elementer x_1, \dots, x_m i M udgør mængden af alle linearkombinationer,

$$Rx_1 + \cdots + Rx_m = \{r_1 x_1 + \cdots + r_n x_n \mid r_1, \dots, r_n \in R\},$$

en undermodul; det er undermodulen *frembragt* af x_1, \dots, x_n .

Bemærk, at i modulen R er undermodulerne netop idealerne i ringen R . Idealet frembragt af endelig mange elementer $a_1, \dots, a_n \in R$ betegnes næsten altid (a_1, \dots, a_n) .

Lad N og P være undermoduler i R -modulen M . Det er klart, at fællesmængden $N \cap P$ igen er en undermodul. Ved *summen* $N + P$ forstås undermodulen bestående af summer $n + p$, hvor $n \in N$ og $p \in P$. Lad \mathfrak{a} være et ideal i R . Ved *produktet* $\mathfrak{a}N$ forstås undermodulen bestående af alle endelige summer af produkter an , hvor $a \in \mathfrak{a}$ og $n \in N$. Hvis idealet er et hovedideal (a) , så er produktet lig med undermodulen $aN = \{an \mid n \in N\}$.

(1.19) Kvotientmodul. Til hver undermodul N i M hører en *kvotientmodul* M/N : Elementerne i M/N er *restklasser* (eller *sideklasser*) *modulo* N , dvs ækvivalensklasser svarende til følgende ækvivalensrelation:

$$x \equiv x' \stackrel{\text{DEF}}{\iff} x' - x \in N.$$

Relationen kaldes også *kongruens modulo N* . Klassen, der indeholder x , er delmængden $x + N = \{x + n \mid n \in N\}$. Når denne klasse opfattes som element i M/N betegnes den \bar{x} , og x siges at være en *repræsentant* for klassen. Kvotienten, dvs mængden af restklasser modulo N , organiseres som R -modul ved regning med repræsentanter: Lad U og V være klasser, og vælg repræsentanter, u for U og v for V . Summen $U + V$ er da klassen, der indeholder $u + v$, og produktet rU (for $r \in R$) er klassen, der indeholder produktet ru . Det følger umiddelbart af disse definitioner, at der for alle x, y i M og r i R gælder,

$$\bar{x} + \bar{y} = \overline{x+y}, \quad r\bar{x} = \overline{rx}.$$

Afbildningen $x \mapsto \bar{x}$ er altså en homomorfi $M \rightarrow M/N$, kaldet den *kanoniske homomorfi*.

Isomorfiætning for moduler. Lad $\varphi: M \rightarrow N$ være en modulhomomorfi. Da gælder: Kernen for φ , dvs originalmængden $\varphi^{-1}(0)$, er en undermodul i M , og billedet φM er en undermodul i N . Videre bestemmes ved

$$\bar{x} \mapsto \varphi(x)$$

en veldefineret isomorfi fra kvotientmodulen $M/\varphi^{-1}(0)$ på billedmodulen φM .

Bevis. Det vides allerede, fra Isomorfiætning for grupper, at forskriften bestemmer en veldefineret isomorfi fra kvotientgruppen til billedgruppen. Det skal altså blot tilføjes, at denne isomorfi også bevarer multiplikation med skalarer. Og det følger af, at φ er lineær. \square

(1.20) Annullator og nuldivisor; cyklisk modul. Lad x være et element i modulen M . Ved $r \mapsto rx$ defineres da en homomorfi $R \rightarrow M$. Kernen for denne homomorfi er en undermodul i R , altså et ideal. Dette ideal består af de skalarer r , som *annullerer* x , dvs opfylder, at $rx = 0$, og det kaldes også *annullatoren* for elementet x , og det betegnes $\text{Ann}(x)$.

Hvis ligningen $rx = 0$ er opfyldt med $x \neq 0$, kaldes r en nuldivisor på M . Mængden af nuldivisorer, betegnet $Z_R(M)$, er altså foreningsmængden af annullatorerne $\text{Ann}(x)$ for alle $x \neq 0$. De elementer i R , der ikke er nuldivisorer på M , siges også at være *regulære* på M . Er ligningen $rx = 0$ opfyldt med en skalar r , som ikke er nuldivisor i R , kaldes x et *torsionselement*.

De skalarer, der annullerer alle elementer i M , udgør et ideal i R , kaldet modulens *annullator*, og betegnet $\text{Ann } M$.

Billedet ved homomorfien $r \mapsto rx$ består af elementerne i M af formen rx for $r \in R$, og det betegnes også Rx . Isomorfiætningen er her en isomorfi,

$$R/\text{Ann}(x) \xrightarrow{\sim} Rx.$$

Modulen M kaldes *cyklisk*, hvis der i M findes et element e således, at $M = Re$. Det fremgår af det foregående, at M er cyklisk, hvis og kun hvis M er isomorf med en kvotientmodul R/I af R modulo et ideal.

(1.21) Struktursætning for endeligt frembragte moduler over et PID. Hvis R er et hovedidealområde (et PID), så gælder, at enhver endelig frembragt R -modul M er en direkte sum af cykliske moduler. Der findes med andre ord en isomorfi af R -moduler,

$$M \simeq R/\mathfrak{a}_1 \oplus \cdots \oplus R/\mathfrak{a}_n,$$

hvor \mathfrak{a}_i 'erne er (hoved-)idealer i R .

For $R = \mathbb{Z}$ og en endelig kommutativ gruppe M som modulen, er resultatet blot den velkendte Struktursætning for endelige kommutative gruppe. Vi viser ikke det generelle resultat.

(1.22) Determinant. For en (kvadratisk) $(n \times n)$ -matrix $\alpha = (\alpha_{ij})$ med koefficienter α_{ij} i R betegnes med α_j den j 'te søjle og med ${}_i\alpha$ den i 'te række i α . Videre defineres *determinanten* af α ved udtrykket,

$$\det \alpha = \sum_{\sigma \in S_n} \text{sign}(\sigma) \alpha_{\sigma_1,1} \cdots \alpha_{\sigma_n,n}, \quad (1.22.1)$$

hvor der summeres over alle permutationer $\sigma = (\sigma_1, \dots, \sigma_n)$ i den symmetriske gruppe S_n . Der er $n!$ led i summen, og hvert led består ud over et fortegn af et produkt af n af matrixens elementer udvalgt ved hjælp af permutationen σ med ét element fra hver søjle og ét fra hver række.

Det er let ud fra definitionen at vise de simple regler: Determinanten er alternerende som funktion af søjlerne, dvs R -lineær som funktion af den k 'te søjle (når de øvrige søjler fastholdes) og lig med 0 når to søjler er ens. Det er en konsekvens, at når matrixens søjler permuteres, så multipliceres determinanten med permutationens fortegn. Desuden ændres determinanten ikke, hvis matrixen transponeres. Heraf følger videre, at determinanten også er alternerende som funktion af rækkerne.

Endelig er *determinanten multiplikativ*: Er β endnu en $(n \times n)$ -matrix, så er $\det(\beta\alpha) = \det(\beta)\det(\alpha)$. Mere generelt betragtes R -moduler M og N og en alternerende afbildning $\Psi: M^n \rightarrow N$. Betragt to sæt $u = (u_1, \dots, u_n)$ og $v = (v_1, \dots, v_n)$ af n elementer i M . Antag, at elementerne v_i i det andet sæt er bestemt som linearkombinationer af elementerne u_1, \dots, u_n i det første sæt; det svarer til en matrixligning,

$$(v_1, \dots, v_n) = (u_1, \dots, u_n)\alpha, \quad (\text{eller kort: } v = u\alpha)$$

som udtrykker, at den i 'te koordinat v_i på venstresiden er det produkt, der fås ved på højresiden at gange rækken (u_1, \dots, u_n) med den i 'te søjle i α . Med denne antagelse gælder, at

$$\Psi(u\alpha) = \det(\alpha)\Psi(u). \quad (1.22.2)$$

Udregningen er umiddelbar: Med $v = u\alpha$ har vi $v_i = \sum_{\sigma_i=1}^n \alpha_{\sigma_i,i} u_{\sigma_i}$, hvor vi har ladet navnet på summationsindex afhænge af i . Da Ψ er lineær i hver variabel, følger det, at

$$\Psi(u\alpha) = \sum_{\sigma_1=1}^n \cdots \sum_{\sigma_n=1}^n \alpha_{\sigma_1,1} \cdots \alpha_{\sigma_n,n} \Psi(u_{\sigma_1}, \dots, u_{\sigma_n}). \quad (*)$$

De mulige sæt af indices $(\sigma_1, \dots, \sigma_n)$ svarer til afbildningerne $\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$, så summen i (*) er over alle sådanne afbildninger. Da ψ er alternerende, er leddet på højresiden 0, hvis to argumenter er ens. Det er derfor nok at summere over de afbildninger σ , der er injektive (og dermed bijektive), dvs over permutationerne $\sigma \in S_n$. For en permutation σ har vi, da Ψ er alternerende, at $\Psi(u_{\sigma_1}, \dots, u_{\sigma_n}) = \text{sign}(\sigma)\Psi(u_1, \dots, u_n)$. Udtrykket i (*) reduceres altså til følgende:

$$\Psi(u\alpha) = \sum_{\sigma \in S_n} \text{sign}(\sigma) \alpha_{\sigma_1 1} \cdots \alpha_{\sigma_n n} \Psi(u);$$

det er, ifølge definitionen af determinanten, den ønskede formel (1.22.2). Formlen for determinanten af et matrixprodukt, i formen $\det(\beta\alpha) = \det(\alpha) \det(\beta)$, følger af (1.22.2) ved at bemærke, at i matrixproduktet $\gamma = \beta\alpha$ er den i 'te søjle i γ præcis den linearkombination af søjlerne i β , hvis koefficienter er den i 'te søjle i α . Ligningen $\gamma = \beta\alpha$ svarer altså til $v = u\alpha$, med $v = \gamma$ og $u = \beta$.

(1.23) Cramer's formler. Betragt nu for en given matrix α den matrix, der fås ved at erstatte den k 'te søjle i α med en søjle x . Determinanten af denne matrix *udvikles efter den k 'te søjle*. Det betyder følgende: I hvert led i summen i (1.22.1) er den k 'te faktor efter fortegnet et element fra matrixens k 'te søjle. For den betragtede matrix er den k 'te faktor altså en af koordinaterne x_j i x . Nu samles i summen alle led, hvor den k 'te faktor er x_1 (og x_1 sættes uden for parentes), dernæst samles alle led hvor den k 'te faktor er x_2 (og x_2 sættes uden for parentes), osv. Herved fremkommer et udtryk for determinanten, der øjensynlig har formen,

$$\det(\alpha_1, \dots, x, \dots, \alpha_n) = \tilde{\alpha}_{k1}x_1 + \cdots + \tilde{\alpha}_{kn}x_n, \quad (1.23.1)$$

hvor faktorerne $\tilde{\alpha}_{kj}$ kun afhænger af matrixen α og ikke af søjlen x . Følgelig kan $\tilde{\alpha}_{kj}$ bestemmes ved i udtrykket (1.23.1) at indsætte den søjle x , der har 1 på den j 'te plads og 0 på de øvrige pladser. Det følger, at $\tilde{\alpha}_{kj}$ er determinanten af den matrix, der fås fra α ved at erstatte elementet på plads jk med 1 og erstatte de øvrige elementer i den k 'te søjle med 0. Determinanten af denne sidste matrix ændres øjensynlig ikke, hvis man yderligere erstatter de øvrige elementer i j 'te række med 0.

Elementet $\tilde{\alpha}_{kj}$ er uafhængigt af elementerne i den k 'te søjle og den j 'te række. Derfor giver et tilsvarende argument *udvikling efter l 'te række*:

$$\det({}_1\alpha, \dots, x^{\text{tr}}, \dots, {}_n\alpha)^{\text{tr}} = x_1\tilde{\alpha}_{1l} + \cdots + x_n\tilde{\alpha}_{nl}, \quad (1.23.2)$$

med den *samme* matrix af koefficienter $\tilde{\alpha}_{ij}$.

Matrixen $\tilde{\alpha} = \tilde{\alpha}_{ij}$ kaldtes klassisk den *adjungerede* til matrixen α ; vi vil oftest kalde den for *kofaktormatrixen* for α . Definitionen indeholder en slags „transponering“: Kofaktoren $\tilde{\alpha}_{ij}$ er determinanten af den matrix, der fås ved at erstatte α_{ji} med 1 og de øvrige elementer i j 'te række og i 'te søjle med 0. Sammenlignet med determinanten af den $(n-1) \times (n-1)$ -matrix, der fås fra α ved at fjerne j 'te række og i 'te søjle, er der også „indbygget“ et fortegn i $\tilde{\alpha}_{ij}$.

Bemærk, at højresiderne i formlerne (1.23.1) og (1.23.2) kan udtrykkes ved rækker og søjler i matricen $\tilde{\alpha}$ som, henholdsvis, produkterne ${}_k\tilde{\alpha}x$ og $x^{\text{tr}}\tilde{\alpha}_l$. Formlerne kan altså bruges til at beregne matrixprodukterne $\tilde{\alpha}x$ og $x^{\text{tr}}\tilde{\alpha}$. Specielt, ved at anvende formlerne, når x og x^{tr} er søjler og rækker i matricen α , udledes *Cramer's formler*:

$$\tilde{\alpha}\alpha = \alpha\tilde{\alpha} = \det(\alpha)1_n,$$

hvor 1_n er enhedsmatricen i $\text{Mat}_n(R)$.

(1.24) Algebra. Ved en *generel algebra* over R forstås en R -modul A , i hvilken der er givet en multiplikation $(x, y) \mapsto x * y$, som er R -lineær i hver variabel. Af lineariteten følger specielt at multiplikationen er additiv i hver variabel, dvs at den *distributive lov* gælder.

Specielle krav til multiplikationen giver specielle klasser af algebraer. Fx fastlægges en *Lie-algebra* ved følgende krav:

$$x * x = 0, \quad x * (y * z) + y * (z * x) + z * (x * y) = 0 \quad x, y, z \in A.$$

En *associativ algebra med et-element* fastlægges ved følgende krav:

$$x * (y * z) = (x * y) * z, \quad 1_A * x = x * 1_A, \quad x, y, z \in A$$

hvor 1_A er algebraens et-element. Vi betragter udelukkende sådanne associative algebraer med et-element, og vi reserverer betegnelsen R -algebra for denne type. I en R -algebra A er der altså tre operationer: En addition $(x, y) \mapsto x + y$ som gør $(A, +)$ til en kommutativ gruppe, en multiplikation med skalarer fra R , $(r, x) \mapsto rx$, som gør $(A, +, R)$ til en R -modul, og en multiplikation $(x, y) \mapsto x * y$, som gør $(A, +, *)$ til en ring. Det kræves yderligere, at multiplikation i ringen A og multiplikation med skalarer fra R *harmonerer* i den forstand at

$$r(x * y) = (rx) * y = x * (ry).$$

Sædvanligvis skrives blot xy for $x * y$.

(1.25) Opgaver.

- U1 1. Betragt i ringen \mathbb{Z} (hoved)idealene $\mathfrak{a} = (24)$ og $\mathfrak{b} = (32)$. Bestem summen $\mathfrak{a} + \mathfrak{b}$, produktet $\mathfrak{a}\mathfrak{b}$, og radikalerne $\text{Rad}(\mathfrak{a})$ og $\text{Rad}(\mathfrak{b})$.
- U1 2. Vis, at antallet af monomier $X_1^{i_1} \cdots X_n^{i_n}$ af grad d i $R[X_1, \dots, X_n]$ er bestemt ved binomialkoefficienten $\binom{n+d-1}{n-1}$. [Vink: Etabler, for n -sæt af ikke-negative tal, en bijektiv korrespondence mellem sæt (i_1, \dots, i_n) med sum d og strengt voksende sæt (j_1, \dots, j_n) med $j_n = d + n - 1$.]
3. Vis, at hvis R er delring af en ring A og $\alpha_1, \dots, \alpha_n$ er elementer i A , så er *evaluering*,

$$F = \sum_{i_1, \dots, i_n} r_{i_1, \dots, i_n} X_1^{i_1} \cdots X_n^{i_n} \mapsto F(\alpha_1, \dots, \alpha_n) = \sum_{i_1, \dots, i_n} r_{i_1, \dots, i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n},$$

en ringhomomorfi $R[X_1, \dots, X_n] \rightarrow A$.

- U1 4. Vis, for elementer x i en R -modul M , at $0x = 0$ og $(-1)x = -x$.
- U1 5. Er det virkelig korrekt at tale om søjlen $(x_1, \dots, x_n)^{\text{tr}}$? Er der ikke snarere tale om en række?
6. Lad $\alpha \in \text{Mat}_{pm}(R)$ være en $p \times m$ -matrix. Vis, at $x \mapsto \alpha x$ er en R -lineær afbildning $R^m \rightarrow R^p$. Vis, at enhver R -lineær afbildning $R^m \rightarrow R^p$ er af denne form med en entydig bestemt matrix α .
7. Lad der være givet en undermodul $N_i \subseteq M_i$ for $i = 1, \dots, m$. Bestem en isomorfi,

$$\frac{M_1 \oplus \dots \oplus M_m}{N_1 \oplus \dots \oplus N_m} \xrightarrow{\sim} M_1/N_1 \oplus \dots \oplus M_m/N_m.$$

8. Vis for elementer x_1, \dots, x_k i R , at $(x_1) + \dots + (x_k) = (x_1, \dots, x_k)$.
- U1 9. Beskriv, for et naturligt tal n , idealet (n, X) i $\mathbb{Z}[X]$. Vis, at idealet er kernen for en „oplagt“ homomorfi $\mathbb{Z}[X] \rightarrow \mathbb{Z}/n$.
- U2 10. Beskriv idealet (X, Y) i $\mathbb{Q}[X, Y]$. Vis, at $(X, Y)^2 = (X^2, XY, Y^2)$, og at dette ideal ikke kan frembringes af færre end 3 polynomier.
11. Lad d være et normeret polynomium af grad d i $R[X]$. Ringen $R[X]$ og kvotienten $R[X]/(d)$ er specielt moduler over R . Lad ξ være restklassen af X modulo (d) . Vis, at de potenser $1, \xi, \dots, \xi^{n-1}$ er en R -basis for $R[X]/(d)$.
- U2 12. Beskriv de cykliske \mathbb{Z} -moduler. Hvilken sammenhæng er der mellem elementorden og annullator for elementer i kommutative grupper?
- U2 13. For hvilke elementer x i R -modulen M er $\text{Ann}(x)$ et ægte ideal?
- U2 14. Antag, at R er et integritetsområde. Hvad kan du sige om $\text{Ann}(r)$ for $r \in R$?
15. Betragt for et ideal \mathfrak{a} kvotienten R/\mathfrak{a} som R -modul. Lad $\bar{1} \in R/\mathfrak{a}$ betegne restklassen af 1. Vis, at $\text{Ann}(\bar{1}) = \mathfrak{a}$.
- U2 16. Hvad plejer vi at kalde cykliske undermoduler af en given \mathbb{Z} -modul?
- U2 17. Hvis M er en fri modul med basis e_1, \dots, e_n , kaldes antallet n af basiselementer også modulens *rang*. Kan du finde et problem i denne definition? *Og løse det?
18. Vis, at en kvadratisk matrix α er invertibel i $\text{Mat}_n(R)$, hvis og kun hvis $\det \alpha$ er invertibel i R .
19. Vis for en given mængde I , at mængden R^I af alle afbildninger $x: I \rightarrow R$ på naturlig måde er en R -modul. For et element $x \in R^I$ og $i \in I$ skrives ofte $x_i = x(i)$ for værdien i i ; elementet $x_i \in R$ er den i 'te *koordinat* af x . Vis, at delmængden bestående af de elementer $x \in R^I$, der kun har endelig mange koordinater (evt ingen) forskellige fra 0, udgør en undermodul af R^I ; den betegnes $R^{\oplus I}$.
- For $i \in I$ betegnes med δ_i den karakteristiske funktion for i , dvs værdien δ_{ij} er 1 (et elementet i R) når $i = j$, og 0 ellers. Øjensynlig er $\delta_i \in R^{\oplus I}$. Vis, at hvert element $x \in R^{\oplus I}$ har en entydig fremstilling som en (endelig) linearkombination af elementerne δ_i , nemlig som

$$x = \sum_{i \in I} x_i \delta_i$$

30. marts 2007

(hvor summen er endelig i den forstand, at skalaren x_i kun er forskellig fra 0 i endelig mange af leddene).

Oftest identificeres elementerne $i \in I$ med de tilsvarende elementer δ_i , og I opfattes som delmængde af $R^{\oplus I}$. Man kan så tænke på elementerne i $R^{\oplus I}$ som *formelle linearkombinationer* af elementerne i den givne mængde. Modulen $R^{\oplus I}$ kaldes den frie modul med basis I . Vis, at enhver afbildning $\varphi: I \rightarrow M$, fra mængden I til en R -modul M , entydigt kan udvides til en lineær afbildning $\tilde{\varphi}: R^{\oplus I} \rightarrow M$.

20. Elementerne i en direkte sum $M_1 \oplus \dots \oplus M_n$ er søjler af n -sæt x , hvor den i 'te koordinat x_i tilhører M_i . Betragt for simpelhedens skyld tilfældet $n = 2$, altså en direkte sum $P \oplus Q$. I overensstemmelse med denne konvention skrives homomorfier *ind* i $P \oplus Q$ som søjler: idet $\varphi: M \rightarrow P$ og $\psi: M \rightarrow Q$ er givne homomorfier, betegner søjlen $\begin{pmatrix} \varphi \\ \psi \end{pmatrix}$ homomorfien,

$$\begin{pmatrix} \varphi \\ \psi \end{pmatrix}: M \rightarrow P \oplus Q, \quad \text{bestemt ved } x \mapsto \begin{pmatrix} \varphi \\ \psi \end{pmatrix} x = \begin{pmatrix} \varphi x \\ \psi x \end{pmatrix}.$$

Tilsvarende skrives homomorfier *fra* $P \oplus Q$ som rækker: idet $\alpha: P \rightarrow N$ og $\beta: Q \rightarrow N$ er givne homomorfier, betegner rækken $(\alpha \ \beta)$ homomorfien,

$$(\alpha \ \beta): P \oplus Q \rightarrow N \quad \text{bestemt ved } \begin{pmatrix} x \\ y \end{pmatrix} \mapsto (\alpha \ \beta) \begin{pmatrix} x \\ y \end{pmatrix} = \alpha x + \beta y.$$

Betragt mere generelt to direkte summer $M = M_1 \oplus \dots \oplus M_m$ og $N = N_1 \oplus \dots \oplus N_p$. Vis, at de lineære afbildninger $\alpha: M \rightarrow N$ er afbildningerne $x \mapsto \alpha x$, hvor α er en $p \times m$ -matrix af lineære afbildninger (mere præcist, hvor α på plads i, j har en lineær afbildning $\alpha_{ij}: M_j \rightarrow N_i$).

21. Vis, at hvis $(A, +, \cdot, R)$ er en R -algebra (associativ, med et-element, det forudsættes altid), så defineres ved

$$r \mapsto r 1_A$$

en ringhomomorfi $\varphi: R \rightarrow A$ som opfylder $r x = \varphi(r)x$. Præciser, hvad der menes med følgende påstand: En kommutativ R -algebra A er „det samme som“ en kommutativ ring A med en ringhomomorfi $\varphi: R \rightarrow A$. Og vis påstanden. Hvorfor indgår ordet „kommutativ“ i påstanden?

22. Bestem, for polynomiumsringen i $m + k$ variable, en isomorfi,

$$R[X_1, \dots, X_m, Y_1, \dots, Y_k]/(Y_1, \dots, Y_k) \xrightarrow{\sim} R[X_1, \dots, X_m].$$

U2 **23.** Antag, at R er et PID. Vis, at enhver undermodul $K \subseteq R^n$ er fri, og at der for rangen, dvs elementantallet i en basis, gælder $\text{rk } K \leq n$.

H1 **24.** Vis for et ideal $\mathfrak{a} \subseteq R$, at delmængden $\text{Rad}(\mathfrak{a})$ faktisk er et ideal i R , og at $\mathfrak{a} \subseteq \text{Rad}(\mathfrak{a})$. Vis, at for et primideal \mathfrak{p} er $\text{Rad}(\mathfrak{p}) = \mathfrak{p}$; og mere generelt: $\text{Rad}(\mathfrak{p}^n) = \mathfrak{p}$ for $n \geq 1$.

U3 **25.** Vis for et ideal \mathfrak{a} i R og en modul M , at mængden $\mathfrak{a}M$, af alle summer af produkter ax for $a \in \mathfrak{a}$ og $x \in M$, er en undermodul. Vis (og præciser), at kvotienten $M/\mathfrak{a}M$ naturligt er en R/\mathfrak{a} -modul.

- U3 **26.** Lad p være et primtal og lad M være en endelig kommutativ gruppe (additivt skrevet). Vis, at M/pM naturligt er et vektorrum over \mathbb{F}_p . Vis, at vektorrumsdimensionen af M/pM er „relateret“ til de cykliske grupper af primtalspotensorden, der indgår i M ifølge Struktursætningen for endelige kommutative grupper.
- 27.** Vis, at de lineære afbildninger $e: R^n \rightarrow M$ er afbildningerne af formen $e(x) = (e_1, \dots, e_n)$ svarende til et sæt af n elementer e_1, \dots, e_n i R -modulen M .
 Vis, at sættet (e_1, \dots, e_n) er et frembringersystem for M , hvis og kun hvis $e: R^n \rightarrow M$ er surjektiv. Sættet (e_1, \dots, e_n) er *lineært uafhængigt*, hvis den eneste *lineære relation* $x_1e_1 + \dots + x_n e_n = 0$ er den *trivielle*, hvor $x_1 = \dots = x_n = 0$. Vis, at sættet er lineært uafhængigt, hvis og kun hvis $e: R^n \rightarrow M$ er injektiv. Vis, at sættet er en basis for M , hvis og kun hvis $e: R^n \rightarrow M$ er en isomorfi.
- 28.** Det er et fundamentalt resultat i lineær algebra, at en lineær afbildning $\alpha: R^d \rightarrow R^d$ er injektiv, hvis og kun hvis determinanten $\det(\alpha)$ ikke er en nuldivisor, dvs hvis og kun hvis multiplikation med $\det(\alpha)$ er en injektiv afbildning $R \rightarrow R$. Vis, at „hvis“ følger af Cramer's formler. Det generelle resultat er ikke så let at eftervise. Vis resultatet for integritetsområder R . Vis, ved hjælp af resultatet, at en lineær afbildning $R^n \rightarrow R^d$ kun kan være injektiv når $n \leq d$ (eller når R er nulringen).
 Ved *rangen* af en modul M , betegnet $\text{rk } M$, forstås det største antal elementer, der kan være i et lineært uafhængigt system i M . Ved *frembringerdimensionen*, betegnet $\dim_{\text{gen}} M$, forstås det mindste antal elementer, der kan være i et frembringersystem for M . [Bemærk, at notationen $\dim_{\text{gen}} M$ ikke er en standardnotation.] Vis, ved hjælp af resultatet, at der generelt gælder $\text{rk } M \leq \dim_{\text{gen}} M$. Vis yderligere, at hvis M er endeligt frembragt, så er M fri, hvis og kun hvis $\text{rk } M = \dim_{\text{gen}} M$.
- H1 **29.** Vis, at de cykliske moduler R/\mathfrak{a} og R/\mathfrak{b} er isomorfe, hvis og kun hvis idealerne \mathfrak{a} og \mathfrak{b} er det samme: $\mathfrak{a} = \mathfrak{b}$. [Vink: Overvej, hvordan du ud fra R -modulen R/\mathfrak{a} kan bestemme idealet \mathfrak{a} .]
- H2 **30.** Antag, at $x \in R$ er nilpotent. Vis, at så er $1 + x$ invertibel i R .
31. Betragt polynomiumsringen $G = R[X_1, \dots, X_n]$. Vis, for idealet $\mathfrak{M} = (X_1, \dots, X_n)$ i G , at $G/\mathfrak{M} = R$. Lad G_d være undergruppen af homogene polynomier af grad d . Det er en fri R -modul, der som basis har monomierne af grad d . Vis, at $G_d \subseteq \mathfrak{M}^d$. Vis, at $\mathfrak{M}^d/\mathfrak{M}^{d+1}$ er en modul over $G/\mathfrak{M} = R$. Beskriv \mathfrak{M}^d , og bestem en naturlig R -lineær isomorfi $\mathfrak{M}^d = G_d \oplus \mathfrak{M}^{d+1}$. Udled heraf en R -isomorfi $G_d \xrightarrow{\sim} \mathfrak{M}^d/\mathfrak{M}^{d+1}$.
- U6 **32.** Vis for en R -modul M og $a \in R$, at $(a)M = aM$ (hvor $aM := \{ax \mid x \in M\}$).
33. Et element x i R -modulen M kaldes et *torsionselement*, hvis der findes en skalar r , der ikke er nuldivisor i R , således, at $rx = 0$. Vis, at torsionselementerne i M udgør en undermodul M_{tors} af M og at kvotientmodulen M/M_{tors} er „torsionsfri“.
34. Antag, at R er et PID. Antag, at Q er en R -modul frembragt af e, f , og at der findes en lineær relation $ae + bf = 0$ med $a \neq 0$. Lad d være største fælles divisor for a, b . Vis, at der findes $x, y \in R$ således, at $ax + by = d$, og at der så gælder: elementerne $\hat{e} = (a/d)e + (b/d)f$ og $\hat{f} = -ye + xf$ frembringer Q og $d\hat{e} = 0$.

Antag, at M er en endeligt frembragt torsionsfri R -modul (dvs $\text{Ann}(x) = (0)$ for $x \neq 0$). Vis, at M fri. [Vink: Vis, ved induktion efter n , at ethvert frembringersystem e_1, \dots, e_n for M , hvor n er mindst mulig, er en basis.]

H3 35. Vis, at enhver surjektiv homomorfi $\alpha: R^n \rightarrow R^n$ er en isomorfi. [Vink: Vis, ved hjælp af Cramer's formler, at for kvadratiske matricer α, β medfører ligningen $\alpha\beta = 1$, at α er invertibel med β som den inverse.]

U9 36. Den adjungerede til en 2×2 -matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ er matricen $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. I matricen $\begin{pmatrix} 2 & 3 \\ 3 & 8 \end{pmatrix}$ står tallene for deres restklasser modulo 24. Bestem den inverse matrix.

37. Betragt en $(n \times k)$ -matrix β og en $(k \times p)$ -matrix α , og produktmatricen $\gamma := \beta\alpha$. Overvej om følgende matrixligninger er rigtige:

$$\gamma_i = (\beta_1, \dots, \beta_k)\alpha_i, \quad (\gamma_1, \dots, \gamma_p) = (\beta_1, \dots, \beta_k)\alpha.$$

38. Antag, at $\Psi: M^n \rightarrow N$ er lineær i hver af de n variable, og alternerende, dvs lig med 0 når to af de n argumenter er ens. Vis, for $(x_1, \dots, x_n) \in M^n$ og en permutation $\sigma \in S_n$, at $\Psi(x_{\sigma_1}, \dots, x_{\sigma_n}) = \text{sign}(\sigma)\Psi(x_1, \dots, x_n)$.

39. Hvordan løser man ved hjælp af Cramer's formler, for en invertibel matrix α i $\text{Mat}_n(R)$, et lineært ligningssystem $\alpha x = b$?

2. Kerne og kokerne. Exakte følger.

(2.1) Kerne og kokerne. Lad der være givet en homomorfi, dvs en R -lineær afbildning, $\varphi: M \rightarrow N$. Ved *kernen* for φ forstås som bekendt originalmængden $\varphi^{-1}(0)$. Kernen betegnes $\text{Ker } \varphi$. Øjensynlig er kernen en undermodul af M . Videre er *billedet* φM en undermodul af N . Ved *kokernen* for φ forstås den tilhørende kvotientmodul $N/\varphi M$. Kokernen betegnes $\text{Coker } \varphi$.

Som bekendt er φ injektiv, hvis og kun hvis $\text{Ker } \varphi = 0$. Af definitionen fremgår umiddelbart, at φ er surjektiv, hvis og kun hvis $\text{Coker } \varphi = 0$.

(2.2) Observation. Lad der være givet et kommutativt diagram af moduler,

$$\begin{array}{ccc} M & \xrightarrow{\mu} & M' \\ \varphi \downarrow & & \downarrow \varphi' \\ N & \xrightarrow{\nu} & N'. \end{array}$$

[Her, som i det følgende, siges et diagram bestående af moduler og homomorfier at være *kommutativt*, hvis det for hvilket som helst to moduler M og P i diagrammet gælder, at alle homomorfier fra M til P , der kan fås ved sammensætning af diagrammets homomorfier, er ens.]

I diagrammet er altså $\nu\varphi = \varphi'\mu$. Homomorfien μ vil da afbilde undermodulen $\text{Ker } \varphi$ af M ind i undermodulen $\text{Ker } \varphi'$ af M' . Antag nemlig, at x tilhører $\text{Ker } \varphi$. Så er altså $\varphi x = 0$, og dermed også $\nu\varphi x = 0$. Da diagrammet er kommutativt, følger det at $\varphi'\mu x = 0$. Og det betyder jo, at μx tilhører $\text{Ker } \varphi'$.

Det kommutative diagram vil altså *inducere* en homomorfi mellem kernerne,

$$\text{Ker } \varphi \rightarrow \text{Ker } \varphi'.$$

Tilsvarende vil ν afbilde undermodulen φM af N ind i undermodulen $\varphi' M'$ af N' . Heraf fås en veldefineret afbildning $N/\varphi M \rightarrow N'/\varphi' M'$ mellem kvotienterne: en klasse i $N/\varphi M$ med repræsentanten $x \in N$ afbildes på den klasse i $N'/\varphi' M'$, som repræsenteres af $\nu x \in N'$. Der *induceres* altså en homomorfi mellem kokerne,

$$\text{Coker } \varphi \rightarrow \text{Coker } \varphi'.$$

(2.3) Nulfølge og eksakt følge. Lad der være givet en følge af moduler og homomorfier,

$$\cdots \longrightarrow M_{i+1} \xrightarrow{\varphi_{i+1}} M_i \xrightarrow{\varphi_i} M_{i-1} \longrightarrow \cdots$$

Følgen kan være endelig, eller uendelig i en eller begge retninger. Følgen siges da at være en *nulfølge*, hvis sammensætningen af to på hinanden følgende homomorfier altid er nul. Dette betyder, at billedet af φ_{i+1} er indeholdt i kernen for φ_i for alle i . Følgen kaldes *eksakt i modulen* M_i , hvis billedet af φ_{i+1} er lig med kernen for φ_i , og den kaldes en *eksakt følge*, hvis den er eksakt i M_i for alle i .

I definitionen forudsættes naturligvis, at M_i ikke er følgens første eller sidste modul, således at både φ_{i+1} og φ_i er definerede.

(2.4) Observation. Betragt for en given homomorfi $\varphi: M \rightarrow N$ følgerne herunder:

$$0 \longrightarrow M \xrightarrow{\varphi} N, \quad (2.4.1)$$

$$M \xrightarrow{\varphi} N \longrightarrow 0, \quad (2.4.2)$$

$$0 \longrightarrow M \xrightarrow{\varphi} N \longrightarrow 0. \quad (2.4.3)$$

Følgen (2.4.1) er naturligvis en nulfølge. Billedet ved den første homomorfi er nul-undermodulen 0 i M . Følgen er altså eksakt, netop når kernen for φ kun består af 0, altså netop når φ er injektiv.

Tilsvarende ses, at følgen (2.4.2) er eksakt, netop når φ er surjektiv. Heraf ses, at følgen (2.4.3) eksakt netop når φ er bijektiv, dvs en isomorfi.

Betragt nu videre følgerne:

$$0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P, \quad (2.4.4)$$

$$M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0. \quad (2.4.5)$$

Følgen (2.4.4) er eksakt i M , netop når φ er injektiv, dvs når φ afbilder M isomorft på billedet φM . Den er eksakt i N , hvis φM er lig med kernen for ψ . At følgen er eksakt betyder altså at φ afbilder M isomorft på kernen af ψ . Lidt løst betyder det, at M „er“ kernen for homomorfien ψ .

Følgen (2.4.5) er eksakt i P , netop når ψ er surjektiv. Lad K betegne kernen for ψ . Ifølge isomorfisætningen induceres da en injektiv homomorfi $N/K \rightarrow P$ med billedet ψN . Homomorfien ψ er altså surjektiv, netop når den inducerede homomorfi $N/K \rightarrow P$ er en isomorfi. At følgen er eksakt i N betyder, at K er lig med billedet af φ , altså at N/K er lig med kokernen for φ . At følgen er eksakt betyder altså at ψ afbilder kokernen for φ isomorft på P . Lidt løst betyder det, at P „er“ kokernen for homomorfien φ .

(2.5) Isomorfisætning. Følgen,

$$0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0,$$

er eksakt, hvis og kun hvis φ „er“ inklusionen af en undermodul af N og ψ „er“ den kanoniske homomorfi på den tilhørende kvotient.

Bevis. Påstanden er øjensynlig et specialtilfælde af overvejelserne i (2.4). □

(2.6) Slangelemma. Lad der være givet et kommutativt diagram med eksakte rækker,

$$\begin{array}{ccccccc} M' & \xrightarrow{\mu'} & M & \xrightarrow{\mu} & M'' & \longrightarrow & 0 \\ \varphi' \downarrow & & \varphi \downarrow & & \varphi'' \downarrow & & \\ 0 & \longrightarrow & N' & \xrightarrow{\nu'} & N & \xrightarrow{\nu} & N'' \end{array}.$$

Da induceres naturligt en eksakt følge mellem kerner og kokerner,

$$\text{Ker } \varphi' \longrightarrow \text{Ker } \varphi \longrightarrow \text{Ker } \varphi'' \xrightarrow{\delta} \text{Coker } \varphi' \longrightarrow \text{Coker } \varphi \longrightarrow \text{Coker } \varphi'' .$$

Hvis homomorfien μ' er injektiv, så er den første homomorfi mellem kernerne injektiv. Hvis homomorfien ν er surjektiv, så er den sidste homomorfi mellem kokernerne surjektiv.

(2.7) Kerne-kokerner-følgen. Følgen af kerner og kokerner i Slangelemma'et kaldes *kerne-kokerner-følgen*. Homomorfien δ , der indgår heri, kaldes også den *forbindende homomorfi*. Den defineres således: Lad x være et element i kernen for φ'' . Specielt er x så element i M'' , og da homomorfien μ er surjektiv findes et element w i M , så at $\mu w = x$. Betragt billedet φw i N . Da diagrammet er kommutativt og x tilhører kernen for φ'' , får vi at

$$\nu \varphi w = \varphi'' \mu w = \varphi'' x = 0.$$

Altså vil φw tilhøre kernen for ν . Da diagrammets nederste række er eksakt i N , følger det, at φw tilhører billedet $\nu' N'$. Altså findes et element y i N' , så at $\nu' y = \varphi w$. Billedelementet δx defineres nu som den klasse i $\text{Coker } \varphi'$, der repræsenteres af elementet $y \in N'$.

Det er naturligvis en del af Slangelemma'et, at denne definition er lovlig, dvs at billedet δx ikke afhænger af de valg (af w og y), der indgik i definitionen.

Bevis for Slangelemma. Det skal vises, at definitionen af δ er lovlig, og at δ er en homomorfi. Videre skal det vises, at følgen er eksakt på 4 steder. Endelig skal lemma'ets to sidste påstande bevises. Beviserne udføres ved en såkaldt *diagramjagt*, hvor elementer føres rundt i diagrammet langs pilene under udnyttelse af eksaktheden. Vi efterviser kun to af påstandene, og overlader resten til læseren.

Følgen er eksakt i $\text{Coker } \varphi$: Betragt hertil en klasse i $\text{Coker } \varphi$, og vælg en repræsentant x for den. Det skal vises, at klassen afbildes i nul-klassen i $\text{Coker } \varphi''$, hvis og kun hvis klassen kommer fra en klasse i $\text{Coker } \varphi'$. At klassen repræsenteret ved x afbildes i 0 i $\text{Coker } \varphi''$ betyder at νx tilhører billedet $\varphi'' M''$, altså at der findes et element z i M'' så at $\varphi'' z = \nu x$. Ifølge antagelsen er μ surjektiv, så et sådant element z har formen μy . Klassen afbildes derfor i 0, hvis og kun hvis der findes et element y i M , så at $\nu x = \varphi'' \mu y$. Da diagrammet er kommutativt, er $\varphi'' \mu = \nu \varphi$, og betingelsen kan derfor også skrives $\nu x = \nu \varphi y$. Klassen afbildes derfor i 0, hvis og kun hvis der findes et element y i M , så at

$$\nu(x - \varphi y) = 0.$$

Elementerne af formen $x - \varphi y$, hvor $y \in M$, er netop samtlige repræsentanter for den givne klasse. Heraf ses, at klassen afbildes i 0, hvis og kun hvis den har en repræsentant, der tilhører kernen for ν . Da den nederste række i diagrammet er eksakt, er den sidste betingelse ækvivalent med at klassen har en repræsentant, der tilhører billedet for ν' . Nu er det klart, at klassen afbildes i 0, hvis og kun hvis den kommer fra en klasse i $\text{Coker } \varphi'$.

Følgen er eksakt i $\text{Ker } \varphi''$: Lad nemlig x være et element i $\text{Ker } \varphi''$. Det skal vises, at $\delta x = 0$, hvis og kun hvis der findes et element v i $\text{Ker } \varphi$ så at $\mu v = x$.

„hvis“: Antag, at $v \in \text{Ker } \varphi$ og $\mu v = x$. Som det element w der indgår i definitionen på δx kan vi så bruge $w := v$. Da w så tilhører $\text{Ker } \varphi$, er $\varphi w = 0$. Som det element y der indgår i definitionen af δx kan vi derfor vælge $y := 0$. Da klassen δx så er repræsenteret ved $y = 0$, er $\delta x = 0$.

„kun hvis“: Antag omvendt, at $\delta x = 0$. I definitionen af δ indgår to valgte elementer y og w . Da $\delta x = 0$, er repræsentanten y element i $\varphi' M'$. Der findes altså et element u i M' så at $\varphi' u = y$. Ifølge valget af y i definitionen af δ er $v' y = \varphi w$. Videre er $v' \varphi' = \varphi \mu'$ da diagrammet er kommutativt. Altså er

$$\varphi \mu' u = v' \varphi' u = v' y = \varphi w.$$

Heraf ses, at elementet $v := w - \mu' u$ tilhører kernen for φ . Yderligere er $\mu \mu' = 0$ ifølge forudsætningen, og heraf fås, at

$$\mu v = \mu w - \mu \mu' u = \mu w = x,$$

idet den sidste ligning følger af valget af w . Altså er v element i kernen for φ og $\mu v = x$, som ønsket. \square

(2.9) Bemærkning. De to ekstra antagelser i slutningen af Slangelemma'et kan under ét udtrykkes ved at følgende kommutative diagram har eksakte rækker:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{\mu'} & M & \xrightarrow{\mu} & M'' & \longrightarrow & 0 \\ & & \varphi' \downarrow & & \varphi \downarrow & & \varphi'' \downarrow & & \\ 0 & \longrightarrow & N' & \xrightarrow{v'} & N & \xrightarrow{v} & N'' & \longrightarrow & 0. \end{array}$$

Konklusionen er så en udvidet eksakt kerne-kokerne-følge,

$$0 \longrightarrow \text{Ker } \varphi' \longrightarrow \text{Ker } \varphi \longrightarrow \text{Ker } \varphi'' \xrightarrow{\delta} \text{Coker } \varphi' \longrightarrow \text{Coker } \varphi \longrightarrow \text{Coker } \varphi'' \longrightarrow 0.$$

Slangelemma'et har en lang række anvendelser. Her indskrænker vi os til at vise nogle klassiske isomorfi-sætninger.

(2.10) Korollar. Lad der være givet en homomorfi $\varphi: M \rightarrow P$ og undermoduler $F_1 \subseteq F_2$ af M . For $i = 1, 2$ betegnes med F'_i kernen for φ 's restriktion til F_i og med F''_i billedet af F_i i P . Da induceres en eksakt følge mellem kvotienterne,

$$0 \longrightarrow F'_2/F'_1 \longrightarrow F_2/F_1 \longrightarrow F''_2/F''_1 \longrightarrow 0.$$

Bevis. Undermodulen F'_i af M er blot fællesmængden af F_i og $\text{Ker } \varphi$, så det er klart, at $F'_1 \subseteq F'_2$. Det er ligeledes klart, at $F''_1 \subseteq F''_2$. Afbildningen φ definerer ved restriktion en

surjektiv afbildning $F_i \rightarrow F_i''$, og kernen for denne afbildning er øjensynlig undermodulen F_i' . Vi får derfor følgende diagram,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F_1' & \longrightarrow & F_1 & \longrightarrow & F_1'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & F_2' & \longrightarrow & F_2 & \longrightarrow & F_2'' & \longrightarrow & 0, \end{array}$$

hvor de lodrette pile er inklusionsafbildninger. Rækkerne er eksakte ifølge Isomorfinisætning (2.5). Det er klart, at diagrammet er kommutativt. Da den sidste lodrette pil i diagrammet er injektiv, er den tilsvarende kerne lig med 0. Den søgte eksakte følge af kvotienter er altså den sidste del af den eksakte kerne-kernerne-følge. \square

(2.11) Noether's første Isomorfinisætning. Lad P og Q være undermoduler i modulen M . Da findes en naturlig isomorfi,

$$\frac{P}{P \cap Q} \xrightarrow{\sim} \frac{P + Q}{Q}.$$

Bevis. Lad $\varphi: M \rightarrow M/P$ være den kanoniske homomorfi af M på kvotienten. Undermodulen P er da kernen for φ . Anvend nu Korollar (2.10) med $F_1 := Q$ og $F_2 := P + Q$. Øjensynlig er $F_1' = P \cap Q$, og $F_2' = P$, da $F_2 \supseteq P$. Billedet F_i'' er billedet af F_i i kvotienten M/P . Her er $F_1'' = F_2''$, thi elementerne i F_2'' er jo ækvivalensklasserne modulo P med repræsentanter af formen $p + q$, hvor $p \in P$ og $q \in Q$, og modulo P vil $p + q$ og q repræsentere samme klasse. I den eksakte følge fra (2.10) er altså $F_2''/F_1'' = 0$. Eksaktheden sikrer derfor, at homomorfien $F_2'/F_1' \rightarrow F_2/F_1$ er en isomorfi. Og det er netop Noether's første isomorfi. \square

(2.12) Noether's anden Isomorfinisætning. Lad der være givet en modul M , og heri undermoduler $N \subseteq F$. Da findes en naturlig eksakt følge,

$$0 \longrightarrow F/N \longrightarrow M/N \longrightarrow M/F \longrightarrow 0.$$

Bevis. Lad $\varphi: M \rightarrow M/F$ være den kanoniske afbildning af M på kvotienten. Undermodulen F er da kernen for φ . Anvend nu Korollar (2.10) med $F_1 := N$ og $F_2 := M$. Her finder vi $F_2' = F$ og $F_1' = N$. Billedet F_2'' er billedet for φ , altså $F_2'' = M/F$, og billedet F_1'' er nulmodulen i M/F , da $F_1 = N$ er indeholdt i F . Kvotienten F_2''/F_1'' er altså lig med M/F . Den eksakte følge i (2.10) er altså den ønskede. \square

(2.13) Bemærkning. Ifølge Isomorfinisætning (2.5) kan eksaktheden af følgen i Noether's anden isomorfinisætning udtrykkes således: Modulen F/N er en undermodul i M/N , og M/F er den tilhørende kvotientmodul. Med andre ord findes en naturlig isomorfi,

$$\frac{M/N}{F/N} \xrightarrow{\sim} M/F.$$

I anvendelserne af Noether's anden Isomorfinisætning vil man ofte udnytte, at undermodulerne i M/N netop er undermodulerne af formen F/N , hvor $F \supseteq N$ er entydigt bestemt. Eftervisningen heraf overlades til læseren.

(2.14) Kerne-kokerne-følgen for sammensat homomorfi. Lad $\varphi: M \rightarrow N$ og $\psi: N \rightarrow P$ være homomorfier. Da induceres naturligt en eksakt følge,

$$0 \longrightarrow \text{Ker } \varphi \longrightarrow \text{Ker } \psi\varphi \xrightarrow{\varphi} \text{Ker } \psi \xrightarrow{\delta} \text{Coker } \varphi \xrightarrow{\psi} \text{Coker } \psi\varphi \longrightarrow \text{Coker } \psi \longrightarrow 0.$$

Bevis. Det er klart, at $\text{Ker } \varphi$ er indeholdt i $\text{Ker } \psi\varphi$. Følgens første homomorfi er den tilsvarende inklusionsafbildning. Det er også klart, at $\psi\varphi M$ er indeholdt i ψN . Disse to billeder er undermoduler af P , og følgens sidste homomorfi er den tilsvarende surjektive homomorfi mellem kvotienterne.

Homomorfin markeret φ i følgen er induceret af $\varphi: M \rightarrow N$: når x tilhører $\text{Ker } \psi\varphi$, vil φx tilhøre $\text{Ker } \psi$. Tilsvarende er homomorfin ψ i følgen induceret af $\psi: N \rightarrow P$: denne homomorfi afbilder nemlig φM på $\psi\varphi M$, så når $x \in M$ er repræsentant for en klasse i $\text{Coker } \varphi$, så er ψx repræsentant for en veldefineret klasse i $\text{Coker } \psi\varphi$.

Endelig afbilder δ et element x i $\text{Ker } \psi$ på ækvivalensklassen af x modulo φM .

Beviset for at kerne-kokerne-følgen er eksakt overlades til læseren. □

(2.15) Opgaver.

1. Lad der nu være givet homomorfier $\varphi: M \rightarrow N$ og $\psi: N \rightarrow P$, og lad $\gamma := \psi\varphi$ betegne den sammensatte homomorfi. Betragt følgende diagram,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\begin{pmatrix} 1 \\ \varphi \end{pmatrix}} & M \oplus N & \xrightarrow{(\varphi \ -1)} & N & \longrightarrow & 0 \\ & & \varphi \downarrow & & \begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix} \downarrow & & \psi \downarrow & & \\ 0 & \longrightarrow & N & \xrightarrow{\begin{pmatrix} 1 \\ \psi \end{pmatrix}} & N \oplus P & \xrightarrow{(-\psi \ 1)} & P & \longrightarrow & 0. \end{array}$$

Gør rede for hvorledes afbildningerne, specielt den midterste lodrette, er definerede. Vis, at rækkerne er eksakte og at diagrammet er kommutativt. Vis, at kerne-kokerne-følgen for diagrammet kan identificeres med følgen i (2.14), og giv herved et alternativt bevis for at denne sidste følge er eksakt.

2. Følgen $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \xrightarrow{\gamma} D \xrightarrow{\delta} E \rightarrow 0$ er eksakt. Endvidere vides, at β er nulafbildningen. Hvad kan du sige om de øvrige afbildninger i følgen?

3. Betragt en nul-følge,

$$0 \longrightarrow C_p \longrightarrow C_{p-1} \longrightarrow \dots \longrightarrow C_1 \longrightarrow C_0 \longrightarrow 0, \tag{*}$$

og lad $Z_i \subseteq C_i$ være kernen for $C_i \rightarrow C_{i-1}$, for alle i (det er underforstået, at $C_i = 0$ når i ikke er et af tallene $i = 0, \dots, p$). Gør rede for at homomorfin $C_{i+1} \rightarrow C_i$ afbilder ind i undermodulen Z_i . Vis, at følgen (*) er eksakt, hvis og kun hvis følgerne herunder, for alle i , er eksakte:

$$0 \longrightarrow Z_i \longrightarrow C_i \longrightarrow Z_{i-1} \longrightarrow 0.$$

Vis, at hvis $0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$ er en eksakt følge af endeligdimensionale vektorrum, så er $\dim V = \dim U + \dim W$. Vis, at hvis (*) er en eksakt følge af endeligdimensionale vektorrum, så er den alternerende sum af dimensionerne lig med 0,

$$\sum_p (-1)^p \dim C_p = 0.$$

- U2 **4.** Betragt en korteksakt følge $0 \rightarrow K \rightarrow M \rightarrow L \rightarrow 0$. Antag, at K og L er frie moduler. Vis, at M er fri. [Vink: „løft“ elementerne fra en basis for L til elementer i M , og suppler med (billederne af) en basis for K . Vis, at der herved fremkommer en basis for M .]
- U3 **5.** Lad \mathfrak{a} være et ideal. Vis, at hvis følgen $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ er eksakt, så er også følgen $M'/\mathfrak{a}M' \rightarrow M/\mathfrak{a}M \rightarrow M''/\mathfrak{a}M'' \rightarrow 0$ eksakt. Manglede pilen $0 \rightarrow M'/\mathfrak{a}M'$ i den sidste følge?
- 6.** Lad N og M være moduler, og betragt inklusionen $i: N \rightarrow N \oplus M$ (bestemt ved $x \mapsto (x, 0)$) og projektionen $p: N \oplus M \rightarrow M$ bestemt ved $(x, y) \mapsto y$. Gør rede for, at følgen $0 \rightarrow N \xrightarrow{i} N \oplus M \xrightarrow{p} M \rightarrow 0$ er eksakt.
- H4 **7.** Lad φ være en endomofi i modulen M , dvs en lineær afbildning $\varphi: M \rightarrow M$. Vis, at kæden af kerner er stigende: $\text{Ker } \varphi \subseteq \text{Ker } \varphi^2 \subseteq \text{Ker } \varphi^3 \subseteq \dots$, og at kæden af billeder er dalende: $\varphi M \supseteq \varphi^2 M \supseteq \varphi^3 M \supseteq \dots$. Vis, at der findes et kommutativt diagram med exakte rækker,

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \text{Ker } \varphi^n & \longrightarrow & M & \xrightarrow{\varphi^n} & \varphi^n M \longrightarrow 0 \\
 & & \text{inkl.} \downarrow & & \downarrow = & & \downarrow \varphi \\
 0 & \longrightarrow & \text{Ker } \varphi^{n+1} & \longrightarrow & M & \xrightarrow{\varphi^{n+1}} & \varphi^{n+1} M \longrightarrow 0.
 \end{array}$$

Slut heraf, at $\text{Ker } \varphi^n = \text{Ker } \varphi^{n+1}$, hvis og kun hvis restriktionen $\varphi: \varphi^n M \rightarrow \varphi^n M$ er injektiv. Antag nu, at (mindst) et af billederne $\varphi^i M$ har endelig længde. Vis, at når $n \gg 0$, så er restriktionen $\varphi: \varphi^n M \rightarrow \varphi^n M$ bijektiv og $M = \text{Ker } \varphi^n \oplus \varphi^n M$.

3. Brøkring og brøkmodul.

I det følgende betegner S en *multiplikativ delmængde* af ringen R , dvs en delmængde, som er stabil over for multiplikation og indeholder et-elementet 1 i R .

(3.1) Definition. Lad M være en R -modul. Betragt produktmængden $M \times S$, altså mængden af par (x, s) , hvor $x \in M$ og $s \in S$. Er (x, s) et sådant par og er $u \in S$, siges parret (ux, us) at fremgå af (x, s) ved at *forlænge* med u . To par (x, s) og (x', s') siges at være *ækvivalente par*, hvis de kan forlænges til samme par, dvs hvis der findes $u, u' \in S$ så at $(ux, us) = (u'x', u's')$.

Det er ikke svært at vise, at denne relation i mængden af par er en ækvivalensrelation. Ækvivalensklasserne kaldes *brøker* (med tællere fra M og nævnere fra S), og mængden af brøker betegnes $S^{-1}M$. Brøken med tæller x nævner s , dvs den ækvivalensklasse som indeholder parret (x, s) , betegnes x/s .

(3.2) Observation. Det er en umiddelbar følge af definitionen, at brøker kan „forlænges“: Brøken x/s er samme brøk som $(ux)/(us)$. Dette følger af at parrene (x, s) og (ux, us) begge kan forlænges til (ux, us) (det første par forlænges med u , det andet par med 1). Tilsvarende kan man „forkorte“ $(ux)/(us)$ til x/s .

Enhver afbildning defineret på mængden af brøker er naturligvis bestemt ved en forskrift af følgende form:

$$x/t \mapsto \Phi(x, t), \text{ for } x \in M, t \in S.$$

Omvendt ses, at en sådan forskrift bestemmer en veldefineret afbildning på mængden af brøker, når blot værdien $\Phi(x, t)$ ikke ændres ved forlængelse af parret (x, t) .

(3.3) Lemma. (1) I mængden af brøker $S^{-1}M$ er additionen,

$$x/s + y/t := (tx + sy)/st,$$

en veldefineret komposition $S^{-1}M \times S^{-1}M \rightarrow S^{-1}M$, og multiplikationen,

$$(r/s)(x/t) := (rx)/(st),$$

er en veldefineret afbildning $S^{-1}R \times S^{-1}M \rightarrow S^{-1}M$. Med disse operationer er $S^{-1}R$ en ring, og $S^{-1}M$ er en $S^{-1}R$ -modul. Nul-elementet i modulen $S^{-1}M$ er brøken $0/1$, og et-elementet i ringen $S^{-1}R$ er brøken $1/1$.

(2) For hver R -lineær afbildning $\varphi: M \rightarrow N$ induceres ved forskriften,

$$x/s \mapsto (\varphi x)/s,$$

en veldefineret $S^{-1}R$ -lineær afbildning $S^{-1}\varphi: S^{-1}M \rightarrow S^{-1}N$.

(3) Betragt den kanoniske afbildning $M \rightarrow S^{-1}M$ defineret ved

$$x \mapsto x/1.$$

30. marts 2007

Herom gælder: Den kanoniske afbildning $R \rightarrow S^{-1}R$ er en ringhomomorfi, og for hvert element s i S er billedet $s/1$ invertibelt i $S^{-1}R$. Videre er den kanoniske afbildning $M \rightarrow S^{-1}M$ en R -lineær afbildning, og for hver R -lineær afbildning $\varphi: M \rightarrow N$ er følgende diagram kommutativt:

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ \downarrow & & \downarrow \\ S^{-1}M & \xrightarrow{S^{-1}\varphi} & S^{-1}N. \end{array}$$

Bevis. Beviset for disse påstande er langt og omstændeligt. Men længden skyldes alene antallet af påstande, og de trivielle beviser overlades til læseren. \square

(3.4) Lemma. (1) En brøk x/t i $S^{-1}M$ er nul-elementet, hvis og kun hvis der findes et element s i S , således at $sx = 0$. Specielt består kernen for den kanoniske homomorfi $M \rightarrow S^{-1}M$ af de elementer x i M for hvilke der findes et element s i S så at $sx = 0$.

(2) Den kanoniske homomorfi $M \rightarrow S^{-1}M$ er injektiv (henh bijektiv), hvis og kun hvis der for hvert element s i S gælder at multiplikation med s er en injektiv (henh bijektiv) afbildning $M \rightarrow M$. Hvis den kanoniske homomorfi er injektiv, så er en brøk x/t nul-elementet i $S^{-1}M$, hvis og kun hvis $x = 0$, og to brøker x/t og x'/t' ens, hvis og kun hvis $t'x = tx'$.

(3) Brøkringen $S^{-1}R$ er nul-ringen, hvis og kun hvis S indeholder nul-elementet 0 i R .

Bevis. (1) Nul-elementet i brøkmodulen $S^{-1}M$ er brøken $0/1$, så x/t er nul-elementet, hvis og kun parrene (x, t) og $(0, 1)$ er ækvivalente. Parret $(0, 1)$ kan netop forlænges til parrene af formen $(0, u)$, hvor $u \in S$. Øjensynlig kan (x, t) forlænges til et par af denne form, hvis og kun hvis der findes et element s i S så at $sx = 0$. Hermed er den første påstand bevist. Kernen for den kanoniske homomorfi består af de elementer $x \in M$, for hvilke $x/1 = 0/1$. Den anden påstand i (1) følger derfor umiddelbart af den første.

(2) Den kanoniske homomorfi er injektiv, hvis og kun hvis dens kerne kun består af nul-elementet 0 i M . Af (1) følger derfor, at den kanoniske homomorfi er injektiv, hvis og kun hvis der for alle x i M og alle $s \in S$ gælder, at $sx = 0 \Rightarrow x = 0$. Og det er øjensynlig den første påstand i (2).

Antag nu, at den kanoniske homomorfi er injektiv. Den sidste påstand i (2) følger da af (1) ved at betragte differensen $x/t - x'/t' = (t'x - tx')/tt'$. Heraf følger videre den mellemste påstand i (2). Brøken x/t tilhører nemlig billedet ved den kanoniske homomorfi, hvis og kun hvis den har formen $y/1$, dvs, hvis og kun hvis der findes y således at $x = ty$. Hermed er påstandene i (2) bevist.

(3) Hvis $S^{-1}R$ er nul-ringen, så er specielt $1/1 = 0/1$; ifølge (1) findes så et element $s \in S$ så at $s1 = 0$, og så er $0 = s$ element i S . Antag omvendt, at $0 \in S$. Det følger da af (1), at enhver brøk er nul-elementet, så $S^{-1}R$ består kun af nul-elementet. \square

(3.5) Brøkring og brøkmodul. Ringen $S^{-1}R$ kaldes *brøkringen for R mht S* , og den siges at fremkomme ved at *lokalisere mht S* ; den betegnes også $R[S^{-1}]$. Tilsvarende siges $S^{-1}M$ at være *brøkmodulen for M* . De to vigtigste eksempler på multiplikative delmængder er følgende:

30. marts 2007

(1) Delmængden S består af potenserne f^i af et givet element f i ringen R . I dette tilfælde bruges betegnelserne R_f (eller $R[f^{-1}]$) for brøkringen og M_f for brøkmodulen. Brøker har her formen x/f^i . Det følger af Lemma (3.4)(3), at R_f er nul-ringen, hvis og kun hvis der findes en eksponent i så at $f^i = 0$, dvs hvis og kun hvis elementet f er *nilpotent*.

(2) Delmængden S består af komplementærmængden i R af et givet primideal \mathfrak{p} . I dette tilfælde bruges betegnelserne $R_{\mathfrak{p}}$ for brøkringen og $M_{\mathfrak{p}}$ for brøkmodulen, og de siges at fremkomme ved at *lokalisere* i \mathfrak{p} . Brøker har her formen x/s , hvor $s \notin \mathfrak{p}$. Det følger af Lemma (3.4)(3), at brøkringen $R_{\mathfrak{p}}$ aldrig er nul-ringen.

Bemærk, at brøkringen \mathbb{Z}_f , hvor f er et helt tal forskelligt fra 0, ikke må forveksles med restklasseringen modulo f . Den sidste betegnes \mathbb{Z}/f . Bemærk videre, at for et primtal p er brøkringene \mathbb{Z}_p og $\mathbb{Z}_{(p)}$ forskellige. Begge kan opfattes som delringe af \mathbb{Q} . Den første består af rationale tal af formen r/p^n , den anden af tal af formen r/s , hvor p ikke går op i s .

(3.6) Sætning. *Lad R være et integritetsområde. Brøkringen K , der fremkommer ved at lokalisere mht alle elementer forskellige fra 0, er da et legeme, som omfatter R . For enhver multiplikativ delmængde S , som ikke indeholder nul-elementet, er brøkringen $S^{-1}R$ naturligt en delring af K ; specielt er $S^{-1}R$ et integritetsområde.*

Bevis. Da R er et integritetsområde, er delmængden bestående af alle elementer forskellige fra 0 en multiplikativ delmængde. Yderligere følger det, at multiplikationen $x \mapsto sx$, med et element $s \neq 0$, er en injektiv afbildning $R \rightarrow R$. Af Lemma (3.4)(2) følger, at den kanoniske homomorfi fra R til brøkringen K er injektiv. Vi kan altså opfatte R som delring af K .

Videre er K et legeme. Elementerne i K er nemlig brøker r/s , hvor r, s tilhører R og $s \neq 0$. Hvis en sådan brøk r/s ikke er nul-brøken, så er $r \neq 0$, og følgelig er s/r en brøk i K ; denne brøk er invers til den givne brøk r/s , idet $(r/s)(s/r) = (rs/rs) = 1/1$ er et-elementet i K . Altså har enhver brøk forskellig fra nul-brøken en invers.

Lad nu S være en multiplikativ delmængde af R , så at $0 \notin S$. Det påstås, at afbildningen,

$$r/s \mapsto r/s,$$

der til en brøk r/s i $S^{-1}R$ lader svare brøken r/s i K , er en veldefineret, injektiv ringhomomorfi. Det er klart, at afbildningen er veldefineret (ja, hvorfor egentlig det?), og at den er en ringhomomorfi. Og den er injektiv, thi hvis r/s i $S^{-1}R$ afbildes på nul-elementet i K , så følger det af Lemma (3.4)(2) at $r = 0$, og så er brøken r/s nul-elementet i $S^{-1}R$. Altså er $S^{-1}R$ en delring af K . Da en delring af et legeme er et integritetsområde, er $S^{-1}R$ altså specielt et integritetsområde. \square

(3.7) Brøklegame. Legemet K , der fremkommer ved at lokalisere et integritetsområde R mht alle elementer forskellige fra 0, kaldes *brøklegame* for R . Bemærk, at den multiplikative delmængde netop er komplementærmængden til (0) , og at idealet (0) i R er et primideal, da R er et integritetsområde. Brøklegame fremkommer altså ved at lokalisere i primidealet (0) , jfr Definition (3.5)(2), og det kan betegnes $R_{(0)}$.

Brøklegame for ringen \mathbb{Z} af hele tal er legemet \mathbb{Q} af rationale tal.

Ringene $k[X_1, \dots, X_m]$ af polynomier i m variable over et legeme k er et integritetsområde. Det tilhørende brøklegame betegnes $k(X_1, \dots, X_m)$, og det kaldes legemet af *rationale funktioner* i m variable.

(3.8) Sætning. Lokalisering bevarer direkte sum.

Hermed menes: For en direkte sum $M_1 \oplus \cdots \oplus M_n$ af R -moduler findes en naturlig isomorfi af $S^{-1}R$ -moduler,

$$S^{-1}(M_1 \oplus \cdots \oplus M_n) \simeq S^{-1}M_1 \oplus \cdots \oplus S^{-1}M_n. \quad (3.8.1)$$

Specielt findes en naturlig isomorfi $S^{-1}(R^n) \simeq (S^{-1}R)^n$.

Bevis. En brøk på venstresiden af (3.8.1) har formen x/s , hvor $x = (x_1, \dots, x_n)$ er et n -sæt med $x_i \in M_i$. Ved isomorfien svarer denne brøk til n -sættet $(x_1/s, \dots, x_n/s)$ af brøker. Det skal vises, at denne tilordning er veldefineret, og at den herved definerede afbildning fra venstresiden til højresiden er en isomorfi.

Tilordningen er veldefineret, thi ved forlængelse med t af en brøk på venstresiden ændres n -sættet (x_1, \dots, x_n) til $t(x_1, \dots, x_n) = (tx_1, \dots, tx_n)$, og s ændres til ts . Det er derfor klart, at forlængelsen ikke ændrer det tilordnede sæt af brøker.

Det er let at se, at tilordningen er en homomorfi. Videre er den injektiv. Antag nemlig at en brøk x/s , hvor $x = (x_1, \dots, x_n)$, ved tilordningen afbildes på nul-elementet på højresiden. Dette betyder at hver koordinat x_i/s er nul-elementet i $S^{-1}M_i$. Af (3.4)(1) følger derfor, at der for hvert i findes et element $t_i \in S$ så at $t_i x_i = 0$. Når t er produktet af t_i 'erne gælder derfor, at $tx_i = 0$ for alle i . Men det betyder at $tx = 0$. Altså er $x/s = 0$.

Endelig er tilordningen surjektiv. Lad der nemlig være givet et element på højresiden, altså et n -sæt af brøker x_i/s_i . Efter forlængelse kan vi antage, at de optrædende s_i 'er er det samme element s i S . Den i 'te brøk kan nemlig forlænges med produktet af alle s_j 'erne for $j \neq i$, og så får den formen x_i/s , hvor $s = s_1 \cdots s_n$. Herefter er det klart, at det givne n -sæt tilhører billedmængden. \square

(3.9) Lemma. Lad $N \xrightarrow{\varphi} M \xrightarrow{\psi} P$ være en eksakt følge af R -lineære afbildninger. Da induceres en eksakt følge af $S^{-1}R$ -lineære afbildninger,

$$S^{-1}N \xrightarrow{S^{-1}\varphi} S^{-1}M \xrightarrow{S^{-1}\psi} S^{-1}P.$$

Bevis. Lad der være givet en brøk i $S^{-1}M$. Det skal vises, at brøken ved $S^{-1}\psi$ afbildes i nulbrøken i $S^{-1}P$, hvis og kun hvis brøken er billede ved $S^{-1}\varphi$ af en brøk i $S^{-1}N$.

„hvis“: Ifølge definitionen afbildes en brøk y/u i $S^{-1}N$ ved $S^{-1}\varphi$ på brøken $(\varphi y)/u$ i $S^{-1}M$. Antag altså at den givne brøk har formen $(\varphi y)/u$. Brøkens billede ved $S^{-1}\psi$ er da brøken $(\psi \varphi y)/u$ i $S^{-1}P$. Her er $\psi \varphi y = 0$, da den givne følge specielt var en nulfølge. Billedet er derfor $(\psi \varphi y)/u = 0/u$, som er nul-brøken i $S^{-1}P$.

„kun hvis“: Lad x/t være den givne brøk, og antag, at den ved $S^{-1}\psi$ afbildes i nul-brøken. Det antages altså at brøken $(\psi x)/t$ er nul-brøken i $S^{-1}P$. Ifølge Lemma (3.4)(1) findes så et element s i S , således at $s(\psi x) = 0$. Da ψ er lineær, følger det at $\psi(sx) = 0$. Da den givne følge var eksakt, slutes videre, at sx tilhører billedet for φ . Altså findes et element y i N , så at $\varphi y = sx$. Nu er y/st en brøk i $S^{-1}N$, og vi får

$$(S^{-1}\varphi)(y/st) = (\varphi y)/(st) = (sx)/(st) = x/t.$$

Den givne brøk x/t er altså billedet af brøken y/st i $S^{-1}N$.

Hermed er eksaktheden bevist. \square

(3.10) Isomorfiætning for brøkmøduler. Lad N være en undermødøl i R -mødøl M . Da er $S^{-1}N$ naturligt en undermødøl i $S^{-1}R$ -mødøl $S^{-1}M$, og for den tilhørende kvotientmødøl findes en isomorfi,

$$(S^{-1}M/S^{-1}N) \xrightarrow{\sim} S^{-1}(M/N). \quad (3.10.1)$$

Lad omvendt Q være en undermødøl i $S^{-1}R$ -mødøl $S^{-1}M$, og lad Q_0 betegne originalmængden af Q ved den kanoniske afbildning $M \rightarrow S^{-1}M$. Da er $Q = S^{-1}Q_0$.

Bevis. Følgen $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$ er eksakt. Ved gentagen anvendelse af Lemma (3.9) fås derfor, at den lokaliserede følge er eksakt,

$$0 \longrightarrow S^{-1}N \longrightarrow S^{-1}M \longrightarrow S^{-1}(M/N) \longrightarrow 0.$$

Men det betyder netop, at mødøl til venstre er en undermødøl i mødøl i midten og at mødøl til højre er den tilhørende kvotientmødøl.

Bemærk, at den injektive homomorfi $S^{-1}N \rightarrow S^{-1}M$ er den oplagte identifikation: brøken y/s i $S^{-1}N$, hvor $y \in N$ og $s \in S$, identificeres med brøken y/s i $S^{-1}M$.

Lad nu Q være en undermødøl i $S^{-1}M$. Ifølge definitionen består Q_0 da af de elementer $x \in M$ for hvilke $x/1$ tilhører Q . Det påstås, at

$$Q = S^{-1}Q_0.$$

„ \subseteq “: Lad x/s være en brøk i Q . Da Q er en undermødøl i $S^{-1}M$, er produktet $(s/1)(x/s)$ ligeledes element i Q . På den anden side er produktet lig med $(sx)/s = x/1$. Altså er $x/1$ element i Q , og følgelig er x element i Q_0 . Brøken x/s tilhører derfor $S^{-1}Q_0$.

„ \supseteq “: Betragt en brøk på højresiden, dvs en brøk af formen x/s , hvor $x \in Q_0$. Da er $x/1$ element i Q . Da Q er en undermødøl i $S^{-1}M$, er produktet $(1/s)(x/1)$ ligeledes element i Q . På den anden side er produktet lig med x/s . Altså er x/s element i Q .

Hermed er ligheden bevist, og beviset for Isomorfiætningen fuldført. \square

(3.11) Bemærkning. Det følger af Isomorfiætningens sidste resultat, at enhver undermødøl i $S^{-1}M$ er af formen $S^{-1}N$ for en passende undermødøl N af M .

Yderligere fremhæves følgende konsekvens: Betragt en *filtration* i M , dvs en voksende kæde af undermøduler: $(0) = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n = M$. Da fremkommer ved lokalisering en filtration i brøkmødøl,

$$(0) = S^{-1}F_0 \subseteq S^{-1}F_1 \subseteq \dots \subseteq S^{-1}F_n = S^{-1}M,$$

og for de successive kvotienter fås isomorfier $S^{-1}F_i/S^{-1}F_{i-1} \simeq S^{-1}(F_i/F_{i-1})$.

(3.12) Korollar. Lad \mathfrak{a} være et ideal i R . Da er $S^{-1}\mathfrak{a}$ et ideal i brøkringen $S^{-1}R$. Videre er $S^{-1}\mathfrak{a} = S^{-1}R$, hvis og kun hvis $\mathfrak{a} \cap S \neq \emptyset$. Lad endelig M være en R -mødøl. Da er $(S^{-1}\mathfrak{a})(S^{-1}M) = S^{-1}(\mathfrak{a}M) = \mathfrak{a}S^{-1}M$, og der findes en naturlig isomorfi,

$$S^{-1}M/(S^{-1}\mathfrak{a}S^{-1}M) \xrightarrow{\sim} S^{-1}(M/\mathfrak{a}M). \quad (3.12.1)$$

Bevis. Ifølge Isomorfiætningen (3.10) er $S^{-1}\mathfrak{a}$ en undermodul i $S^{-1}R$, altså et ideal i brøkringen $S^{-1}R$. Antag først, at $\mathfrak{a} \cap S \neq \emptyset$, altså at der findes et element a som tilhører både \mathfrak{a} og S . Det følger da at $1/1 = a/a$ tilhører $S^{-1}\mathfrak{a}$, og så er $S^{-1}\mathfrak{a} = S^{-1}R$. Antag omvendt, at $S^{-1}\mathfrak{a} = S^{-1}R$. Et-elementet $1/1$ vil da tilhøre $S^{-1}\mathfrak{a}$, så der findes $a \in \mathfrak{a}$ og $s \in S$ så at $1/1 = a/s$. Ligheden af brøkerne betyder, at parret (a, s) kan forlænges med $u \in S$ til et par (ua, us) der er af formen (t, t) , hvor $t \in S$. Da \mathfrak{a} er et ideal er $t = ua \in \mathfrak{a}$. Altså er t element i fællesmængden $\mathfrak{a} \cap S$, og fællesmængden er derfor ikke-tom, som ønsket.

Betragt nu en R -modul M . Produktet $\mathfrak{a}M$ betegner da undermodulen i M bestående af endelige summer af produkter ax , hvor $a \in \mathfrak{a}$ og $x \in M$. I modulen $S^{-1}M$ kan vi tilsvarende betragte produktet $S^{-1}\mathfrak{a} S^{-1}M$, og undermodulen $S^{-1}(\mathfrak{a}M)$, og videre produktet $\mathfrak{a}S^{-1}M$. Det påstås at disse tre undermoduler i $S^{-1}M$ er den samme.

Betragt et element i den første undermodul. Elementet er da en endelig sum af produkter $(a/s)(x/t)$, hvor $a \in \mathfrak{a}$ og $x \in M$. Af ligningen $(a/s)(x/t) = (ax)/(st)$ ses, at hvert af produkterne tilhører den anden undermodul. Følgelig er den første undermodul indeholdt i den anden.

Betragt et element i den anden undermodul. Da $(y_1 + y_2)/s = y_1/s + y_2/s$, er elementet en sum af brøker af formen $(ax)/s$, hvor $a \in \mathfrak{a}$ og $x \in M$. Af ligningen $(ax)/s = a(x/s)$ ses, at hver af brøkerne tilhører den tredje undermodul. Altså er den anden undermodul indeholdt i den tredje.

Betragt et element i den tredje undermodul. Elementet er da en endelig sum af produkter $a(x/s)$, hvor $a \in \mathfrak{a}$ og $x \in M$. Af ligningen $a(x/s) = (a/1)(x/s)$ ses, at hvert produkt tilhører den første undermodul. Følgelig er den tredje undermodul indeholdt i den første.

Hermed er vist, at de tre undermoduler er ens. Isomorfi (3.12.1) er nu blot isomorfi (3.10.1) for $N := \mathfrak{a}M$. \square

(3.13) Observation. Lad der være givet en ringhomomorfi $\theta: R \rightarrow R'$. Billedmængden θS er da en multiplikativ delmængde af R' . Lad videre N være en R' -modul. Som sådan kan N lokaliseres mht θS . På den anden side kan R' -modulen N opfattes som R -modul, idet produktet defineres ved $rx := \theta(r)x$. Som R -modul kan N altså lokaliseres mht S . Her kan man naturligt identificere,

$$S^{-1}N = (\theta S)^{-1}N,$$

idet en brøk x/t på venstresiden herved svarer til brøken $x/(\theta t)$ på højresiden. Mere præcist er $x/t \mapsto x/(\theta t)$ en veldefineret surjektiv afbildning, og den er injektiv. Er nemlig $x/(\theta t)$ nulbrøken i $(\theta S)^{-1}N$, så findes ifølge (3.4)(1) et element i θS , dvs et element af formen θs , hvor $s \in S$, således at $(\theta s)x = 0$. Med den definerede multiplikation er altså $sx = 0$, og så er den givne brøk x/t lig med nul-brøken.

Specielt fås for $N = R'$ en isomorfi,

$$S^{-1}R' = (\theta S)^{-1}R'.$$

Venstresiden, der a priori er en brøkmodul for R -modulen R' , kan altså opfattes som en brøkring for ringen R' . Videre er det let at se, at den inducerede afbildning $S^{-1}\theta: S^{-1}R \rightarrow S^{-1}R'$ er en ringhomomorfi.

(3.14) Bemærkning. Isomorfien (3.12.1) skal ses i lyset af observationen i (3.13). Lad $\theta: R \rightarrow R/\mathfrak{a}$ være den kanoniske homomorfi ind i kvotientringen. For $M = R$ fås af Korollar (3.12) følgende isomorfi af $S^{-1}R$ -moduler:

$$S^{-1}R/S^{-1}\mathfrak{a} \xrightarrow{\sim} S^{-1}(R/\mathfrak{a}). \quad (3.14.1)$$

Her kan højresiden ifølge (3.13) opfattes som brøkringen af R/\mathfrak{a} mht til den multiplikative delmængde θS , og venstresiden er kvotientringen af brøkringen $S^{-1}R$ modulo idealet $S^{-1}\mathfrak{a}$. Det er let at se, at isomorfien er en isomorfi af ringe. Isomorfien (3.14.1) udtrykker, at dannelse af kvotientring og dannelse af brøkring er ombyttelige operationer.

Også isomorfien (3.12.1) udtrykker en sådan ombyttelighed. Som bekendt gælder, at kvotienten $M/\mathfrak{a}M$ kan opfattes som R/\mathfrak{a} -modul, og højresiden i (3.12.1) kan ifølge (3.13) opfattes som lokaliseringen af denne modul mht θS . Højresiden af (3.12.1) er altså en modul over ringen $(\theta S)^{-1}(R/\mathfrak{a})$. Venstresiden kan tilsvarende opfattes som modul over ringen $S^{-1}R/S^{-1}\mathfrak{a}$. Som bemærket er de to ringe den samme ring, og isomorfien (3.12.1) udtrykker, at de to sider er isomorfe som moduler over denne ring.

Billedmængden θS i R/\mathfrak{a} består af restklasser modulo \mathfrak{a} af elementer i S . Det er derfor naturligt at betegne denne mængde med S/\mathfrak{a} . Isomorfien (3.14.1) og, mere generelt, isomorfien (3.12.1) er altså isomorfier,

$$S^{-1}R/S^{-1}\mathfrak{a} = (S/\mathfrak{a})^{-1}(R/\mathfrak{a}), \quad S^{-1}M/(S^{-1}\mathfrak{a}S^{-1}M) = (S/\mathfrak{a})^{-1}(M/\mathfrak{a}M).$$

(3.15) Opgaver.

1. Vis for et integritetsområde R med brøklege K , at for enhver „melletring“ $R \subseteq T \subseteq K$ kan man identificere brøkleget for T med K .
2. Lad S være en multiplikativ delmængde af R . Vis for $r \in R$, at brøken r/s er invertibel i $R[S^{-1}]$, hvis og kun hvis der findes et element $b \in R$ således, at $rb \in S$.
- U3 3. Lad M være en kommutativ gruppe, og altså en \mathbb{Z} -modul. Gør rede for, at $M_{(0)}$ er et vektorrum over \mathbb{Q} . Hvad bliver $M_{(0)}$, hvis M er en endelig gruppe.
- U3 4. Vis, at $\mathbb{Q} = \mathbb{Z}_{(p)}[p^{-1}]$.
- U3 5. Antag, at R er et integritetsområde og at S er en multiplikativ delmængde med $0 \notin S$. Vis, at hvis R er et PID, så er $R[S^{-1}]$ et PID. Vis, at hvis R er et UFD, så er $R[S^{-1}]$ et UFD.
- U3 6. En multiplikativ delmængde $S \subseteq R$ kan også opfattes som en multiplikativ delmængde af $R[X]$. Bestem en isomorfi: $R[X][S^{-1}] \xrightarrow{\sim} R[S^{-1}][X]$.
Gør rede for, at hvis R er et integritetsområde, så er de to ringe $R_{(0)}[X]$ og $R[X]_{(0)}$ ikke ens. Beskriv de to ringe udtrykt ved brøkleget K for R .
7. Lad R være et UFD med brøklege K . Lad \mathcal{P} være et repræsentantsystem for primelementerne på nær associering, og antag, at der for hvert $p \in \mathcal{P}$ er valgt et repræsentantsystem \mathcal{U}_p for restklasserne forskellige fra 0 i $R/(p)$. En brøk af formen u/p^n , hvor $p \in \mathcal{P}$ og $u \in \mathcal{U}_p$ (og $n \geq 1$) kaldes da – relativt til disse valg – en *stambrøk*.
Beskriv de naturlige valg af stambrøker, når $R = \mathbb{Z}$, når $R = \mathbb{C}[X]$, når $R = \mathbb{R}[X]$, og når $R = k[X]$ hvor k er et legeme.

Vis, at enhver brøk α i K entydigt kan skrives som et element i R plus en endelig sum af stambrøker med forskellige nævnere. [Vink: overvej, hvordan man for et givet $p \in \mathcal{P}$ bestemmer den største eksponent n for hvilken en stambrøk u/p^n forekommer i fremstillingen, – og hvordan man dernæst bestemmer tælleren u i denne stambrøk.]

8. Hvornår er $M \rightarrow S^{-1}M$ injektiv? Kan det indtræffe, at $M \rightarrow S^{-1}M$ er en isomorfi?

H1 9. Lad p være et primtal. Brøkringene $\mathbb{Z}_{(p)}$ og $\mathbb{Z}[1/p]$ er delringe af \mathbb{Q} . Bestem fællesmængden $\mathbb{Z}_{(p)} \cap \mathbb{Z}[1/p]$.

10. Lad R være et integritetsområde med brøklege $K := R_{(0)}$. Vis for enhver R -modul M , at $\text{rk } M = \dim M_{(0)}$, hvor dimensionen er dimensionen som vektorrum over K .

H2 11. Lad \mathfrak{a} og \mathfrak{b} være idealer i R , og lad $S \subseteq R$ være en multiplikativ delmængde. Vis, at $S^{-1}(\mathfrak{a} \cap \mathfrak{b}) = S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b}$.

U6 12. Betragt ringen \mathbb{Z} og heri et tal $n > 1$. Vis, at mængden $S = \{s \mid (s, n) = 1\}$ er en multiplikativ delmængde af \mathbb{Z} . Beskriv primidealene i brøkringen $S^{-1}\mathbb{Z}$, og de tilsvarende primidealere i \mathbb{Z} .

13. Betragt i R en multiplikativ delmængde S og et ideal \mathfrak{a} . Vis, at idealet $S^{-1}\mathfrak{a} \subseteq S^{-1}R$ er extensionen $\mathfrak{a}S^{-1}R$ af \mathfrak{a} til $S^{-1}R$.

U9 14. Betragt primidealere $\mathfrak{q} \subseteq \mathfrak{p}$. Hvilken relation er der mellem $M_{\mathfrak{q}}$ og $M_{\mathfrak{p}}$?

15. Lad S være en multiplikativ delmængde af R . Vis, at homomorfien $M \rightarrow S^{-1}M$ er injektiv, hvis og kun hvis $Z_R(M) \cap S = \emptyset$, hvor $Z_R(M)$ er mængden af nuldivisorer på M .

U9 16. Lad \mathfrak{q} være et \mathfrak{p} -primært ideal i en noethersk ring R , og lad $S \subseteq R$ være en multiplikativ delmængde, disjunkt med \mathfrak{p} . Vis, at \mathfrak{q} er kontraktionen af sin extension: $\mathfrak{q} = R \cap S^{-1}\mathfrak{q}$. [Vink: $R \cap S^{-1}\mathfrak{q}$ er kernen for den sammensatte homomorfi $R \rightarrow R/\mathfrak{q} \rightarrow S^{-1}(R/\mathfrak{q})$.]

H4 17. Vis i ringen $R := \mathbb{Z}_{(5)}$, at idealet (0) og potenserne (5^n) for $n = 0, 1, 2, \dots$ er samtlige idealere.

18. Lad $S \subseteq R$ være en multiplikativ delmængde med $0 \notin S$. Vis, at hvis R er et UFD så er $S^{-1}R$ et UFD. Hvad med PID?

19. Bestem for $f \in R$ en isomorfi (af R -algebraer) $R[X]/(fX - 1) \simeq R[1/f]$. [Vink: Lad ξ være restklassen af X modulo $(fX - 1)$. Vis, at de to afbildninger $P(\xi) \rightarrow P(1/f)$ og $a/f^n \rightarrow a\xi^n$ er veldefinerede og hinandens inverse.]

4. Primideal og maksimalideal.

(4.1) Definition. Et ideal m i ringen R , der er maksimalt blandt de ægte idealer i R , kaldes som bekendt et *maksimalideal*. Dette betyder, at m selv er et ægte ideal, dvs $m \subset R$, og at der for alle idealer a i R gælder følgende betingelse:

$$m \subseteq a \subset R \implies m = a.$$

Som bekendt gælder følgende karakterisering: *Et ideal m i R er et maksimalideal, hvis og kun hvis kvotientringen R/m er et legeme.*

Et ideal p i ringen R kaldes som bekendt et *primideal*, hvis $p \subset R$, og hvis der for alle elementer x, y i R gælder følgende betingelse:

$$xy \in p \implies x \in p \vee y \in p.$$

Som bekendt gælder følgende karakterisering: *Et ideal p i R er et primideal, hvis og kun hvis kvotientringen R/p er et integritetsområde.*

Da et legeme er et integritetsområde, følger det af karakteriseringerne, at ethvert maksimalideal er et primideal.

(4.2) Eksistenssætning. *Lad a være et ideal i R således, at $a \subset R$. Da findes i R et maksimalideal m , som omfatter a .*

Bevis. Ideen i beviset er følgende: Enten er a et maksimalideal (og så er vi færdige), eller også findes et ideal a_1 forskelligt fra R således at $a \subset a_1$. Her er enten a_1 et maksimalideal (og så er vi færdige), eller også findes et ideal a_2 forskelligt fra R således at $a_1 \subset a_2$. Således fortsættes. Enten stopper processen efter endelig mange skridt (og så har vi fundet det ønskede maksimalideal), eller også fås en uendelig kæde af idealer,

$$a \subset a_1 \subset a_2 \subset \dots$$

Noetherske ringe er karakteriseret ved at en sådan kæde ikke kan eksistere. Hvis R er noethersk, stopper processen altså efter endelig mange skridt med det ønskede maksimalideal. Hvis R ikke er noethersk, så kræves der yderligere aksiomer fra mængdelæren (Zorn's Lemma) for at vise, at ideen kan udbygges til et bevis for eksistensen af det ønskede maksimalideal. \square

(4.3) Bemærkning. Det følger af Sætningen, at der i enhver ring R forskellig fra nul-ringen findes maksimalideal. Specielt findes altså primideal i enhver ring, der ikke er nul-ringen.

(4.4) Lokal ring. En ring R kaldes en *lokal ring*, hvis der findes et ideal $m \subset R$, som er det største blandt de ægte idealer i R , dvs opfylder, at ethvert ideal forskelligt fra R er indeholdt i m . Det er klart, at et sådant ideal m må være et maksimalideal i R (og endda det eneste maksimalideal i R); den tilsvarende kvotient R/m kaldes *restklasselegemet* for den lokale ring R . For en R -modul M er kvotienten M/mM så naturligt en R/m -modul, dvs et vektorrum over restklasselegemet R/m .

(4.5) Observation. Det følger af Sætning (4.2), at R er en lokal ring, hvis og kun hvis R har præcis ét maksimalideal.

Det er klart, at et element r i en ring R er invertibelt, hvis og kun hvis hovedidealet Rr er hele ringen R . I en lokal ring med maksimalidealet \mathfrak{m} gælder derfor, at alle elementer i komplementærmængden til \mathfrak{m} er invertible.

(4.6) Nakayama's Lemma. *Lad R være en lokal ring med maksimalidealet \mathfrak{m} . Lad videre M være en endeligt frembragt R -modul. Hvis $M = \mathfrak{m}M$, så er $M = 0$.*

Bevis. Antag, at elementerne v_1, \dots, v_m frembringer M . Hvert element v i M er altså en R -linearkombination $v = \sum r_i v_i$. Det er klart, at undermodulen $\mathfrak{m}M$ består af de elementer v , der tilfredsstillende en ligning af formen $v = \sum a_i v_i$, hvor $a_i \in \mathfrak{m}$. En sådan ligning kan skrives som et matrixprodukt,

$$v = (v_1, \dots, v_m)\alpha,$$

hvor α er en søjle af koefficienter i \mathfrak{m} . Ifølge forudsætningen findes for alle elementer i M , og specielt for frembringerne v_i , en sådan ligning. Ligningerne svarende til de m frembringere kan under ét skrives som en matrixligning,

$$(v_1, \dots, v_m) = (v_1, \dots, v_m)\alpha,$$

hvor α nu er en $m \times m$ -matrix med koefficienter i \mathfrak{m} . Den sidste matrixligning kan omformes til ligningen,

$$(v_1, \dots, v_m)(1_m - \alpha) = 0,$$

hvor 1_m betegner enhedsmatricen. Betragt nu determinanten $d := \det(1_m - \alpha)$ i R . Af matrixligningen følger ved hjælp af Cramer's formler, at $(v_1, \dots, v_m)d = 0$. Determinanten d annullerer derfor alle v_i 'erne, og dermed også enhver linearkombination af v_i 'erne. Da v_i 'erne var et frembringersystem for M , vil d altså annullere alle elementer i M . På den anden side har matricen α koefficienter i \mathfrak{m} , så determinanten $d = \det(1_m - \alpha)$ har formen $d = 1 + a$, hvor $a \in \mathfrak{m}$. Heraf følger, at $d \notin \mathfrak{m}$, thi ellers var $1 = (1 + a) - a \in \mathfrak{m}$. Da R er lokal, følger det videre, at d er invertibel i R . Da d er invertibel og annullerer alle elementer i M , må M være nul-modulen. \square

(4.7) Korollar. *Lad R være en lokal ring med maksimalidealet \mathfrak{m} , og lad M være en endeligt frembragt R -modul. Hvis et sæt (v_1, \dots, v_n) af elementer v_i i M opfylder, at restklasserne \hat{v}_i modulo $\mathfrak{m}M$ frembringer kvotientmodulen $M/\mathfrak{m}M$, da vil v_i 'erne frembringe M .*

Bevis. Sæt $F := R^n$ og lad $\varphi: F \rightarrow M$ være den lineære afbildning svarende til v_i 'erne, dvs afbildningen,

$$(r_1, \dots, r_n) \mapsto r_1 v_1 + \dots + r_n v_n.$$

Det skal vises, at afbildningen φ er surjektiv. Idet Q betegner kokernen for φ skal det altså vises, at $Q = 0$. Da M er endeligt frembragt, er Q endeligt frembragt. Videre har vi den eksakte følge $F \rightarrow M \rightarrow Q \rightarrow 0$, og heraf fås umiddelbart den eksakte følge,

$$F/\mathfrak{m}F \rightarrow M/\mathfrak{m}M \rightarrow Q/\mathfrak{m}Q \rightarrow 0.$$

30. marts 2007

Forudsætningerne medfører, at afbildningen $F/mF \rightarrow M/mM$ er surjektiv. Af eksaktheden følger derfor, at $Q/mQ = 0$. Af Nakayama's Lemma følger endelig, at $Q = 0$. Hermed er sætningen bevist. \square

(4.8) Lemma. *Antag, at primidealet \mathfrak{p} omfatter et produkt $\alpha_1 \cdots \alpha_n$ af n idealer α_i . Da vil \mathfrak{p} omfatte et af α_i 'erne.*

Bevis. Det antages, at $\alpha_1 \cdots \alpha_n \subseteq \mathfrak{p}$, og det skal vises, at der findes et i så at $\alpha_i \subseteq \mathfrak{p}$. Antag, indirekte, at et sådant i ikke fandtes. Da findes for hvert i et element $a_i \in \alpha_i$, så at $a_i \notin \mathfrak{p}$. Betragt produktet $a = a_1 \cdots a_n$. På den ene side er a element i produktet af α_i 'erne. På den anden side er a ikke element i \mathfrak{p} , da \mathfrak{p} er et primideal og ingen af faktorerne tilhørte \mathfrak{p} . Men det er i modstrid med at produktet af α_i 'erne er indeholdt i \mathfrak{p} . \square

(4.9) Lemma. *Antag, at idealet α er indeholdt i en forening $\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$ af n primidealer \mathfrak{p}_i . Da er α indeholdt i et af \mathfrak{p}_i 'erne.*

Bevis. Betragt først følgende relationer mellem idealer:

$$\alpha \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n, \quad (1)$$

$$\alpha \cap \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{n-1} \not\subseteq \mathfrak{p}_n, \quad (2)$$

$$\alpha \not\subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_{n-1}. \quad (3)$$

Det påstås, at disse tre relationer ikke samtidigt kan være sande. Antag, indirekte, at alle tre relationer er opfyldt. Vælg så et element $a \in \alpha$ som tilhører venstresiden i (2) og ikke højresiden, og et element $b \in \alpha$, som tilhører venstresiden i (3) og ikke højresiden. Da er

$$a \in \mathfrak{p}_i \text{ for } i = 1, \dots, n-1 \text{ og } a \notin \mathfrak{p}_n, \quad (4)$$

$$b \notin \mathfrak{p}_i \text{ for } i = 1, \dots, n-1 \text{ og } b \in \mathfrak{p}_n, \quad (5)$$

idet den sidste relation i (5) følger af de $n-1$ foregående da (1) gælder. Elementerne a og b er valgt i α , så $a+b \in \alpha$. Af (1) følger derfor, at $a+b$ tilhører et af \mathfrak{p}_i 'erne. Men nu opnås den ønskede modstrid. Hvis nemlig $a+b \in \mathfrak{p}_i$ med $i < n$, så følger af (4) at $b = (a+b) - a \in \mathfrak{p}_i$, i modstrid med (5). Og hvis $a+b \in \mathfrak{p}_n$, så følger af (5) at $a = (a+b) - b \in \mathfrak{p}_n$, i modstrid med (4).

Beviset for Lemma'et føres nu ved induktion efter n . Påstanden er triviell for $n = 1$, og det kan derfor antages, at $n > 1$ og at påstanden gælder for $n-1$ primidealer. Ifølge forudsætningen gælder relationen (1). Af det lige viste følger derfor, at en af relationerne (2) og (3) er falsk.

Antag, at (3) er falsk. Det følger da umiddelbart af induktionsforudsætningen, at α er indeholdt i et \mathfrak{p}_i med $i < n$.

Antag endelig, at (2) er falsk. Fællesmængden på venstresiden i (2) omfatter produktet $\alpha \mathfrak{p}_1 \cdots \mathfrak{p}_{n-1}$. Da (2) er antaget falsk, gælder derfor relationen:

$$\alpha \mathfrak{p}_1 \cdots \mathfrak{p}_{n-1} \subseteq \mathfrak{p}_n.$$

30. marts 2007

Af Lemma (4.8) følger, at en af faktorerne på venstresiden er indeholdt i \mathfrak{p}_n . Hvis faktoren α er indeholdt i \mathfrak{p}_n , så er den ønskede inklusion opnået. Hvis faktoren \mathfrak{p}_i for $i < n$ er indeholdt i \mathfrak{p}_n , så kan \mathfrak{p}_i undværes i foreningsmængden på højresiden af (1); i dette tilfælde er α indeholdt i en forening af $n - 1$ af \mathfrak{p}_j 'erne, og så følger den ønskede inklusion af induktionsforudsætningen.

Hermed er den ønskede inklusion nået i alle tilfælde. \square

(4.10) Kontraktion og ekstension. Lad $\theta: R \rightarrow R'$ være en ringhomomorfi. For hvert ideal \mathfrak{b} i R' er originalmængden $\theta^{-1}(\mathfrak{b})$ øjensynlig et ideal i R , kaldet *kontraktionen* af \mathfrak{b} . Hvis θ er inklusionen af en delring R af R' , er kontraktionen blot fællesmængden $R \cap \mathfrak{b}$. Ofte bruges betegnelsen $R \cap \mathfrak{b}$ for kontraktionen også når θ ikke er en inklusionsafbildning.

Lad omvendt \mathfrak{a} være et ideal i R . Det er let at se, at produktet $\mathfrak{a}R'$ så er et ideal i ringen R' . Det kaldes *ekstensionen* af idealet \mathfrak{a} .

(4.11) Observation. Kontraktionen $\theta^{-1}(\mathfrak{b})$ af et ideal \mathfrak{b} i R' er øjensynlig kernen for den sammensatte ringhomomorfi $R \rightarrow R' \rightarrow R'/\mathfrak{b}$. Af isomorfisætningen for ringe følger derfor, at kvotienten $R/\theta^{-1}(\mathfrak{b})$ er isomorf med en delring af R'/\mathfrak{b} . Heraf følger umiddelbart, at et primideal i R' kontraheres til et primideal i R .

Derimod er kontraktionen af et maksimalideal i R' ikke nødvendigvis et maksimalideal i R , og ekstension af et primideal er ikke nødvendigvis et primideal.

(4.12) Kvotientprincip. Lad \mathfrak{a} være et ideal i R , og lad $\theta: R \rightarrow R/\mathfrak{a}$ betegne den kanoniske afbildning på kvotientringen. Da vil ekstension og kontraktion,

$$\mathfrak{p} \mapsto \mathfrak{p}/\mathfrak{a} \quad \text{og} \quad \mathfrak{q} \mapsto \theta^{-1}(\mathfrak{q}),$$

definere en bijektiv, ordenstro forbindelse mellem på den ene side de primidealer \mathfrak{p} i R , som omfatter \mathfrak{a} , og på den anden side samtlige primidealer \mathfrak{q} i R/\mathfrak{a} . Hvis \mathfrak{p} og \mathfrak{q} svarer til hinanden ved denne bijektive forbindelse, da er de tilhørende kvotientringe isomorfe. Endelig findes, for hver modul M og hvert primideal \mathfrak{p} der omfatter \mathfrak{a} , en naturlig isomorfi,

$$M_{\mathfrak{p}}/\mathfrak{a}M_{\mathfrak{p}} \simeq (M/\mathfrak{a}M)_{\mathfrak{p}/\mathfrak{a}}. \quad (4.12.1)$$

Bevis. Det er en del af Noether's anden Isomorfisætning, at ekstension og kontraktion, som defineret ovenfor, er en bijektiv forbindelse mellem idealer i R , som indeholder \mathfrak{a} , og samtlige idealer i R/\mathfrak{a} . Det skal altså vises, at primideal svarer til primideal ved denne forbindelse. Men det følger af Noether's anden Isomorfi: for idealer, der svarer til hinanden ved den bijektive forbindelse, er de tilhørende kvotientringe isomorfe. Den ene er altså et integritetsområde, hvis og kun hvis den anden er. Desuden følger, at for tilsvarende primidealer er de tilhørende kvotientringe isomorfe.

Endelig er den naturlige isomorfi (4.12.1) blot isomorfien (3.12.1) anvendt på $S := R \setminus \mathfrak{p}$. Som nævnt i Bemærkning (3.14) kan højresiden i (3.12.1) nemlig fås ved at lokalisere $M/\mathfrak{a}M$ som R/\mathfrak{a} -modul mht billedet θS ; og det er klart, at dette billede netop er komplementærmængden i R/\mathfrak{a} til primidealet $\mathfrak{p}/\mathfrak{a}$. \square

(4.14) Lokaliseringsprincip. Lad S være en multiplikativ delmængde af R , og betragt den kanoniske homomorfi $R \rightarrow S^{-1}R$. Da vil ekstension og kontraktion,

$$\mathfrak{p} \mapsto S^{-1}\mathfrak{p} \quad \text{og} \quad \mathfrak{q} \mapsto R \cap \mathfrak{q},$$

definere en bijektiv, ordenstro forbindelse mellem på den ene side de primidealer \mathfrak{p} i R , som er disjunkte med S , og på den anden side samtlige primidealer \mathfrak{q} i $S^{-1}R$. For et primideal \mathfrak{p} disjunkt med S gælder, at kvotienten $S^{-1}R/S^{-1}\mathfrak{p}$ er isomorf med lokaliseringen af integritetsområdet R/\mathfrak{p} mht billedet af S i R/\mathfrak{p} . Endelig findes, for hver modul M og hvert primideal \mathfrak{p} der er disjunkt med S , en naturlig isomorfi,

$$(S^{-1}M)_{S^{-1}\mathfrak{p}} \simeq M_{\mathfrak{p}}. \quad (4.14.1)$$

Bevis. Det er klart, at idealet $S^{-1}\mathfrak{p}$ netop er ekstensionen af \mathfrak{p} . Det skal vises, at kontraktion af et primideal \mathfrak{q} er et primideal $\mathfrak{q}_0 = R \cap \mathfrak{q}$ disjunkt med S , og at ekstension af et primideal \mathfrak{p} , der er disjunkt med S , er et primideal $S^{-1}\mathfrak{p}$. Videre skal det vises, at kontraktion og ekstension er „hinandens inverse“, altså at $S^{-1}\mathfrak{q}_0 = \mathfrak{q}$ og $R \cap S^{-1}\mathfrak{p} = \mathfrak{p}$. Idet \bar{S} betegner billedmængden af S ved den kanoniske homomorfi $R \rightarrow R/\mathfrak{p}$, skal det endelig vises, at $S^{-1}R/S^{-1}\mathfrak{p}$ er isomorf med $\bar{S}^{-1}(R/\mathfrak{p})$.

Betragt først i brøkringen $S^{-1}R$ et primideal \mathfrak{q} . Det er klart, at kontraktionen \mathfrak{q}_0 er et primideal i R . Videre følger det af Isomorfiætning for brøkmøduler (3.10), at $\mathfrak{q} = S^{-1}\mathfrak{q}_0$. Af Korollar til Isomorfiætningen (3.12) følger nu videre, at $\mathfrak{q}_0 \cap S = \emptyset$.

Betragt omvendt i R et primideal \mathfrak{p} , der er disjunkt med S . Af Isomorfiætningen for brøkmøduler (3.10) fås nu en naturlig isomorfi,

$$S^{-1}R/S^{-1}\mathfrak{p} \xrightarrow{\sim} S^{-1}(R/\mathfrak{p}).$$

Som nævnt i Observation (3.13) er højresiden netop brøkringen $\bar{S}^{-1}(R/\mathfrak{p})$, og isomorfien er isomorfi af ringe. Hermed er den anførte isomorfi mellem ringe etableret. Forudsætningen om at $S \cap \mathfrak{p} = \emptyset$ betyder præcis, at \bar{S} ikke indeholder nul-elementet i R/\mathfrak{p} . Højresiden er derfor brøkringen af et integritetsområde mht en multiplikativ delmængde, der ikke indeholder 0. Af Sætning (3.6) følger derfor, at højresiden er et integritetsområde. Altså er venstresiden et integritetsområde. Følgelig er $S^{-1}\mathfrak{p}$ et primideal i ringen $S^{-1}R$.

Betragt videre kontraktionen $R \cap S^{-1}\mathfrak{p}$. Kontraktionen er kernen for den sammensatte homomorfi $R \rightarrow S^{-1}R \rightarrow S^{-1}R/S^{-1}\mathfrak{p}$. Det er klart, at denne homomorfi er den samme som den sammensatte homomorfi $R \rightarrow R/\mathfrak{p} \rightarrow \bar{S}^{-1}(R/\mathfrak{p})$. Kontraktionen er følgelig kernen for denne sidste sammensatte homomorfi. Her er homomorfien $R/\mathfrak{p} \rightarrow \bar{S}^{-1}(R/\mathfrak{p})$ injektiv, jfr Sætning (3.6). Kontraktionen er derfor kernen for homomorfien $R \rightarrow R/\mathfrak{p}$. Følgelig er kontraktionen lig med \mathfrak{p} .

Hermed er vist, at kontraktion og ekstension er „hinandens inverse“ på de betragtede mængder af primidealer. Den anførte isomorfi mellem ringe blev etableret undervejs.

Betragt endelig en R -modul M og et primideal \mathfrak{p} disjunkt med S . Venstresiden af (4.14.1) består af brøker, hvor tæller og nævner er brøker, af formen

$$\frac{x/s_1}{t/s_2}. \quad (*)$$

Tælleren x/s_1 tilhører $S^{-1}M$, og nævneren t/s_2 tilhører komplementærmængden til primidealet $S^{-1}\mathfrak{p}$. Højresiden af (4.14.1) består af brøker x/t , hvor nævneren t tilhører komplementærmængden til \mathfrak{p} . Det er nu let at vise, at forskriften, der til en brøk x/t på højresiden af (4.14.1) lader svare brøken $(x/1)/(t/1)$ på venstresiden, er en veldefineret injektiv homomorfi. For at vise, at denne homomorfi er surjektiv betragtes en brøk $(*)$. Brøken $s_1s_2/1$ tilhører ikke ekstensionen $S^{-1}\mathfrak{p}$, thi ellers ville s_1s_2 tilhøre kontraktionen \mathfrak{p} , i modstrid med at s_1s_2 tilhører S som er disjunkt med \mathfrak{p} . Følgelig gælder i $(S^{-1}M)_{S^{-1}\mathfrak{p}}$ ligningen,

$$\frac{x/s_1}{t/s_2} = \frac{(s_1s_2/1)(x/s_1)}{(s_1s_2/1)(t/s_2)} = \frac{s_2x/1}{s_1t/1},$$

og heraf følger surjektiviteten. \square

(4.15) Bemærkning. To specialtilfælde af Lokaliseringsprincippet skal fremhæves:

(1) Lad f være et element i R . Der er da en bijektiv forbindelse mellem samtlige primidealer i brøkringen R_f , og de primidealer i R , som ikke indeholder f . Dette følger af at brøkringen R_f er lokaliseringen af R mht mængden af potenser f^i ; et primideal er øjensynlig disjunkt med denne mængde, hvis og kun hvis det ikke indeholder f .

(2) Lad \mathfrak{p} være et primideal i R . Der er da en bijektiv forbindelse mellem samtlige primidealer i brøkringen $R_{\mathfrak{p}}$, og de primidealer i R , som er indeholdt i \mathfrak{p} . Dette følger af at brøkringen $R_{\mathfrak{p}}$ er lokaliseringen af R mht til komplementærmængden $S := R \setminus \mathfrak{p}$; et primideal er disjunkt med denne komplementærmængde, hvis og kun hvis det er indeholdt i \mathfrak{p} .

Yderligere gælder, at brøkringen $R_{\mathfrak{p}}$ er en lokal ring med maksimalidealet $\mathfrak{p}R_{\mathfrak{p}}$. Et ægte ideal i brøkringen, dvs et ideal forskelligt fra $R_{\mathfrak{p}}$, har nemlig formen $\mathfrak{a}R_{\mathfrak{p}}$, hvor \mathfrak{a} er et ideal i R disjunkt med S , jfr Korollar (3.12). At \mathfrak{a} er disjunkt med S betyder at $\mathfrak{a} \subseteq \mathfrak{p}$. Altså er $\mathfrak{a}R_{\mathfrak{p}} \subseteq \mathfrak{p}R_{\mathfrak{p}}$. Ethvert ægte ideal er altså indeholdt i $\mathfrak{p}R_{\mathfrak{p}}$.

Endelig gælder, at restklasselegemet $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ er isomorft med brøklegemet for integritetsområdet R/\mathfrak{p} . Af beskrivelsen i Lokaliseringsprincippet følger nemlig, at restklasselegemet er brøkringen for R/\mathfrak{p} mht til billedet \bar{S} af S , og da S er komplementærmængden til \mathfrak{p} , består \bar{S} netop af elementerne forskellige fra 0 i R/\mathfrak{p} .

(4.16) Sætning. Lad \mathfrak{m} være et maksimalideal i R . Den lokale ring $R_{\mathfrak{m}}$ har da maksimalidealet $\mathfrak{m}R_{\mathfrak{m}}$, og dens restklasselegeme er isomorft med legemet R/\mathfrak{m} . Mere generelt findes for hver R -modul M og $i \geq 1$ en naturlig isomorfi,

$$M/\mathfrak{m}^i M \xrightarrow{\sim} M_{\mathfrak{m}}/\mathfrak{m}^i M_{\mathfrak{m}}. \quad (4.16.1)$$

Bevis. Den første påstand følger af Lokaliseringsprincippet, jfr Bemærkning (4.15). Restklasselegemet $R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}}$ er nemlig isomorft med brøklegemet for kvotienten R/\mathfrak{m} . Da \mathfrak{m} er et maksimalideal, er denne sidste kvotient et legeme, og altså lig med sit brøklegeme.

Lad nu S betegne komplementærmængden $S := R \setminus \mathfrak{m}$. Højresiden i (4.16.1) er da isomorf med brøkmødule $S^{-1}(M/\mathfrak{m}^i M)$, jfr Korollar (3.12). Det er således påstanden, at den kanoniske homomorfi $M/\mathfrak{m}^i M \rightarrow S^{-1}(M/\mathfrak{m}^i M)$ er en isomorfi.

Ifølge Lemma (3.4)(2) er det nok at vise for hvert element $s \in S$, at multiplikation med s er bijektiv på $M/\mathfrak{m}^i M$. Da s ikke tilhører \mathfrak{m} og \mathfrak{m} er et maksimalideal, er $Rs + \mathfrak{m} = R$. Der findes altså elementer $r \in R$ og $m \in \mathfrak{m}$ så at $1 = rs + m$. Opløft $rs + m$ til i 'te potens og anvend den distributive lov. Herved fås en sum af led, hvoraf ét led er m^i og hvor de øvrige led indeholder s som faktor. Idet s sættes uden for parentes i disse øvrige led, fremkommer en ligning af formen,

$$1 = r_i s + m^i.$$

Heraf fremgår det ønskede. Potensen m^i tilhører jo \mathfrak{m}^i , så ligningen viser, at der for alle x i M gælder, at $r_i s x = s r_i x$ er kongruent med x modulo $\mathfrak{m}^i M$. I kvotienten $M/\mathfrak{m}^i M$ er multiplikation med r_i derfor invers til multiplikation med s . \square

(4.17) Komaksimale idealer. To idealer \mathfrak{a} og \mathfrak{b} i R kaldes *komaksimale*, hvis summen $\mathfrak{a} + \mathfrak{b}$ er hele ringen R . Øjensynlig er betingelsen ækvivalent med at et-elementet 1 tilhører $\mathfrak{a} + \mathfrak{b}$, altså ækvivalent med at der eksisterer en fremstilling,

$$1 = a + b \quad \text{hvor } a \in \mathfrak{a}, b \in \mathfrak{b}.$$

(4.18) Lemma. Lad \mathfrak{a} , \mathfrak{b} og \mathfrak{c} være idealer i R . (1) Hvis \mathfrak{a} og \mathfrak{b} er komaksimale, så er fællesmængden lig med produktet, dvs $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

(2) Hvis \mathfrak{a} er komaksimal med \mathfrak{b} og komaksimal med \mathfrak{c} , så er \mathfrak{a} komaksimal med produktet $\mathfrak{b}\mathfrak{c}$.

Bevis. Øjensynlig gælder for idealer \mathfrak{a} , \mathfrak{b} og \mathfrak{c} den distributive lov, $\mathfrak{c}(\mathfrak{a} + \mathfrak{b}) = \mathfrak{c}\mathfrak{a} + \mathfrak{c}\mathfrak{b}$.

Det er klart, at (1) er en konsekvens af følgende relationer mellem idealer:

$$\mathfrak{a} \cap \mathfrak{b} = (\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) = (\mathfrak{a} \cap \mathfrak{b})\mathfrak{a} + (\mathfrak{a} \cap \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}.$$

Den første relation gælder, da \mathfrak{a} og \mathfrak{b} er komaksimale, den anden følger af den distributive lov, den tredje er oplagt idet $\mathfrak{a} \cap \mathfrak{b}$ er indeholdt i både \mathfrak{a} og \mathfrak{b} , og den sidste relation gælder for vilkårlige idealer.

Af relationerne $R = (\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) = \mathfrak{a}\mathfrak{a} + \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{a} + \mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a} + \mathfrak{b}\mathfrak{c}$ følger tilsvarende påstanden i (2). \square

(4.19) Observation. Af definitionen følger, at to forskellige maksimalideal \mathfrak{m}_1 og \mathfrak{m}_2 er komaksimale. Da idealerne er forskellige, er summen $\mathfrak{m}_1 + \mathfrak{m}_2$ nemlig effektivt større end (fx) \mathfrak{m}_1 , og da \mathfrak{m}_1 er et maksimalideal, følger det at $\mathfrak{m}_1 + \mathfrak{m}_2 = R$. Ved gentagen anvendelse af Lemma (4.18)(2) følger det nu, at vilkårlige potenser $\mathfrak{m}_1^{n_1}$ og $\mathfrak{m}_2^{n_2}$ er komaksimale.

(4.20) Den Kinesiske Restklassesætning. Lad $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ være et sæt af parvis komaksimale idealer. Da er $\mathfrak{a}_1 \cdots \mathfrak{a}_r = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r$, og der findes en naturlig isomorfi,

$$R/\mathfrak{a}_1 \cdots \mathfrak{a}_r \xrightarrow{\sim} R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_r.$$

Bevis. For $i = 1, \dots, r$ betegnes med \mathfrak{a}'_i produktet af \mathfrak{a}_j 'erne for $j \neq i$. Ved gentagen anvendelse af Lemma (4.18)(2) følger det, at \mathfrak{a}_i er komaksimal med \mathfrak{a}'_i . Videre følger ligheden $\mathfrak{a}_1 \cdots \mathfrak{a}_r = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r$ af Lemma (4.18)(1) ved induktion.

Den søgte isomorfi fås ved at betragte den kanoniske afbildning, der til hvert element x i R lader svare r -sættet bestående af restklasserne af x modulo hvert af de r idealer \mathfrak{a}_i . Denne kanoniske afbildning er øjensynlig en ringhomomorfi,

$$R \rightarrow R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_r,$$

hvor højresiden er *produktringen*, med koordinatvise kompositioner. Kernen for denne ringhomomorfi er fællesmængden af \mathfrak{a}_i 'erne, der ifølge det allerede viste er lig med produktet af \mathfrak{a}_i 'erne. For at vise, at denne ringhomomorfi inducerer en isomorfi som ønsket, er det derfor nok at vise, at den er surjektiv.

Videre er det, da afbildningen er en ringhomomorfi, nok at vise for $i = 1, \dots, r$, at det specielle r -sæt, der har restklassen af 1 modulo \mathfrak{a}_i på den i 'te plads og 0 på de øvrige pladser, tilhører billedet. Hertil bemærkes, at da \mathfrak{a}_i og \mathfrak{a}'_i er komaksimale, findes elementer $a_i \in \mathfrak{a}_i$ og $a'_i \in \mathfrak{a}'_i$ således at $1 = a_i + a'_i$. Betragt elementet a'_i . Det tilhører \mathfrak{a}'_i og dermed alle \mathfrak{a}_j 'erne for $j \neq i$. Elementets restklasse modulo \mathfrak{a}_j er derfor lig med 0 for $j \neq i$. Desuden er $a'_i - 1 = -a_i$ element i \mathfrak{a}_i , så er a'_i kongruent med 1 modulo \mathfrak{a}_i . Restklassen modulo \mathfrak{a}_i af elementet a'_i er altså lig med restklassen af 1.

Hermed er vist, at elementet a'_i ved den kanoniske afbildning afbildes på det specielle r -sæt, som ønsket. \square

(4.21) Eksempel. Den klassiske anvendelse af den kinesiske restklassesætning er på ringen \mathbb{Z} af hele tal. Her er alle idealer hovedideal, dvs af formen (n) , hvor $n \geq 0$. To hovedideal (n_1) og (n_2) er komaksimale, hvis og kun hvis tallene n_1 og n_2 er primiske, dvs ikke har fælles primdivisorer. Dette følger af at idealsummen $(n_1) + (n_2)$ øjensynlig er hovedidealet (d) , hvor d er den største fælles divisor for n_1 og n_2 ; idealsummen er således hele ringen \mathbb{Z} , hvis og kun hvis $d = 1$ er den største fælles divisor for n_1 og n_2 .

Heraf fås den klassiske restklassesætning: For givne parvis primiske tal n_1, \dots, n_r og $n := n_1 \cdots n_r$ er

$$\mathbb{Z}/(n) \xrightarrow{\sim} \mathbb{Z}/(n_1) \times \cdots \times \mathbb{Z}/(n_r).$$

(4.22) Opgaver.

- U3 1. Vis, for et primtal p , at idealet (p, X) i $\mathbb{Z}[X]$ er et maksimalideal, og beskriv legemet $\mathbb{Z}[X]/(p, X)$. [Vink: Bestem en surjektiv ringhomomorfi ind i „det rigtige“ legeme, med det givne ideal som kerne.]
- U3 2. Vis, at idealet (X, Y) i $\mathbb{Q}[X, Y]$ er et maksimalideal.
- U3 3. Vis, at idealerne $(0) \subset (X) \subset (X, Y) \subset (X, Y, Z)$ i $\mathbb{Z}[X, Y, Z]$ er primideal. Er der maksimalideal imellem dem?
4. Vis, at hvis \mathfrak{a} er en fællesmængde af primideal, så er $\mathfrak{a} = \text{Rad}(\mathfrak{a})$.
- H1 5. Vis, at en endelig fællesmængde $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ af primideal kun kan være et primideal, hvis et \mathfrak{p}_i er indeholdt i de øvrige.

6. Vis, at hvis en familie af primidealer \mathfrak{p}_i , $i \in I$, er totalt ordnet (dvs, at for alle i, j er $\mathfrak{p}_i \subseteq \mathfrak{p}_j$ eller $\mathfrak{p}_j \subseteq \mathfrak{p}_i$), så er fællesmængden $\bigcap_i \mathfrak{p}_i$ igen et primideal.

U7 7. Vis, at $\text{Rad}(0)$ er delmængden bestående af alle nilpotente elementer i R . *Vis, at

$$\text{Rad}(0) = \bigcap \mathfrak{p},$$

hvor højresiden er fællesmængden af alle primidealer i R . [Vink: For at vise inklusionen „ \supseteq “ skal det vises, at hvis f ikke er nilpotent, så findes et primideal \mathfrak{p} med $f \notin \mathfrak{p}$. Anvend hertil eksistensen af et primideal (endda et maksimalideal) i ringen R_f .]

8. Lad I være en mængde. Betragt ringen $R := \mathbb{F}_2^I$ af alle funktioner $I \rightarrow \mathbb{F}_2$. Vis, at ved $f \mapsto f^{-1}(0)$ bestemmes en bijektiv afbildning af R på mængden af alle delmængder af I ; den inverse afbildning knytter til en delmængde $F \subseteq I$ den karakteristiske funktion for komplementærmængden til F . Herved svarer delmængder $\mathfrak{a} \subseteq R$ til systemer af delmængder $\mathcal{F} \subseteq \mathcal{P}(I)$. Vis, at $\mathfrak{a} \subseteq R$ er et ægte ideal, hvis og kun hvis $\mathcal{F} \subseteq \mathcal{P}(I)$ er et filter på I , dvs opfylder følgende: (1) $G \supseteq F \in \mathcal{F} \implies G \in \mathcal{F}$, og (2) $F_1, F_2 \in \mathcal{F} \implies F_1 \cap F_2 \in \mathcal{F}$, og (3) $\mathcal{F} \neq \emptyset$ og $\emptyset \notin \mathcal{F}$. Vis, at følgende betingelser er ækvivalente: (i) \mathfrak{a} er et primideal, (ii) \mathcal{F} er et ultrafilter, dvs et filter som opfylder, at for enhver delmængde F af I gælder: $F \in \mathcal{F} \vee \complement F \in \mathcal{F}$, (iv) Filtret \mathcal{F} er maksimalt blandt filtre, (iv) \mathfrak{a} er et maksimalideal.

9. Betragt ringen $R := \mathbb{F}_2^{\mathbb{N}}$ af alle følger $\alpha: \mathbb{N} \rightarrow \mathbb{F}_2$. Vis, at delmængden $\mathfrak{a} \subseteq R$ bestående af de følger, der er 0 fra et vist trin, er et ægte ideal i R . Kan du bestemme et maksimalideal \mathfrak{m} med $\mathfrak{m} \supseteq \mathfrak{a}$?

H1 10. Bestem en kæde af tre primidealer $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \mathfrak{p}_2$ i ringen $\mathbb{Q}[X, Y]$. –Og i ringen $\mathbb{Z}[X]$.

U6 11. Betragt en ringhomomorfi $R \rightarrow R'$ og for idealer $\mathfrak{a} \subseteq R$ og $\mathfrak{a}' \subseteq R'$ extension $R'\mathfrak{a}$ og kontraktion $R \cap \mathfrak{a}'$. Vis, at $\mathfrak{a} \subseteq R \cap R'\mathfrak{a}$ og at $R'(R \cap \mathfrak{a}') \subseteq \mathfrak{a}'$. Vis, at hvis \mathfrak{a} er en kontraktion, så er $\mathfrak{a} = R \cap R'\mathfrak{a}$, og hvis \mathfrak{a}' er en extension, så er $\mathfrak{a}' = R'(R \cap \mathfrak{a}')$.

U9 12. Antag, at R er lokal med maksimalideal \mathfrak{m} . Vis, at hvis idealet \mathfrak{m} er endeligt frembragt, så er enten $\mathfrak{m}^k = (0)$ for et (passende stort) k , eller også er $\mathfrak{m}^n \supset \mathfrak{m}^{n+1}$ for alle n . Vis, at hvis den første mulighed indtræffer, så er \mathfrak{m} det eneste primideal i R .

5. Graduerede ringe og moduler.

(5.1) Gradueret ring. Lad G være en ring. Ved en *graduering* af G forstås da en familie af (additive) undergrupper G_n for $n \in \mathbb{Z}$, som opfylder følgende to betingelser:

- (1) Som gruppe er G den direkte sum af undergrupperne G_n . Med andre ord, hvert element g i G har en entydig fremstilling som en endelig sum,

$$g = \sum_n g_n,$$

hvor g_n tilhører G_n for alle $n \in \mathbb{Z}$. (At summen er endelig betyder, at kun enelig mange g_n i fremstillingen er forskellige fra 0.)

- (2) For alle i, j gælder, at $G_i G_j \subseteq G_{i+j}$.

Gradueringen siges at være en *positiv graduering*, hvis $G_n = 0$ for $n < 0$. En ring G med en given graduering kaldes en *gradueret ring*.

Antag, at G er en gradueret ring. Elementerne i undergruppen G_n siges da at være *homogene af grad n* , og fremstillingen i (1) af et element g i G kaldes den *homogene dekomposition*; leddene g_n kaldes de *homogene komponenter* eller *homogene led* i g . Nul-elementet i G tilhører naturligvis enhver af grupperne G_n , så det er homogent af enhver grad. Det følger af betingelsen (1), at elementer forskellige fra 0 ikke kan tilhøre to forskellige af undergrupperne G_i ; homogene elementer forskellige fra 0 har altså en veldefineret grad.

Betingelsen (2) udsiger, at produkt af to homogene elementer igen er et homogent element, og mere præcist, at et produkt af to elementer, der er homogene af grader i og j , er homogent af grad $i + j$.

(5.2) Observation. Et-elementet 1 i G er homogent af grad 0. Et-elementet har nemlig en homogen dekomposition, $1 = \sum_i g_i$. Er h et homogent element af grad n , får vi ligningen,

$$h = 1h = \sum_i g_i h.$$

På venstresiden er h homogent af grad n . På højresiden er leddet $g_i h$ homogent af grad $i + n$. Af entydigheden af dekompositionen følger nu specielt, at h må være lig med det homogene led af grad n på højresiden, altså at der gælder ligningen, $h = g_0 h$. Denne sidste ligning gælder altså når h er et homogent element i G . Ved addition slutes så, at den gælder når h er en endelig sum af homogene elementer. Ligningen $h = g_0 h$ gælder derfor for alle elementer h i G . Men denne ligning betyder netop, at g_0 er et-elementet i G . Altså er $1 = g_0$ homogent af grad 0.

Undergruppen G_0 i G er ifølge betingelsen (2) stabil under multiplikationen i G , og den indeholder et-elementet. Den er derfor en delring af G . En gradueret ring G kan altså naturligt opfattes som algebra over G_0 . Bemærk desuden, at de homogene undergrupper G_n er G_0 -moduler ifølge (2).

(5.3) Eksempel. Polynomiumsringen $G = R[X_1, \dots, X_d]$ i d variable over R er en gradueret ring, idet G_n defineres som gruppen af polynomier, der (i sædvanlig forstand) er homogene af grad n . Gradueringen er øjensynlig positiv.

(5.4) Gradueret modul. Lad G være en gradueret ring. En G -modul M siges da at være *gradueret*, hvis der i M er givet en familie af undergrupper M_n for $n \in \mathbb{Z}$, som opfylder følgende to betingelser:

- (1) Som gruppe er M den direkte sum af undergrupperne M_n . Med andre ord, hvert element x i M har en entydig fremstilling som en endelig sum,

$$x = \sum_n x_n,$$

hvor x_n tilhører M_n for alle $n \in \mathbb{Z}$.

- (2) For alle i, j gælder, at $G_i M_j \subseteq M_{i+j}$.

Fremstillingen i (1) kaldes den *homogene dekomposition* af x , idet der for graduerede moduler benyttes en sprogbrug ganske svarende til den der benyttes for graduerede ringe.

Det er klart, at G , opfattet som G -modul, er en gradueret modul.

(5.5) Homogen undermodul. Lad M være en gradueret modul (over en gradueret ring G). En undermodul N i M siges da at være en *homogen undermodul*, hvis der for hvert element x i N gælder, at de homogene led i x også tilhører N . Ækvivalent betyder dette, at N er sum af undermodulerne,

$$N_n := N \cap M_n,$$

og det medfører, at disse undermoduler er en graduering af N . En homogen undermodul er altså specielt selv en gradueret modul.

(5.6) Observation. En gradueret modul M , der er frembragt af endelig mange elementer, er også frembragt af endelig mange homogene elementer. Er nemlig M frembragt af endelig mange elementer x i M , så vil de homogene led i x 'erne også frembringe M . Omvendt er det klart, at homogene elementer i M vil frembringe en homogen undermodul i M .

(5.7) Lemma. *Lad G være en gradueret ring, således at G som algebra over G_0 er frembragt af elementer i G_1 . Da er gradueringen i G positiv. Lad videre M være en gradueret G -modul frembragt af endelig mange homogene elementer. Da gælder: Hvis n er mindre end den mindste grad af disse frembringere, så er $M_n = 0$. Hvis d er større end eller lig med den største grad af disse frembringere, så vil M_d frembringe hele den homogene undermodul*

$$M_{\geq d} := M_d \oplus M_{d+1} \oplus M_{d+2} \oplus \cdots$$

Bevis. Da G er frembragt som G_0 -algebra af elementer i G_1 , er hvert element g i G en G_0 -linearkombination af endelige produkter af elementer i G_1 . Et sådant produkt er homogent af grad lig med antallet af faktorer, og graden ændres ikke når produktet multipliceres med en skalar fra G_0 ; specielt er graden altså ikke-negativ. Ud fra linearkombinationen fås den homogene dekomposition ved at samle led, der har samme grad. Der er således ingen homogene led i g , der får negativ grad. Altså er $G_n = 0$ for $n < 0$.

Lad nu M være en gradueret G -modul, og antag, at M er frembragt af endelig mange homogene elementer e_α . Hvert element x i M er altså en G -linearkombination af e_α 'erne. Indsættes

i en sådan linearkombination for hver af koefficienterne den homogene dekomposition, og videre, for hvert af disse homogene elementer i G fremstillingen som en G_0 -linearkombination af endelige produkter af elementer i G_1 , fås en fremstilling af x som en endelig sum af produkter af formen he_α , hvor h er et produkt af et element i G_0 og endelig mange elementer i G_1 . Elementet h har ikke-negativ grad, og graden af produktet he_α er derfor større end eller lig med graden af e_α . Graden af produktet he_α kan derfor aldrig være mindre end den mindste grad af e_α 'erne. Når n er mindre end denne mindste grad, må M_n altså være lig med 0.

Lad nu d_α være graden af frembringeren e_α . Antag, at d er større end eller lig med hvert af d_α 'erne. Betragt et element x i M_n , hvor $n \geq d$. Ifølge det foregående har x en fremstilling som en sum af produkter he_α , hvor h er et produkt af et element i G_0 og endelig mange faktorer i G_1 . Da x er homogent af grad n , kan man fra fremstillingen bortkaste eventuelle produkter he_α som ikke er af grad n . Det kan altså antages, at alle produkter he_α i fremstillingen har grad n . Nu var h et produkt beskrevet ovenfor, og h 's grad er derfor lig med antallet af faktorer fra G_1 . På den anden side har produktet he_α graden n , og $n \geq d \geq d_\alpha$. Ved at samle faktorerne i h passende kan h derfor skrives som et produkt $h'h''$ således at $h''e_\alpha$ har grad d . Hvert led i fremstillingen af x kan altså skrives som et produkt $h'e$, hvor $e \in M_d$ og $h' \in G_{n-d}$. Specielt ses, at x er en G -linearkombination af elementer i M_d . Da x var et vilkårligt element i M_n for $n \geq d$ følger det, at hvert element i undermodulen $M_{\geq d}$ er en G -linearkombination af elementer i M_d . \square

(5.8) Homogen afbildning. Lad M og N være graduerede moduler. En lineær afbildning $f: M \rightarrow N$ siges da at være *homogen*, hvis der gælder

$$f(M_n) \subseteq N_n \text{ for alle } n.$$

Lidt mere generelt siges f at være *homogen af grad i* , hvis $f(M_n) \subseteq N_{n+i}$ for alle i . Det er klart, at kernen for en homogen homomorfi $f: M \rightarrow N$ er en homogen undermodul i M og at billedet er en homogen undermodul i N .