Kommutativ algebra, 2005

Anders Thorup

Matematisk Afdeling
Københavns Universitet

Anders Thorup, e-mail: `thorup@math.ku.dk`
Kommutativ algebra, 2005

Matematisk Afdeling
Universitetsparken 5
2100 København Ø

Deklaration

Dette er ikke en bog, men en samling af forelæsningsnoter brugt ved forelæsningerne i Kommutativ Algebra 2005. Materialet er løst organiseret, og ikke gennemarbejdet, og det er – med stor sikkerhed – fyldt med trykfejl.

Anders Thorup
September 2011

Indhold

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 *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 nul-elementet en nuldivisor. 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 $a = 0$.

Ringen $\mathbb{Z}$ 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

$$\overbrace{1 + \cdots + 1}^{n} = 0. \tag{1.3.1}$$

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 karakteristikken. Hvis ligningen (1.3.1) ikke er opfyldt for noget tal n, siges ringen at have karakteristik 0.

(1.4) Ringhomomorfi. En afbildning $\theta\colon S \to R$ 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 $\varphi(1) = 1$. Homomorfien 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 $R' \to R$.

(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 hovedidealer, og et *hovedidealområde* (eller et *PID*), hvis den desuden er et integritetsområde.

De trivielle idealer er hovedidealer: 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 triviel 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.

Ringen 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 skrive 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* 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 $\mathfrak{ab}$ er indeholdt i fællesmængden $\mathfrak{a} \cap \mathfrak{b}$. Bemærk videre, at radikalet 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 $R \to R/\mathfrak{a}$, 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 $\theta\colon R \to S$ 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 *højestegradskoefficienten* 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 højestegradskoefficienterne. 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,*

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

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 $1, \alpha, \alpha^2, \ldots$ 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. $\square$

(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 $\overline{\alpha}$ rod i f. Disse tal er forskellige, så inden for $\mathbb{C}[X]$ er f delelig med produktet $p = (X - \alpha)(X - \overline{\alpha})$. 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. □

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 førstegradspolynomium. Af det foregående resultat følger derfor, at p er et andengradspolynomium $p = (X-a)^2 + b^2$, 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. □

(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,

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

altså en sum af endelige mange led af formen $rX_1^{i_1} \cdots X_n^{i_n}$. 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:

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

den indre sum, for en fast værdi 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:

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

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 $f = a_0X^n + a_1X^{n-1} + \cdots + a_n \in R[X]$, 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 $R \times M \to M$ 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 $\mathbb{R}$) 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 anden og den sidste ligning ovenfor, for $n \in \mathbb{Z}$, $n \geqslant 1$, at

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

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

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 $x = (x_1, \dots, x_n)^{\mathrm{tr}}$, hvor $x_i \in M_i$. Addition og multiplikation med skalarer fra R defineres koordinatvis.

(1.17) Definition. En afbildning $\varphi \colon M \to N$ 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, og en *endomorfi*, hvis $M = N$.

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*,

$$x = r_1e_1 + \cdots + r_ne_n,$$

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

(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,

$$Rx_1 + \cdots + Rx_m = \{\, r_1x_1 + \cdots + r_nx_n \mid r_1, \dots, r_n \in R \,\},$$

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:

$$x \equiv x' \overset{\mathrm{DEF}}{\iff} x' - x \in N.$$

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 $M \to M/N$, kaldet den *kanoniske homomorfi.*

Isomorfisætning for moduler. *Lad $\varphi \colon M \to N$ 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 Isomorfisætning 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 $R \to M$. 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 $\operatorname{Ann}(x)$.

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 $\operatorname{Ann}(x)$ 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 *annulllator*, og betegnet $\operatorname{Ann} M$.

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

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

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 $R/\mathfrak{a}$ 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 som modulen M, 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,

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

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 matricens 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 matricens søjler permuteres, så multipliceres determinanten med permutationens fortegn. Desuden ændres determinanten ikke, hvis matricen 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 $\Psi\colon M^n \to N$. 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

$$\Psi(u\alpha) = \det(\alpha)\Psi(u). \tag{1.22.2}$$

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

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

De mulige sæt af indices $(\sigma_1, \dots, \sigma_n)$ svarer til afbildningerne $\sigma\colon \{1, \dots, n\} \to \{1, \dots, n\}$, 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 $\Psi(u_{\sigma_1}, \dots, u_{\sigma_n}) = \operatorname{sign}(\sigma)\Psi(u_1, \dots, u_n)$. Udtrykket i (*) reduceres altså til følgende:

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

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 matricens 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,

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

hvor faktorerne $\tilde{\alpha}_{kj}$ kun afhænger af matricen 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:*

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

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

Matricen $\tilde{\alpha} = \tilde{\alpha}_{ij}$ kaldtes klassisk den *adjugerede* til matricen α; vi vil oftest kalde den for *kofaktormatricen* 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 $x^{\mathrm{tr}}\tilde{\alpha}_l$. Formlerne kan altså bruges til at beregne matrixprodukterne $\tilde{\alpha}x$ og $x^{\mathrm{tr}}\tilde{\alpha}$. 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 $\mathrm{Mat}_n(R)$.

(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:

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

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

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

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)idealerne $\mathfrak{a} = (24)$ og $\mathfrak{b} = (32)$. Bestem summen $\mathfrak{a} + \mathfrak{b}$, produktet $\mathfrak{ab}$, og radikalerne $\mathrm{Rad}(\mathfrak{a})$ og $\mathrm{Rad}(\mathfrak{b})$.

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*,

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

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

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 $(x_1, \dots, x_n)^{\mathrm{tr}}$? Er der ikke snarere tale om en række?

6. Lad $\alpha \in \mathrm{Mat}_{pm}(R)$ være en $p \times m$-matrix. Vis, at $x \mapsto \alpha x$ er en R-lineær afbildning $R^m \to R^p$. Vis, at enhver R-lineær afbildning $R^m \to R^p$ 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,

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

8. Vis for elementer $x_1, \dots, x_k$ i R, at $(x_1) + \cdots + (x_k) = (x_1, \dots, x_k)$.

U1 **9.** Beskriv, for et naturligt tal n, idealet (n, X) i $\mathbb{Z}[X]$. Vis, at idealet er kernen for en „oplagt“ homomorfi $\mathbb{Z}[X] \to \mathbb{Z}/n$.

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 n 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 $\mathrm{Ann}(x)$ et ægte ideal?

U2 **14.** Antag, at R er et integritetsområde. Hvad kan du sige om $\mathrm{Ann}(r)$ 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 $\mathrm{Ann}(\bar{1}) = \mathfrak{a}$.

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 $\mathrm{Mat}_n(R)$, hvis og kun hvis $\det \alpha$ er invertibel i R.

19. Vis for en given mængde I, at mængden R^I af alle afbildninger $x\colon I \to R$ 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; elmentet $x_i \in R$ 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 (etelementet 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

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

(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 $\varphi\colon I \to M$, fra mængden I til en R-modul M, entydigt kan udvides til en lineær afbildning $\tilde{\varphi}\colon R^{\oplus I} \to M$.

En R-modul M kaldes *fri*, hvis den er isomorf med $M^{\oplus I}$ for en passende mængde I.

20. Elementerne i en direkte sum $M_1 \oplus \cdots \oplus M_n$ er søjler af n-sæt x, hvor den i'te koordinat x_i tilhører M_i. Betragt for simpelheds 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 $\varphi\colon M \to P$ og $\psi\colon M \to Q$ er givne homomorfier, betegner søjlen $\binom{\varphi}{\psi}$ homomorfien,

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

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

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

Betragt mere generelt to direkte summer $M = M_1 \oplus \cdots \oplus M_m$ og $N = N_1 \oplus \cdots \oplus N_p$. Vis, at de lineære afbildninger $\alpha\colon M \to N$ 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 $\alpha_{ij}\colon M_j \to N_i$).

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

$$r \mapsto r1_A$$

en ringhomomorfi $\varphi\colon R \to A$ som opfylder $rx = \varphi(r)x$. Præciser, hvad der menes med følgende påstand: En kommutativ R-algebra A er „det samme som" en kommutativ ring A med en ringhomomorfi $\varphi\colon R \to A$. 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 for K, gælder rk $K \leqslant n$. [Vink: Kernen for den naturlige projektion $R^n \to R^{n-1}$ (for $n \geqslant 2$) kan identificeres med R. Lad $K' \subseteq R^{n-1}$ være billedet af K ved projektionen, og lad $K_0 \subseteq R$ være kernen for den surjektive homomorfi $K \to K'$. Udnyt, at K_0 er fri med rk $K_0 \leqslant 1$ (PID), og at K' er fri med rk $K' \leqslant n - 1$ (induktion).]

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

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 $e\colon R^n \to M$ 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 $e\colon R^n \to M$ er surjektiv. Sættet $(e_1, \dots, e_n)$ er *lineært uafhængigt*, hvis den eneste *lineære relation* $x_1e_1 + \cdots + x_ne_n = 0$ er den *trivielle*, hvor $x_1 = \cdots = x_n = 0$. Vis, at sættet er lineært uafhængigt, hvis og kun hvis $e\colon R^n \to M$ er injektiv. Vis, at sættet er en basis for M, hvis og kun $e\colon R^n \to M$ er en isomorfi.

28. Det er et fundamentalt resultat i lineær algebra, at en lineær afbildning $\alpha\colon R^d \to R^d$ 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 $R \to R$. 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 $R^n \to R^d$ kun kan være injektiv når $n \leqslant d$ (eller når R er nulringen).

Ved *rangen* af en modul M, betegnet $\mathrm{rk}\, M$, forstås det største antal elementer, der kan være i et lineært uafhængigt system i M. Ved den *lineære dimension* (eller *frembringerdimensionen*) af M, betegnet $\dim_{\mathrm{gen}} M$, forstås det mindste antal elemeneter, der kan være i et frembringersystem for M. [Bemærk, at notationen $\dim_{\mathrm{gen}} M$ *ikke* er en standardnotation!] Vis, ved hjælp af resultatet, at der generelt gælder $\mathrm{rk}\, M \leqslant \dim_{\mathrm{gen}} M$. Vis yderligere, at hvis M er endeligt frembragt, så er M fri, hvis og kun hvis $\mathrm{rk}\, M = \dim_{\mathrm{gen}} M$.

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 $\mathfrak{a}$.]

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* (præciser selv!).

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 $\mathrm{Ann}(x) = (0)$ 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.

35. Vis, at enhver surjektiv homomorfi $\alpha\colon R^n \to R^n$ 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 adjugerede 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:

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

38. Antag, at $\Psi\colon M^n \to N$ 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 $\Psi(x_{\sigma_1}, \dots, x_{\sigma_n}) = \mathrm{sign}(\sigma)\Psi(x_1, \dots, x_n)$.

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

40. Den sædvanlige definition af sum og produkt af polynomier fører også for en ikke-kommutativ ring Λ til polynomiumsringen $\Lambda[X]$. Selv om X kommuterer med alle polynomier skrives sædvanligvis koefficienterne (konstanter) til venstre for potenserne af X, altså γX^n. Herefter er det veldefineret for $\alpha \in \Lambda$ at *indsætte* $X = \alpha$ i et polynomium $P \in \Lambda[X]$.

(1) Vis, at indsættelse: $P \mapsto P(\alpha)$ normalt *ikke* er en ringhomomorfi $\Lambda[X] \to \Lambda$. Mere præcist: Vis, at $(QP)(\alpha) = Q(\alpha)P(\alpha)$, når α kommuterer med koefficienterne i P.

(2) Vis, at den oplagte bijektive afbildning $\mathrm{Mat}_n(R)[X] \simeq \mathrm{Mat}_n(R[X])$ er en ringisomorfi.

(3) Betragt for $\alpha \in \mathrm{Mat}_n(R)$ matricen $X1_n - \alpha \in \mathrm{Mat}_n(R[X])$. Determinanten er som bekendt det *karakteristiske polynomium* $P_\alpha(X)$ for α. Lad Q betegne den adjugerede matrix for $X1_n - \alpha$. Oversæt Cramers formler til en ligning i $\mathrm{Mat}_n(R)[X]$:

$$Q \cdot (X - \alpha) = P_\alpha(X),$$

og vis, at indsættelse af $X = \alpha$ i denne ligning giver *Hamilton–Cayley's sætning*: $P_\alpha(\alpha) = 0$.

2. Kerne og kokerne. Eksakte følger.

(2.1) Kerne og kokerne. Lad der være givet en homomorfi, dvs en R-lineær afbildning, $\varphi\colon M \to N$. Ved *kernen* for φ forstås som bekendt originalmængden $\varphi^{-1}(0)$. Kernen betegnes $\operatorname{Ker}\varphi$. 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 $\operatorname{Coker}\varphi$.

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

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

$$\begin{tikzcd} M \arrow[r, "\mu"] \arrow[d, "\varphi"'] & M' \arrow[d, "\varphi'"] \\ N \arrow[r, "\nu"] & N'. \end{tikzcd}$$

[Her, som i det følgende, siges et diagram bestående af moduler og homomorfier at være *kommutativt*, hvis det for hvilkesomhelst to moduler M og P i diagrammet gælder, at alle homorfier 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 $\operatorname{Ker}\varphi$ af M ind i undermodulen $\operatorname{Ker}\varphi'$ af M'. Antag nemlig, at x tilhører $\operatorname{Ker}\varphi$. 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 $\operatorname{Ker}\varphi'$.

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

$$\operatorname{Ker}\varphi \to \operatorname{Ker}\varphi'.$$

Tilsvarende vil ν afbilde undermodulen φM af N ind i undermodulen $\varphi' M'$ af N'. Heraf fås en veldefineret afbildning $N/\varphi M \to N'/\varphi' M'$ 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 kokernerne,

$$\operatorname{Coker}\varphi \to \operatorname{Coker}\varphi'.$$

(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 $\varphi\colon M \to N$ følgerne herunder:

$$0 \longrightarrow M \xrightarrow{\varphi} N, \tag{2.4.1}$$

$$M \xrightarrow{\varphi} N \longrightarrow 0, \tag{2.4.2}$$

$$0 \longrightarrow M \xrightarrow{\varphi} N \longrightarrow 0. \tag{2.4.3}$$

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:

$$0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P, \tag{2.4.4}$$

$$M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0. \tag{2.4.5}$$

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 $N/K \to P$ med billedet ψN. Homomorfien ψ er altså surjektiv, netop når den inducerede homomorfi $N/K \to P$ 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,*

$$\begin{tikzcd}
& M' \arrow[r, "\mu'"] \arrow[d, "\varphi'"'] & M \arrow[r, "\mu"] \arrow[d, "\varphi"'] & M'' \arrow[r] \arrow[d, "\varphi''"'] & 0 \\
0 \arrow[r] & N' \arrow[r, "\nu'"] & N \arrow[r, "\nu"] & N''. &
\end{tikzcd}$$

Da induceres naturligt en eksakt følge mellem kerner og kokerner,

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

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-kokerne-følgen. Følgen af kerner og kokerner i Slangelemma'et kaldes *kerne-kokerne-følgen*. Homorfien 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 $\operatorname{Coker}\varphi'$, 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 $\operatorname{Coker}\varphi$*:* Betragt hertil en klasse i $\operatorname{Coker}\varphi$, og vælg en repræsentant x for den. Det skal vises, at klassen afbildes i nul-klassen i $\operatorname{Coker}\varphi''$, hvis og kun hvis klassen kommer fra en klasse i $\operatorname{Coker}\varphi'$. At klassen repræsenteret ved x afbildes i 0 i $\operatorname{Coker}\varphi''$ 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 $\operatorname{Coker}\varphi'$.

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

„hvis“: Antag, at $v \in \operatorname{Ker}\varphi$ og $\mu v = x$. Som det element w der indgår i definitionen på δx kan vi så bruge $w := v$. Da w så tilhører $\operatorname{Ker}\varphi$, 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 $\nu' y = \varphi w$. Videre er $\nu'\varphi' = \varphi\mu'$ da diagrammet er kommutativt. Altså er

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

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. □

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

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "\mu'"] \arrow[d, "\varphi'"'] & M \arrow[r, "\mu"] \arrow[d, "\varphi"'] & M'' \arrow[r] \arrow[d, "\varphi''"'] & 0 \\
0 \arrow[r] & N' \arrow[r, "\nu'"] & N \arrow[r, "\nu"] & N'' \arrow[r] & 0.
\end{tikzcd}$$

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

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

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

(2.10) Korollar. *Lad der være givet en homomorfi $\varphi\colon M \to P$ 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 $\operatorname{Ker}\varphi$, 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 $F_i \to F_i''$, 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 Isomorfisætning (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-kokerne-følge. ▯

(2.11) Noether's første Isomorfisætning. *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 $\varphi\colon M \to M/P$ 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 $F_2'/F_1' \to F_2/F_1$ er en isomorfi. Og det er netop Noether's første isomorfi. ▯

(2.12) Noether's anden Isomorfisætning. *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 $\varphi\colon M \to M/F$ 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. ▯

(2.13) Bemærkning. Ifølge Isomorfisætning (2.5) kan eksaktheden af følgen i Noether's anden isomorfisætning 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 Isomorfisætning 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* $\varphi\colon M \to N$ *og* $\psi\colon N \to P$ *være homomorfier. Da induceres naturligt en eksakt følge,*

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

Bevis. Det er klart, at $\operatorname{Ker}\varphi$ er indeholdt i $\operatorname{Ker}\psi\varphi$. 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.

Homomorfien markeret φ i følgen er induceret af $\varphi\colon M \to N$: når x tilhører $\operatorname{Ker}\psi\varphi$, vil φx tilhøre $\operatorname{Ker}\psi$. Tilsvarende er homomorfien ψ i følgen induceret af $\psi\colon N \to P$: denne homomorfi afbilder nemlig φM på $\psi\varphi M$, så når $y \in N$ er repræsentant for en klasse i $\operatorname{Coker}\varphi$, så er $\psi y \in P$ repræsentant for en veldefineret klasse i $\operatorname{Coker}\psi\varphi$.

Endelig afbilder δ et element x i $\operatorname{Ker}\psi$ 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 $\varphi\colon M \to N$ og $\psi\colon N \to P$, og lad $\gamma := \psi\varphi$ betegne den sammensatte homomorfi. Betragt følgende diagram,

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\binom{1}{\varphi}"] \arrow[d, "\varphi"'] & M \oplus N \arrow[r, "(\varphi\ -1)"] \arrow[d, "\left(\begin{smallmatrix}0 & 1\\ \gamma & 0\end{smallmatrix}\right)"'] & N \arrow[r] \arrow[d, "\psi"'] & 0 \\
0 \arrow[r] & N \arrow[r, "\binom{1}{\psi}"] & N \oplus P \arrow[r, "(-\psi\ 1)"] & P \arrow[r] & 0.
\end{tikzcd}$$

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

3. Betragt en nul-følge,

$$0 \longrightarrow C_p \longrightarrow C_{p-1} \longrightarrow \cdots \longrightarrow C_1 \longrightarrow C_0 \longrightarrow 0, \qquad (*)$$

og lad $Z_i \subseteq C_i$ være kernen for $C_i \to C_{i-1}$, 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 homomorfien $C_{i+1} \to C_i$ 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,

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

U2 **4.** Betragt en korteksakt følge $0 \to K \to M \to L \to 0$. 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 $0 \to M' \to M \to M'' \to 0$ er eksakt, så er også følgen $M'/\mathfrak{a}M' \to M/\mathfrak{a}M \to M''/\mathfrak{a}M'' \to 0$ eksakt. Manglede pilen $0 \to M'/\mathfrak{a}M'$ i den sidste følge?

6. Lad N og M være moduler, og betragt inklusionen $i\colon N \to N \oplus M$ (bestemt ved $x \mapsto (x, 0)$ og projektionen $p\colon N \oplus M \to M$ bestemt ved $(x, y) \mapsto y$. Gør rede for, at følgen $0 \longrightarrow N \xrightarrow{i} N \oplus M \xrightarrow{p} M \longrightarrow 0$ er eksakt.

7. Lad φ være en endomofi i modulen M, dvs en lineær afbildning $\varphi\colon M \to M$. Vis, at kæden af kerner er stigende: $\operatorname{Ker}\varphi \subseteq \operatorname{Ker}\varphi^2 \subseteq \operatorname{Ker}\varphi^3 \subseteq \cdots$, og at kæden af billeder er dalende: $\varphi M \supseteq \varphi^2 M \supseteq \varphi^3 M \supseteq \cdots$. Vis, at der findes et kommutativt diagram med exakte rækker,

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Ker}\varphi^n \arrow[r] \arrow[d, "\text{inkl.}"'] & M \arrow[r, "\varphi^n"] \arrow[d, "="'] & \varphi^n M \arrow[r] \arrow[d, "\varphi"] & 0 \\
0 \arrow[r] & \operatorname{Ker}\varphi^{n+1} \arrow[r] & M \arrow[r, "\varphi^{n+1}"] & \varphi^{n+1} M \arrow[r] & 0.
\end{tikzcd}$$

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

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:

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

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

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

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

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

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

er en veldefineret afbildning $S^{-1}R \times S^{-1}M \to S^{-1}M$. 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 $\varphi\colon M \to N$ induceres ved forskriften,*

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

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

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

$$x \mapsto x/1\,.$$

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

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d] & N \arrow[d] \\ S^{-1}M \arrow[r, "S^{-1}\varphi"] & S^{-1}N . \end{tikzcd}$$

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

(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 $M \to S^{-1}M$ af de elementer x i M for hvilke der findes et element s i S så at $sx = 0$.*

(2) *Den kanoniske homomorfi $M \to S^{-1}M$ 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 $M \to M$. 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 hvis 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. ▯

(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:

(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 $R \to R$. 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. □

(3.7) Brøklegeme. Legemet K, der fremkommer ved at lokalisere et integritetsområde R mht alle elementer forskellige fra 0, kaldes *brøklegemet 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. Brøklegemet fremkommer altså ved at lokalisere i primidealet (0), jfr Definition (3.5)(2), og det kan betegnes $R_{(0)}$.

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

Ringen $k[X_1, \dots, X_m]$ af polynomier i m variable over et legeme k er et integritetsområde. Det tilhørende brøklegeme 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,

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

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. ▯

(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 billedet 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, sluttes 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. ▯

(3.10) Isomorfisætning for brøkmoduler. *Lad N være en undermodul i R-modulen M. Da er $S^{-1}N$ naturligt en undermodul i $S^{-1}R$-modulen $S^{-1}M$, og for den tilhørende kvotientmodul findes en isomorfi,*

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

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

Bevis. Følgen $0 \to N \to M \to M/N \to 0$ 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 modulen til venstre er en undermodul i modulen i midten og at modulen til højre er den tilhørende kvotientmodul.

Bemærk, at den injektive homomorfi $S^{-1}N \to S^{-1}M$ 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 undermodul 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 undermodul 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 undermodul 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 Isomorfisætningen fuldført. □

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

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

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

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-modul. 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,*

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

Bevis. Ifølge Isomorfisætningen (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 den tredie undermodul. Altså er den anden undermodul indeholdt i den tredie.

Betragt et element i den tredie 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 tredie undermodul indeholdt i den første.

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

(3.13) Observation. Lad der være givet en ringhomomorfi $\theta\colon R \to R'$. 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 $S^{-1}\theta\colon S^{-1}R \to S^{-1}R'$ er en ringhomomorfi.

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

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

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.

(2) 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) Antag at S og T er multiplikative delmængder af R. Det er klart, at ST, defineret som mængden af alle produkter st med $s \in S$ og $t \in T$, så igen er en multiplikativ delmængde af R. Også de følgende isomorfier skal ses i lyset af (3.13):

$$S^{-1}(T^{-1}M) = (ST)^{-1}M, \qquad S^{-1}(T^{-1}R) = (ST)^{-1}R;$$

Brøkmodulen $T^{-1}M$ er en $T^{-1}R$-modul, og venstresiderne i isomorfierne, der a priori er lokaliseringer af R-moduler mht S, kan ligeledes opfattes som lokaliseringer af $T^{-1}R$-moduler mht til billedet af S i ringen $T^{-1}R$; det sidste billede kan i øvrigt naturligt betegnes $S/1$. Det er let at definere de to isomorfier.

Det følger af isomorfierne, at gentagen lokalisering, først mht S og dernæst mht T er uafhængig af rækkefølgen, idet resultatet kan fås ved at lokalisere mht ST.

Bemærk specialtilfældet, hvor $S \subseteq T$: her er $ST = T$.

(3.15) Opgaver.

1. Vis for et integritetsområde R med brøklegeme K, at for enhver „mellemring“ $R \subseteq T \subseteq K$ kan man identificere brøklegemet 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 brøklegemet K for R.

7. Lad R være et UFD med brøklegeme K. Lad $\mathcal{P}$ være et repræsentantsystem for primelementerne på nær associering, og antag, at der for hvert $p \in \mathcal{P}$ er valgt er 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 $n \geqslant 1$) 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 $M \to S^{-1}M$ injektiv? Kan det indtræffe, at $M \to S^{-1}M$ er en isomorfi?

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 brøklegeme $K := R_{(0)}$. Vis for enhver R-modul M, at $\operatorname{rk} M = \dim M_{(0)}$, hvor dimensionen er dimensionen som vektorrum over K.

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

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 primidealerne i brøkringen $S^{-1}\mathbb{Z}$, og de tilsvarende primidealer 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 ekstensionen $\mathfrak{a}S^{-1}R$ af $\mathfrak{a}$ til $S^{-1}R$.

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

15. Lad S være en multiplikativ delmængde af R. Vis, at homomorfien $M \to S^{-1}M$ 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 ekstension: $\mathfrak{q} = R \cap S^{-1}\mathfrak{q}$. [Vink: $R \cap S^{-1}\mathfrak{q}$ er kernen for den sammensatte homomorfi $R \to R/\mathfrak{q} \to S^{-1}(R/\mathfrak{q})$.]

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

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 $P(\xi) \to P(1/f)$ og $a/f^n \to a\xi^n$ er veldefinerede og hinandens inverse.]

4. Primideal og maksimalideal.

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

$$\mathfrak{m} \subseteq \mathfrak{a} \subset R \implies \mathfrak{m} = \mathfrak{a}.$$

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

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

$$xy \in \mathfrak{p} \implies x \in \mathfrak{p} \vee y \in \mathfrak{p}.$$

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

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

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

Bevis. Ideen i beviset er følgende: Enten er $\mathfrak{a}$ et maksimalideal (og så er vi færdige), eller også findes et ideal $\mathfrak{a}_1$ forskelligt fra R således at $\mathfrak{a} \subset \mathfrak{a}_1$. Her er enten $\mathfrak{a}_1$ et maksimalideal (og så er vi færdige), eller også findes et ideal $\mathfrak{a}_2$ forskelligt fra R således at $\mathfrak{a}_1 \subset \mathfrak{a}_2$. 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,

$$\mathfrak{a} \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots .$$

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 axiomer fra mængdelæren (Zorn's Lemma) for at vise, at ideen kan udbygges til et bevis for eksistensen af det ønskede maksimalideal. □

En generalisering. *Lad $S \subseteq R$ være en multiplikativ delmængde. Da gælder om følgende mængde $\mathcal{S}$ af idealer i R:*

$$\mathcal{S} = \{\, \mathfrak{a} \mid \mathfrak{a} \cap S = \emptyset \,\},$$

(1) *Ethvert ideal $\mathfrak{a} \in \mathcal{S}$ er indeholdt i et ideal $\mathfrak{q} \in \mathcal{S}$, der er maksimalt element i mængden $\mathcal{S}$.*
(2) *Ethvert maksimalt element i mængden $\mathcal{S}$ er et primideal.*

Bevis. Beviset for (1) er ganske som beviset for Eksistenssætningen. For at vise (2) betragtes et maksimalt element $\mathfrak{p} \in \mathcal{S}$. Da $1 \in S$, følger det at hvert element i $\mathcal{S}$ er et ægte ideal. Altså er $\mathfrak{p} \subset R$. Antag videre for elementer $a, b \in R$, at $ab \in \mathfrak{p}$, og, indirekte, at $a \notin \mathfrak{p}$, $b \notin \mathfrak{p}$. Af det sidste følger, at de to idealer $(\mathfrak{p}, a)$ og $(\mathfrak{p}, b)$ er strengt større end $\mathfrak{p}$. De to idealer ligger altså ikke i $\mathcal{S}$. Derfor findes der elementer $s, t \in S$ således, at

$$s \in (\mathfrak{p}, a), \quad t \in (\mathfrak{p}, b). \tag{*}$$

Produktet af de to idealer i (*) er indeholdt i $\mathfrak{p}$, da $ab \in \mathfrak{p}$. Derfor følger det af (*), at $st \in \mathfrak{p}$. Da S er multiplikativ, ses specielt, at $\mathfrak{p} \cap S \neq \emptyset$. Men det er i modstrid med at $\mathfrak{p} \in \mathcal{S}$. □

For $S = \{1\}$ består $\mathcal{S}$ af de ægte idealer, og (1) er Eksistenssætningen. (2) er det velkendte resultat, at ethvert maksimalideal er et primideal.

(4.3) Bemærkning. Det følger af Eksistenssætningen, at der i enhver ring R forskellig fra nul-ringen findes maksimalidealer. Specielt findes altså primidealer i R, når $R \neq 0$.

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

(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 hvis kun 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 tilfredsstiller 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. ∎

(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 $\varphi\colon F \to M$ være den lineære afbildning svarende til v_i'erne, dvs afbildningen,

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

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 $F \longrightarrow M \longrightarrow Q \longrightarrow 0$, og heraf fås umiddelbart den eksakte følge,

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

Forudsætningerne medfører, at afbildningen $F/\mathfrak{m}F \to M/\mathfrak{m}M$ er surjektiv. Af eksaktheden følger derfor, at $Q/\mathfrak{m}Q = 0$. Af Nakayama's Lemma følger endelig, at $Q = 0$. Hermed er sætningen bevist. ∎

(4.8) Lemma. *Antag, at primidealet $\mathfrak{p}$ omfatter et produkt $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ af n idealer $\mathfrak{a}_i$. Da vil $\mathfrak{p}$ omfatte et af $\mathfrak{a}_i$'erne.*

Bevis. Det antages, at $\mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \mathfrak{p}$, og det skal vises, at der findes et i så at $\mathfrak{a}_i \subseteq \mathfrak{p}$. Antag, indirekte, at et sådant i ikke fandtes. Da findes for hvert i et element $a_i \in \mathfrak{a}_i$, 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 $\mathfrak{a}_i$'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 $\mathfrak{a}_i$'erne er indeholdt i $\mathfrak{p}$. ∎

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

Bevis. Påstanden vises ved induktion efter n. Den er triviel for $n = 1$. I induktionsskridtet antages, at

$$\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n, \tag{0}$$

med $n > 1$ og at påstanden gælder for vilkårlige $n - 1$ primidealer. Af det sidste følger, at det er nok at vise, at $\mathfrak{a}$ er indeholdt i $n - 1$ af primidealerne. Det vises indirekte: Antag, for $j = 1, \dots, n$, at

$$\mathfrak{a} \not\subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_{j-1} \cup \mathfrak{p}_{j+1} \cup \cdots \cup \mathfrak{p}_n, \tag{j'}$$

Vælg nu for hvert j et element a_j, som ligger på venstresiden i (j'), og ikke på højresiden. Da $a_j \in \mathfrak{a}$ og a_j ikke tilhører højresiden i (j'), følger det af (0), at $a_j \in \mathfrak{p}_j$. For $j = 1, \dots, n$ har vi altså

$$a_j \in \mathfrak{a} \cap \mathfrak{p}_j, \qquad a_j \notin \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_{j-1} \cup \mathfrak{p}_{j+1} \cup \dots \cup \mathfrak{p}_n, \tag{j}$$

Betragt nu elementet

$$a := a_1 + a_2 \cdots a_n\,. \tag{+}$$

Hvert a_i ligger i $\mathfrak{a}$, så $a \in \mathfrak{a}$. Af (0) følger så, at a ligger i et af idealerne $\mathfrak{p}_k$.

Antag først, at $k = 1$, altså at $a \in \mathfrak{p}_1$. Da $a_1 \in \mathfrak{p}_1$ følger det af (+), at $a_2 \cdots a_n \in \mathfrak{p}_1$. Da $\mathfrak{p}_1$ er et primideal, følger det, at $a_j \in \mathfrak{p}_1$ med et $j > 1$, men det er i modstrid med (j).

Antag dernæst, at $k > 1$. Da ligger $a_2 \cdots a_n$ i $\mathfrak{p}_k$, og da $a \in \mathfrak{p}_k$, følger det af (+), at $a_1 \in \mathfrak{p}_k$. Men det er i modstrid med relationerne i (j) for $j = 1$.

Begge antagelser har altså ført til en modstrid, og dermed er det indirekte bevis fuldført. □

Bemærkning. Et nøjere kig på beviset afslører, at det fungerer også hvis man tillader at to af idealerne $\mathfrak{p}_i$ ikke er primidealer. Specielt tilfældet, hvor man blot antager, at $n - 1$ af idealerne $\mathfrak{p}_i$ er primidealer, har faktisk interesse.

(4.10) Kontraktion og ekstension. Lad $\theta\colon R \to R'$ 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. Så er produktet $\mathfrak{a}R'$, bestående af endelige summer af produkter $\theta(a)r$ for $a \in \mathfrak{a}, r \in R'$, et ideal i ringen R'. Det kaldes *ekstensionen* af idealet $\mathfrak{a}$.

(4.11) Bemærkning. Kontraktionen $\theta^{-1}(\mathfrak{b})$ af et ideal $\mathfrak{b}$ i R' er øjensynlig kernen for den sammensatte ringhomomorfi $R \to R' \to R'/\mathfrak{b}$. 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 $\theta\colon R \to R/\mathfrak{a}$ betegne den kanoniske afbildning på kvotientringen. Da vil ekstension og kontraktion,*

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

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,

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

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 $\mathfrak{p}/\mathfrak{a}$. ∎

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

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

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,

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

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 $R \to R/\mathfrak{p}$, 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 Isomorfisætning for brøkmoduler (3.10), at $\mathfrak{q} = S^{-1}\mathfrak{q}_0$. Af Korollar til Isomorfisætningen (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 Isomorfisætningen for brøkmoduler (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 $R \to S^{-1}R \to S^{-1}R/S^{-1}\mathfrak{p}$. Det er klart, at denne homomorfi er den samme som den sammensatte homomorfi $R \to R/\mathfrak{p} \to \bar{S}^{-1}(R/\mathfrak{p})$. Kontraktionen er følgelig kernen for denne sidste sammensatte homomorfi. Her er homomorfien $R/\mathfrak{p} \to \bar{S}^{-1}(R/\mathfrak{p})$ injektiv, jfr Sætning (3.6). Kontraktionen er derfor kernen for homomorfien $R \to R/\mathfrak{p}$. 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

$$\frac{x/s_1}{t/s_2}\,. \tag{$*$}$$

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. □

(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 $i \geqslant 1$ en naturlig isomorfi,*

$$M/\mathfrak{m}^iM \xrightarrow{\sim} M_\mathfrak{m}/\mathfrak{m}^iM_\mathfrak{m}. \tag{4.16.1}$$

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 brøkmodulen $S^{-1}(M/\mathfrak{m}^i M)$, jfr Korollar (3.12). Det er således påstanden, at den kanoniske homomorfi $M/\mathfrak{m}^i M \to S^{-1}(M/\mathfrak{m}^i M)$ 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. □

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

(4.19) Observation. Af definitionen følger, at to forskellige maksimalidealer $\mathfrak{m}_1$ 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,

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

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 ringhomorfi 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' er 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. □

(4.21) Eksempel. Den klassiske anvendelse af den kinesiske restklassesætning er på ringen $\mathbb{Z}$ af hele tal. Her er alle idealer hovedidealer, dvs af formen (n), hvor $n \geqslant 0$. To hovedidealer (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 primidealer. Er der maksimalidealer imellem dem?

4. Vis, at hvis $\mathfrak{a}$ er en fællesmængde af primidealer, så er $\mathfrak{a} = \mathrm{Rad}(\mathfrak{a})$.

5. Vis, at en endelig fællesmængde $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ af primidealer 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 $\mathrm{Rad}(0)$ er delmængden bestående af alle nilpotente elementer i R. *Vis, at

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

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 $I \to \mathbb{F}_2$. 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 $\alpha\colon \mathbb{N} \to \mathbb{F}_2$. 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 $\mathfrak{m} \supseteq \mathfrak{a}$?

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 $R \to R'$ og for idealer $\mathfrak{a} \subseteq R$ og $\mathfrak{a}' \subseteq R'$ ekstensionen $R'\mathfrak{a}$ og kontraktionen $R \cap \mathfrak{a}'$. 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 ekstension, 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.

U6 **13.** 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 primidealerne i brøkringen $S^{-1}\mathbb{Z}$, og de tilsvarende primidealer i $\mathbb{Z}$.

14. Antag for en ringhomomorfi $\theta\colon R \to R'$, at primidealet $\mathfrak{p} \subset R$ er kontraktion $\mathfrak{p} = \mathfrak{b} \cap R$ af et ideal $\mathfrak{b}$ i R'. Vis, at $\mathfrak{p}$ er kontraktion af et primideal i R'. [Vink: Billedmængden $S := \theta(R \setminus \mathfrak{p})$ er multiplikativ, og disjunkt med $\mathfrak{b}$. Slut heraf, at der i R' findes et primideal $\mathfrak{q}$ med $\mathfrak{q} \supseteq \mathfrak{b}$ og $\mathfrak{q} \cap S = \emptyset$, og at $\mathfrak{q}$ løser problemet.]

Endelighedsbetingelser

1. Endeligt frembragte moduler.

(1.1) Endeligt frembragt modul. Lad M være en R-modul. For givne elementer $v_1, \dots, v_m$ i M betegnes da med

$$Rv_1 + \cdots + Rv_m$$

delmængden af M bestående af de elementer, der har formen

$$r_1 v_1 + \cdots + r_m v_m \qquad \text{med } r_i \in R.$$

Øjensynlig er denne delmængde en undermodul i M, endda den mindste, der indeholder v_i'erne. Den kaldes undermodulen *frembragt* af v_i'erne.

Modulen M siges at være *endeligt frembragt*, hvis der i M findes endelig mange elementer $v_1, \dots, v_m$, som *frembringer* M, dvs opfylder at

$$M = Rv_1 + \cdots + Rv_m.$$

En modul M, der er frembragt af et enkelt element, dvs har formen $M = Rv$, siges også at være en *cyklisk modul*.

(1.2) Observation. Modulen R^n er endeligt frembragt, nemlig frembragt af de n-sæt, der har 0 på alle pladser på nær et enkelt 1 på én plads. Specielt er R, som R-modul, endeligt frembragt (endda cyklisk).

For givne elementer $v_1, \dots, v_m$ i en modul M defineres en R-lineær afbildning $R^m \to M$ ved

$$(r_1, \dots, r_m) \mapsto r_1 v_1 + \cdots + r_m v_m.$$

Billedet for denne afbildning er øjensynlig undermodulen frembragt af v_i'erne. Heraf følger let, at en modul M er endeligt frembragt, hvis og kun hvis M er homomorft billede af en modul R^m for passende m, altså hvis og kun hvis M er isomorf med en kvotient R^m/K, hvor K er en undermodul i R^m.

Tilsvarende følger det, at modulen M er cyklisk, hvis og kun hvis M som modul er isomorf med en kvotient $R/\mathfrak{a}$, hvor $\mathfrak{a}$ er et ideal i R.

Hvis ringen R er et legeme, er moduler over R som bekendt blot vektorrum. Et vektorrum er øjensynlig endeligt frembragt, hvis og kun hvis det er endeligdimensionalt, og det er cyklisk, hvis og kun hvis det enten er 1-dimensionalt eller består alene af 0.

(1.3) Sætning. *Lad der være givet en eksakt følge af R-moduler,*

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

Hvis M er endelig frembragt, så er P endelig frembragt. Hvis både N og P er endeligt frembragte, så er M endelig frembragt.

Bevis. Hvis elementer $v_1, \dots, v_m$ frembringer M, så vil deres billeder i P frembringe P, fordi homomorfien $\psi\colon M \to P$ er surjektiv. Heraf følger den første påstand.

For at vise den anden påstand betragtes elementer $v_1, \dots, v_n$ som frembringer N og elementer $u_1, \dots, u_p$, som frembringer P. Da ψ er surjektiv, findes elementer $w_1, \dots, w_p$ i M, som ved ψ afbildes på u_i'erne. Det påstås, at M er frembragt af de endelig mange elementer $\varphi v_1, \dots, \varphi v_n, w_1, \dots, w_p$. Betragt hertil et vilkårligt element x i M. Billedet af x i P er da en linearkombination af u_i'erne, $\psi x = \sum r_i u_i$. Den tilsvarende linearkombination af w_i'erne, $\sum r_i w_i$, har nu samme billede i P som x, og differensen,

$$x - \sum_i r_i w_i,$$

tilhører derfor kernen for ψ. Da følgen er eksakt, vil differensen altså tilhøre billedet φN. Dette billede er frembragt af φv_j'erne, da v_j'erne frembringer N. Differensen er derfor en linearkombination af φv_j'erne. Heraf ses, at elementet x er en linearkombination af w_i'erne og φv_j'erne, som påstået. □

(1.4) Note. Beviset for Sætningen giver mere information: Hvis P er frembragt af p elementer og N er frembragt af n elementer, så er M frembragt af $p + n$ elementer.

(1.5) Bemærkning. Den oplagte anvendelse af sætningen er på den eksakte følge hørende til en undermodul N af M,

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

Hvis N og M/N er endeligt frembragte, så er M endeligt frembragt. Hvis M er endeligt frembragt, så er kvotienten M/N endeligt frembragt.

Bemærk, at man ikke, når M er endeligt frembragt, kan slutte at undermodulen N i M nødvendigvis er endeligt frembragt. I R, der jo som R-modul er frembragt af ét element (nemlig af et-elementet $1 \in R$), er alle idealer ikke nødvendigvis endeligt frembragte.

(1.6) Eksempel. Lad R betegne ringen af reelle talfølger (a_n). Det er klart, at de følger (a_n), der er 0 fra et vist trin, udgør et ideal I i R. Det er let at se, at idealet I ikke er endeligt frembragt.

(1.7) Definition. Lad M være en R-modul. Ved en (endelig) *filtration* i M forstås en følge af undermoduler,

$$0 = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = M.$$

De successive kvotienter F_i/F_{i-1} for $i = 1, \dots, n$ kaldes også *filtrationens kvotienter*. Den i'te kvotient F_i/F_{i-1} er øjensynlig 0, netop når $F_{i-1} = F_i$. Antallet af kvotienter forskellige fra 0 er altså antallet af skarpe $\subset$'er i filtrationen. Dette antal kaldes *filtrationens længde*.

(1.8) Eksempel. Antag, at M er frembragt af elementer $v_1, \dots, v_m$. Sæt

$$F_i := Rv_1 + \cdots + Rv_i$$

for $i = 0, \dots, m$ (for $i = 0$ er $F_0 = 0$). Da udgør F_i'erne en filtration af M. Bemærk, at kvotienten F_i/F_{i-1} er frembragt af billedet af v_i, idet der modulo F_{i-1} gælder, at $\sum_{j=1}^{i} r_j v_j \equiv r_i v_i$. Filtrationens kvotienter er altså cykliske.

(1.9) Observation. Ofte er det bekvemt at kunne udlede egenskaber for en modul M ud fra egenskaberne ved kvotienterne i en given filtration $0 = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = M$ af M. Lad os fx vise, at hvis kvotienterne F_i/F_{i-1} er endeligt frembragte, så er M endeligt frembragt.

Vi viser ved induktion efter i, for $i = 1, \dots, n$, at F_i er endeligt frembragt. For $i = 1$ er $F_1 = F_1/F_0$ endeligt frembragt. Til induktionsskridtet anvendes den eksakte følge,

$$0 \to F_{i-1} \to F_i \to F_i/F_{i-1} \to 0.$$

Induktivt kan det antages, at F_{i-1} er endeligt frembragt, og F_i/F_{i-1} er endeligt frembragt ifølge antagelsen. Af Sætning (1.3) følger derfor, at F_i er endeligt frembragt.

(1.10) Observation. Betragt en direkte sum af moduler, $M = M_1 \oplus \cdots \oplus M_n$. Sæt

$$F_i := M_1 \oplus \cdots \oplus M_i$$

for $i = 0, \dots, n$ (for $i = 0$ er $F_0 = 0$). Her kan F_i opfattes som undermodul af M: Den direkte sum M består af n-sæt, og F_i består af de n-sæt, der har 0 på pladser med index større end i. Herved udgør F_i'erne en filtration af M. Den i'te kvotient F_i/F_{i-1} kan identificeres med M_i. Dette følger af at der generelt for en direkte sum $F \oplus N$ gælder, at $(F \oplus N)/F = N$. Af de foregående resultater følger umiddelbart: M er endeligt frembragt, hvis og kun hvis hver „summand“ M_i er endeligt frembragt.

(1.11) Opgaver.

U4 **1.** Vis, at $\mathbb{Q}$ som $\mathbb{Z}$-modul ikke er endeligt frembragt.

U4 **2.** Betragt delringen $R = \mathbb{Z} \oplus \mathbb{Q}X \oplus \mathbb{Q}X^2 \oplus \mathbb{Q}X^3 \oplus \cdots \subseteq \mathbb{Q}[X]$. Vis, at idealet af polynomier $f \in R$ med $f(0) = 0$ ikke er endeligt frembragt.

3. Præciser hvad der menes med polynomiumsringen $R = \mathbb{Q}[X_1, X_2, X_3, \dots]$ i numerabelt mange variable. Vis, at idealet bestående af polynomier „uden“ konstantled, dvs med konstantled lig med 0, ikke er endeligt frembragt.

U4 **4.** Vis, at en kommutativ gruppe (altså en $\mathbb{Z}$-modul) M er endelig, hvis og kun hvis M har en filtration $(0) = F_0 \subseteq \cdots \subseteq F_n = M$, hvor kvotienterne F_i/F_{i-1} er endelige. Vis, at „i så fald“ er $|M| = |F_1/F_0| \cdots |F_n/F_{n-1}|$.

U5 **5.** Lad der være givet en filtration $0 = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = M$ i M med cykliske kvotienter $F_i/F_{i-1} = R/\mathfrak{a}_i$ for $i = 1, \dots, n$. Vis, at produktet $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ er indeholdt i annullatoren $\operatorname{Ann} M$.

U6 **6.** Vis, at en R-modul M er fri, hvis og kun hvis M har en endelig filtration, hvor alle de successive kvotienter er isomorfe med R.

7. Lad M være en endeligt frembragt R-modul og lad $\mathfrak{a}$ være et ideal således, at for alle $x \neq 0$ i M er $\mathfrak{a}x \subset Rx$. Vis, at hvis $M \neq 0$, så er $\mathfrak{a}M \subset M$. [Vink: Indirekte, som i beviset for Nakayama's Lemma; brug, at en ligning $(1-a)e = 0$, med $a \in \mathfrak{a}$ og $e \in M$ medfører, at $e = 0$.

8. En ring R, hvori idealerne er totalt ordnede (dvs, at for vilkårlige to idealer $\mathfrak{a}$ og $\mathfrak{b}$ er enten $\mathfrak{a} \subseteq \mathfrak{b}$ eller $\mathfrak{b} \subseteq \mathfrak{a}$), kaldes en *valuationsring*. Vis, at i en valuationsring er ethvert endeligt frembragt ideal et hovedideal.

2. Moduler af endelig længde.

(2.1) Definition. Lad M være en R-modul. Ved *længden* af M forstås supremum af længderne af filtrationerne i M. Længden af M betegnes også long M. Længden kan være ∞, nemlig hvis der findes filtrationer i M af vilkårlig stor længde. At længden er endelig betyder, at der er en øvre grænse for længden af en filtration i M, altså en øvre grænse for hvor mange skarpe inklusioner, der kan være i en filtration af M.

I enhver modul $M \neq 0$ er $(0) \subset M$ en filtration af længde 1. Nulmodulen 0 er altså den eneste modul af længde 0.

(2.2) Sætning. *For en R-modul M er følgende betingelser ækvivalente:*

(i) *M har længde* 1.
(ii) *$M \neq 0$ og de eneste undermoduler i M er de trivielle, nemlig* (0) *og* M.
(iii) *$M \neq 0$ og for hvert element $v \neq 0$ i M gælder $M = Rv$.*
(iv) *M er modul-isomorf med en kvotient $R/\mathfrak{m}$, hvor $\mathfrak{m}$ er et maksimalideal i R.*

Bevis. At en modul M har længde mindst 2 betyder, at der i M findes en filtration

$$(0) \subset F_1 \subset M,$$

altså at M har en ikke-triviel undermodul. Betingelserne (i) og (ii) er derfor ækvivalente.

At (ii)$\Rightarrow$(iii) er klart. For hvert element $v \neq 0$ i M er Rv jo en undermodul, og $Rv \neq (0)$; hvis M kun har de trivielle undermoduler, må der altså gælde $Rv = M$. Antag omvendt, at (iii) er opfyldt. Lad $F_1 \neq (0)$ være en undermodul i M. Da $F_1 \neq (0)$, findes $v \neq 0$ i F_1. Af $Rv \subseteq F_1 \subseteq M$ og (iii) følger nu, at $F_1 = M$. Det er således vist, at M kun har de to trivielle undermoduler, så (ii) gælder.

Betingelserne (ii) og (iii) er således ækvivalente. Er de opfyldt, må M specielt være cyklisk ifølge (iii), altså isomorf med en kvotient $R/\mathfrak{m}$, hvor $\mathfrak{m}$ er et ideal i R. Det er derfor nok at vise for en kvotient $M = R/\mathfrak{m}$, at (ii) er opfyldt, hvis og kun hvis $\mathfrak{m}$ er et maximalideal. Denne sidste påstand følger umiddelbart af Noether's anden Isomorfisætning: undermodulerne i kvotienten $R/\mathfrak{m}$ svarer bijektivt til undermoduler (dvs idealer) $\mathfrak{a} \supseteq \mathfrak{m}$. □

(2.3) Definition. En modul M, der opfylder de ækvivalente betingelser i Sætning (2.2), kaldes en *simpel modul*.

Lad M være en modul, og betragt i M en filtration med skarpe inklusioner,

$$(0) = F_0 \subset F_1 \subset \cdots \subset F_n = M.$$

Undermoduler F mellem F_{i-1} og F_i, dvs som opfylder $F_{i-1} \subseteq F \subseteq F_i$, svarer ifølge Noether's anden Isomorfisætning til undermoduler af kvotienten F_i/F_{i-1}. Af betingelsen (2.2)(ii) følger derfor, at kvotienten F_i/F_{i-1} er en simpel modul, hvis og kun hvis der ikke findes undermoduler F, som ligger „ægte“ mellem F_{i-1} og F_i. Med andre ord: filtrationen er *uforfinelig*, hvis og kun hvis alle kvotienterne F_i/F_{i-1} er simple moduler.

Hvis modulen M har endelig længde, så findes naturligvis en sådan uforfinelig filtration i M. Vi skal senere se, at det omvendte også gælder.

(2.4) Sætning. *Lad der være givet en eksakt følge af moduler,*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0.$$

Da gælder formlen,

$$\operatorname{long} M = \operatorname{long} M' + \operatorname{long} M''.$$

Bevis. Vi kan antage, at M' er en undermodul i M og at $M'' = M/M'$ er den tilhørende kvotientmodul. Vi viser ligheden ved at vise de to uligheder.

„$\geqslant$“: Betragt to vilkårlige filtrationer i M' og M'',

$$(0) \subseteq F'_1 \subseteq \cdots \subseteq F'_{n-1} \subseteq M', \qquad (0) \subseteq F''_1 \subseteq \cdots \subseteq F''_{m-1} \subseteq M'',$$

og lad k' og k'' betegne længderne af filtrationerne. Ifølge Noether's anden Isomorfisætning svarer undermodulerne F''_i af kvotienten M'' til undermoduler F_i af M, således at $F_i \supseteq M'$. I M fås således en filtration,

$$(0) \subseteq F'_1 \subseteq \cdots \subseteq F'_{n-1} \subseteq M' \subseteq F_1 \cdots \subseteq F_{m-1} \subseteq M.$$

I denne filtration er der ialt $k' + k''$ skarpe inklusioner, så filtrationens længde er $k' + k''$. Altså er $k' + k'' \leqslant \operatorname{long} M$. Da filtrationerne i M' og M'' var vilkårlige, følger det endelig, at

$$\operatorname{long} M \geqslant \operatorname{long} M' + \operatorname{long} M''.$$

„$\leqslant$“: For at vise den omvendte ulighed betragtes en vilkårlig filtration i M,

$$(0) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = M.$$

Sæt $F'_i := F_i \cap M'$, og lad F''_i betegne billedet af F_i i kvotienten M/M'. Da udgør modulerne F'_i en filtration i undermodulen M', og modulerne F''_i udgør en filtration i kvotientmodulen M/M', og F'_i er kernen for den surjektive homomorfi $F_i \to F''_i$. Af Slangelemmaet får vi så eksakte følger,

$$0 \longrightarrow F'_i/F'_{i-1} \longrightarrow F_i/F_{i-1} \longrightarrow F''_i/F''_{i-1} \longrightarrow 0. \tag{*}$$

Lad nu k, k', k'' være længderne af filtrationerne i M, i M' og i M/M'. I (*) er den midterste modul altså forskellig fra 0 for k værdier af $i = 1, \dots n$. Af eksaktheden følger derfor, at for hver af disse k værdier af i er mindst én af de to moduler, F'_i/F'_{i-1} og F''_i/F''_{i-1}, forskellig fra 0. Den første er forskellig fra 0 for k' værdier af i, den anden er forskellig fra 0 for k'' værdier af i. Heraf fås uligheden,

$$k \leqslant k' + k''.$$

Ifølge definitionen er $k' \leqslant \operatorname{long} M'$ og $k'' \leqslant \operatorname{long} M''$. Uligheden ovenfor medfører derfor, at $k \leqslant \operatorname{long} M' + \operatorname{long} M''$. Da k var længden af en vilkårlig filtration i M, følger det endelig, at

$$\operatorname{long} M \leqslant \operatorname{long} M' + \operatorname{long} M''.$$

Hermed er den omvendte ulighed, og dermed den søgte formel, bevist. □

(2.5) Korollar. (1) *For en undermodul N i M gælder formlen,*

$$\operatorname{long} M = \operatorname{long} N + \operatorname{long} M/N.$$

(2) *For en filtration $0 = F_0 \subseteq \cdots \subseteq F_n = M$ gælder formlen,*

$$\operatorname{long} M = \sum \operatorname{long} F_i/F_{i-1}.$$

(3) *For en direkte sum $M = M_1 \oplus \cdots \oplus M_n$ gælder formlen,*

$$\operatorname{long} M = \sum \operatorname{long} M_i.$$

Bevis. (1) Da følgen $0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$ er eksakt, følger (1) umiddelbart af sætningen. Påstand (2) følger ved induktion efter n af sætningen ved hjælp af den eksakte følge,

$$0 \longrightarrow F_{n-1} \longrightarrow F_n \longrightarrow F_n/F_{n-1} \longrightarrow 0.$$

Endelig følger (3) af (2) ved at betragte filtrationen defineret ved $F_i := M_1 \oplus \cdots \oplus M_i$. □

(2.6) Bemærkning. Bemærk, at de anførte formler gælder, når der på oplagt måde regnes med ∞. Fx er det således en del af udsagnet i (2.5)(1), at modulen M har endelig længde, hvis og kun hvis både N og M/N har endelig længde.

(2.7) Korollar. *Modulen M har endelig længde, hvis og kun hvis der i M findes en uforfinelig filtration,*

$$(0) = F_0 \subset F_1 \subset \cdots \subset F_n = M. \tag{$*$}$$

Alle uforfinelige filtrationer har samme længde, nemlig længden af M.

Bevis. Hvis M har endelig længde, så findes øjensynlig en uforfinelig filtration $(*)$ med $n = \operatorname{long} M$. Antag omvendt, at $(*)$ er en uforfinelig filtration. Da er alle kvotienterne F_i/F_{i-1} simple moduler, dvs af længde 1. Tallet n er filtrationens længde. Af Korollar (2.5)(2) følger, at $\operatorname{long} M = n$. Hermed er påstandene bevist. □

(2.8) Eksempel. De simple $\mathbb{Z}$-moduler er kvotienterne $\mathbb{Z}/(p)$ for et primtal p. De er specielt endelige. Heraf følger let, at en $\mathbb{Z}$-modul M har endelig længde, hvis og kun hvis M er endelig. Antag, at M har længde n. I en uforfinelig filtration af M forekommer så kvotienterne $\mathbb{Z}/p_i$ for n ikke nødvendigvis forskellige primtal p_i. Det følger let, at der så gælder $|M| = p_1 \cdots p_n$.

De simple $\mathbb{C}[X]$-moduler er kvotienterne $\mathbb{C}[X]/(X-\alpha)$ for $\alpha \in \mathbb{C}$. De er specielt 1-dimensionale som vektorrum over $\mathbb{C}$. Heraf følger let, at en $\mathbb{C}[X]$-modul M har endelig længde, hvis og kun hvis M har endelig dimension som vektorrum over $\mathbb{C}$, og at der faktisk gælder ligheden $\operatorname{long} M = \dim_{\mathbb{C}} M$.

(2.9) Opgaver.

U4 **1.** Hvor langt er et vektorrum?

U4 **2.** Angiv i $\mathbb{Z}$ som $\mathbb{Z}$-modul en filtration af længde 999.

3. Vis, at enhver modul af endelig længde er endeligt frembragt.

U4 **4.** Vis, hvis ringen R som R-modul har endelig længde, så har enhver endeligt frembragt R-modul også endelig længde.

U8 **5.** Lad $0 \to M_n \to \cdots \to M_1 \to M_0 \to 0$ være en exakt følge af moduler af endelig længde. Vis, at $\sum(-1)^i \operatorname{long} M_i = 0$.

6. Vis, at en $\mathbb{R}[X]$-modul M har endelig længde, hvis og kun hvis M har endelig dimension som vektorrum over $\mathbb{R}$.

7. Lad $\mathfrak{m}$ være et fast maksimalideal i R. For hver uforfinelig filtration i en modul M kan vi spørge om antallet af gange den simple modul $R/\mathfrak{m}$ forekommer blandt filtrationens kvotienter. Lad $\operatorname{long}_{\mathfrak{m}} M$ betegne det største antal gange $R/\mathfrak{m}$ forekommer som simpel kvotient i en uforfinelig filtration af M. Vis, at $\operatorname{long}_{\mathfrak{m}} R/\mathfrak{m} = 1$, og at $\operatorname{long} R/\mathfrak{n} = 0$, når $\mathfrak{n}$ er et maksimalideal, $\mathfrak{n} \neq \mathfrak{m}$. Vis, for en undermodul M' af M, at $\operatorname{long}_{\mathfrak{m}} M = \operatorname{long}_{\mathfrak{m}} M' + \operatorname{long}_{\mathfrak{m}} M/M'$. Vis, at i enhver filtration af M forekommer $R/\mathfrak{m}$ som simpel kvotient præcis $\operatorname{long}_{\mathfrak{m}} M$ gange.

8. Antag, at R er et PID, og at $a = p_1^{\nu_1} \cdots p_r^{\nu_r}$ er en primopløsning. Bestem længden af R-modulen $R/(a)$.

U5 **9.** Antag, at R er et PID og ikke et legeme. Lad M være en endeligt frembragt R-modul. Vis, at M har endelig længde, hvis og kun hvis $\operatorname{Ann} M \neq (0)$.

10. Lad M være en endeligt frembragt modul over en noethersk ring R. Vis, at M har endelig længde, hvis og kun hvis der findes endelig mange maksimalidealer $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ (ikke nødvendigvis forskellige) i R således, at $\mathfrak{m}_1 \cdots \mathfrak{m}_n M = 0$.

Hvad udsiger resultatet, hvis R er lokal?

U9 **11.** Lad $f : M \to N$ være en homomorfi mellem moduler, der har den samme endelige længde. Vis, at følgende betingelser er ækvivalente: (i) f er surjektiv; (ii) f er injektiv; (iii) f er en isomorfi.

3. Lidt om noetherske ringe og moduler.

(3.1) Sætning. *For en modul M er følgende betingelser ækvivalente:*

(i) *Enhver undermodul i M er endeligt frembragt.*

(ii) *I enhver stigende kæde af undermoduler i M,*

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots ,$$

gælder lighed fra et vist trin.

(iii) *I enhver ikke-tom mængde $\mathcal{S}$ af undermoduler i M findes en undermodul, der er maksimal blandt undermodulerne i $\mathcal{S}$.*

Bevis. (i)⇒(ii): Betragt en kæde af undermoduler som i (ii), og dan foreningsmængden,

$$N := \bigcup_i M_i .$$

Foreningsmængden N er stabil under addition. Lad nemlig x og y være elementer i N. Da findes i, j så at $x \in M_i$ og $y \in M_j$. Det kan antages, at $i \leqslant j$. Men så er $M_i \subseteq M_j$, og undermodulen M_j vil altså indeholde både x og y og dermed også summen $x + y$. Følgelig tilhører $x + y$ foreningsmængden N.

Det er klart, at nul-elementet tilhører N, og det er let at vise, at N er stabil under multiplikation med skalar. Da N også er stabil under addition, er N derfor en undermodul. Ifølge antagelsen (i) er N endeligt frembragt. Der findes altså endelig mange elementer $v_1, \dots, v_m$ i N så at

$$N = Rv_1 + \cdots + Rv_m .$$

Hver af frembringerne v_k tilhører en af undermodulerne M_i. Af disse endelig mange M_i'er er en, fx M_n, den største. Da hver af frembringerne v_k tilhører M_n, gælder

$$N = Rv_1 + \cdots + Rv_m \subseteq M_n \subseteq M_{n+1} \subseteq \cdots \subseteq \bigcup M_i = N.$$

Det følger, at lighed gælder overalt i inklusionerne ovenfor. Specielt gælder altså at $M_n = M_{n+1} = \cdots$, hvormed (ii) er bevist.

(ii)⇒(i): Antag, indirekte, at der i M findes en undermodul N, der ikke er endeligt frembragt. Vælg et element v_1 i N (fx $v_1 = 0$), og sæt $M_1 := Rv_1$. Da $v_1 \in N$, er $M_1 \subseteq N$, og da N specielt ikke er frembragt af ét element, gælder endda

$$M_1 \subset N.$$

Vælg nu v_2 i overskudsmængden $N \setminus M_1$, og sæt $M_2 := M_1 + Rv_2$. Øjensynlig er $M_1 \subseteq M_2$, og da M_2 indeholder v_2, som var valgt i komplementærmængden til M_1, gælder endda $M_1 \subset M_2$. Videre er M_2 frembragt af v_1 og v_2, som begge var valgt i N; følgelig er $M_2 \subseteq N$. Da N specielt ikke kan være frembragt af to elementer, fås endda

$$M_1 \subset M_2 \subset N.$$

Vælg nu v_3 i overskudsmængden $N \setminus M_2$, og sæt $M_3 := M_2 + Rv_3$. Idet processen fortsættes induktivt, fås en uendelig følge af undermoduler,

$$M_1 \subset M_2 \subset M_3 \subset \cdots$$

(der alle er skarpt indeholdt i N). Da dette er i modstrid med antagelsen (ii), er det indirekte bevis fuldført.

(ii) $\iff$ (iii): Dette resultat gælder for enhver partielt ordnet mængde, og har intet at gøre med at vi her betragter undermoduler af en modul. Beviset overlades til læseren. □

(3.2) Noethersk modul. En modul M, der opfylder de ækvivalente betingelser (i), (ii), (iii) i Sætning (3.1), kaldes en *noethersk modul*.

Bemærk forskellen og ligheden i definitionen af „noethersk" og „endelig længde". At M er noethersk betyder at i en given kæde af undermoduler,

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots,$$

kan der kun være endelig mange skarpe inklusioner. At M har endelig længde betyder at der er en på forhånd given øvre grænse for antallet af skarpe inklusioner.

(3.3) Sætning. *Lad N være en undermodul i modulen M. Da er M noethersk, hvis og kun hvis både undermodulen N og kvotientmodulen M/N er noetherske.*

Bevis. Antag først, at N og M/N er noetherske. Vi efterviser, at M opfylder betingelsen (3.1)(i). Lad altså K være en undermodul i M. Billedet K'' af K i M/N er da en undermodul i M/N. Altså er K'' endeligt frembragt, da M/N er noethersk. Fællesmængden $K' := K \cap N$ er en undermodul i N. Altså er K' endeligt frembragt, da N er noethersk. Restriktion af den kanoniske afbildning $M \to M/N$ til undermodulen K giver en eksakt følge,

$$0 \longrightarrow K' \longrightarrow K \longrightarrow K'' \longrightarrow 0.$$

Af Sætning (1.3) følger derfor, at K er endeligt frembragt. Da K var en vilkårlig undermodul i M, er M således noethersk.

Antag omvendt, at M er noethersk. Enhver undermodul K i N er da specielt en undermodul i M, og derfor endeligt frembragt, da M er noethersk. Altså er N noethersk. Betragt dernæst en undermodul L i M/N. Ifølge Noether's anden Isomorfisætning er L så homomorft billede af en undermodul K af M (endda med $K \supseteq N$). Da M er noethersk er K endeligt frembragt, og det homomorfe billede L er derfor ligeledes endeligt frembragt, jfr Sætning (1.3). Altså er M/N noethersk. □

(3.4) Korollar. (1) *For en eksakt følge $0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$ gælder, at M er noethersk, hvis og kun hvis M' og M'' er noetherske.*

(2) *For en filtration $(0) = F_0 \subseteq \cdots \subseteq F_n = M$ gælder, at M er noethersk, hvis og kun hvis alle kvotienterne F_i/F_{i-1} er noetherske.*

(3) *For en direkte sum $M = M_1 \oplus \cdots \oplus M_n$ gælder, at M er noethersk, hvis og kun hvis alle addenderne M_i er noetherske.*

Bevis. Ifølge Isomorfisætningen er (1) blot en oversættelse af Sætningen. Påstand (2) følger ved induktion af (1), ved hjælp af den eksakte følge,

$$0 \longrightarrow F_{n-1} \longrightarrow F_n \longrightarrow F_n/F_{n-1} \longrightarrow 0.$$

Endelig følger (3) af (2) ved at betragte filtrationen i den direkte sum defineret ved $F_i := M_1 \oplus \cdots \oplus M_i$. ∎

(3.5) Definition. Ringen R kaldes en *noethersk ring*, hvis den er noethersk som R-modul. Undermodulerne i modulen R er netop idealerne i ringen R, så R er en noethersk ring, netop hvis ethvert ideal i R er endeligt frembragt.

(3.6) Sætning. *Antag, at ringen R er noethersk. Enhver endeligt frembragt R-modul er da noethersk. Desuden er enhver kvotientring af R en noethersk ring.*

Bevis. Modulen R^n er en direkte sum $R^n = R \oplus \cdots \oplus R$ med n addender. Af Korollar (3.4)(3) følger derfor, at R^n er en noethersk modul. Lad nu M være en endeligt frembragt R-modul. Da er M homomorft billede af R^n for passende n. Af Korollar (3.4)(1) følger derfor specielt, at M er noethersk.

Den sidste påstand følger af at idealerne i en kvotientring $R/\mathfrak{a}$ netop er undermodulerne i kvotientmodulen $R/\mathfrak{a}$. ∎

(3.7) Eksempel. Enhver endelig ring er noethersk. Ethvert legeme er en noethersk ring. Enhver hovedidealring er noethersk. Specielt: ringen $\mathbb{Z}$ og polynomiumsringen $k[X]$ over et legeme k er noetherske ringe.

(3.8) Hilbert's Basissætning. *Lad R være en noethersk ring. Da er også polynomiumsringen $R[X]$ en noethersk ring.*

Bevis. Vi viser, at polynomiumsringen $R[X]$ har egenskaben (3.1)(i). Betragt derfor et ideal $\mathfrak{A}$ i $R[X]$. Lad $\mathfrak{l} = \mathfrak{l}(\mathfrak{A})$ betegne mængden bestående af de ledende koefficienter for polynomierne i $\mathfrak{A}$, samt elementet 0. Elementet $a \in R$ tilhører så $\mathfrak{l}$, hvis og kun hvis der i idealet $\mathfrak{A}$ findes et polynomium af formen

$$aX^n + \cdots,$$

hvor „$\cdots$“ står for en sum af led af lavere grad end det første.

Vi viser først, at delmængden $\mathfrak{l}$ er et ideal i R. Det er klart, at 0 tilhører $\mathfrak{l}$. Videre følger af $a \in \mathfrak{l}$ og $r \in R$ at $ra \in \mathfrak{l}$, thi hvis $aX^n + \cdots$ tilhører $\mathfrak{A}$, så vil også polynomiet

$$raX^n + \cdots = r(aX^n + \cdots)$$

tilhøre $\mathfrak{A}$. Antag endelig, at $a, b \in \mathfrak{l}$. Der findes altså i $\mathfrak{A}$ polynomier af formen $aX^n + \cdots$ og $bX^m + \cdots$. Det kan fx antages, at $n \geqslant m$. Da $\mathfrak{A}$ er et ideal følger det, at også polynomiet

$$(a+b)X^n + \cdots = (aX^n + \cdots) + X^{n-m}(bX^m + \cdots)$$

vil tilhøre $\mathfrak{A}$. Altså er også $a + b$ element i $\mathfrak{l}$. Hermed er vist, at $\mathfrak{l}$ er et ideal i R.

Da R er noethersk, er idealet $\mathfrak{l}$ endeligt frembragt. Der findes altså endelig mange polynomier,

$$P_i = a_i X^{n_i} + \cdots ,$$

hvis ledende koefficienter a_i frembringer $\mathfrak{l}$. Lad nu n_0 være den største af graderne n_i, og lad $\mathfrak{A}_{<n_0}$ betegne mængden af polynomier, der tilhører $\mathfrak{A}$ og har grad mindre end n_0. Det er klart, at $\mathfrak{A}_{<n_0}$ er en R-modul, nemlig en undermodul i R-modulen $R[X]_{<n_0}$ bestående af alle polynomier af grad mindre end n_0. Den sidste R-modul er endeligt frembragt, nemlig frembragt af de n_0 monomier 1, X, ... , X^{n_0-1}. Da R er noethersk, følger det af Sætning (3.6) at $R[X]_{<n_0}$ er noethersk som R-modul. I undermodulen $\mathfrak{A}_{<n_0}$ findes derfor endelig mange polynomier Q_j, som frembringer $\mathfrak{A}_{<n_0}$ som R-modul.

Det påstås nu, at idealet $\mathfrak{A}$ i $R[X]$ er frembragt af de endelig mange polynomier P_i og Q_j. Lad $\mathfrak{B}$ betegne idealet frembragt af disse polynomier. Da polynomierne er valgt i $\mathfrak{A}$, er $\mathfrak{B} \subseteq \mathfrak{A}$. Omvendt skal det altså vises for hvert F i $\mathfrak{A}$, at F tilhører $\mathfrak{B}$. Denne påstand vises ved induktion efter graden n af F.

Hvis $n < n_0$ er påstanden klar, thi så tilhører F delmængden $\mathfrak{A}_{<n_0}$, og F er derfor endda en R-linearkombination af Q_j'erne.

Hvis $n \geqslant n_0$ betragtes den ledende koefficient a i F. Da $F \in \mathfrak{A}$, er $a \in \mathfrak{l}$. Følgelig er a en R-linearkombination af a_i'erne,

$$a = \sum r_i a_i .$$

Nu var $P_i = a_i X^{n_i} + \cdots$ og $n \geqslant n_0 \geqslant n_i$, så linearkombinationen,

$$G := \sum r_i X^{n-n_i} P_i ,$$

har grad n og ledende koefficient a. Linearkombinationen G har altså samme grad og samme ledende koefficient som F. Differensen $F - G$ har derfor lavere grad end F. Da G er en linearkombination af P_i'erne, vil G tilhøre $\mathfrak{B}$. Videre er $F - G$ et polynomium i $\mathfrak{A}$ og af lavere grad end F, så ifølge induktionsforudsætningen vil $F - G$ tilhøre $\mathfrak{B}$. Men så vil også $F = G + (F - G)$ tilhøre $\mathfrak{B}$, som påstået. Hermed er Sætningen bevist. □

(3.9) Korollar. *Polynomiumsringen $k[X_1, \dots, X_r]$ i r variable, hvor k er et legeme eller $k = \mathbb{Z}$, er en noethersk ring.*

Bevis. Påstanden gælder generelt, når k er noethersk. Den vises ved induktion. Basissætningen giver både starten, $r = 1$, og induktionsskridtet, idet

$$R[X_1, \dots, X_r] = R[X_1, \dots, X_{r-1}][X_r] .$$

□

(3.10) Note. Det er Korollar (3.9) for et legeme k, der er den oprindelige „basissætning“. Resultatet udsiger, at hvert ideal i $k[X_1, \dots, X_r]$ er frembragt af endelig mange polynomier, dvs har en endelig „basis“.

(3.11) Opgaver.

U4 **1.** Vis, at enhver kvadratisk talring R er noethersk. [Vink: Udnyt, at som $\mathbb{Z}$-modul er $R = \mathbb{Z}^2$, og at hvert ideal i R altså er en undergruppe af $\mathbb{Z}^2$.]

U4 **2.** Lad $\mathfrak{a}$ være et ideal i en noethersk ring R, og sæt $\mathfrak{r} = \operatorname{Rad}\mathfrak{a}$. Vis, at der findes et $N \in \mathbb{N}$ således, at $\mathfrak{r}^N \subseteq \mathfrak{a}$.

U4 **3.** Lad R være et noethersk integritetsområde. Vis, at „irreducible opløsninger eksisterer". Med andre ord: Vis, at hvert element $r \in R$, der ikke er 0 eller en enhed, kan skrives som produkt af irreducible elementer.

U4 **4.** Vis, at hvis et ideal $\mathfrak{a} \subset R$ ikke er et primideal, så findes idealer $\mathfrak{b}$, $\mathfrak{c}$ med $\mathfrak{a} \subset \mathfrak{b}$, $\mathfrak{a} \subset \mathfrak{c}$, og $\mathfrak{bc} \subseteq \mathfrak{a}$. Vis, at i en noethersk ring R vil hvert ideal indeholde et produkt af primidealer; mere præcist: til hvert ideal $\mathfrak{a}$ findes primidealer $\mathfrak{p}_i \supseteq \mathfrak{a}$ for $i = 1, \dots, s$ således, at $\mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq \mathfrak{a}$.

U5 **5.** Antag, at R er noethersk. Vis, at (0) er et produkt af primidealer: $(0) = \mathfrak{p}_1 \cdots \mathfrak{p}_s$. Vis, at hvert primideal $\mathfrak{p} \subset R$ indeholder et $\mathfrak{p}_i$. Specielt er de minimale blandt idealerne $\mathfrak{p}_i$ netop de minimale blandt primidealerne i R. Vis, at $\operatorname{Rad}(0) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$.

Vis for hvert ideal $\mathfrak{a}$, at der i mængden af primidealer $\mathfrak{p}$ med $\mathfrak{p} \supseteq \mathfrak{a}$ findes endelig mange minimale elementer. Vis, at hvis $\mathfrak{q}_1, \dots, \mathfrak{q}_q$ er disse minimale elementer, så er $\operatorname{Rad}(\mathfrak{a}) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_q$.

U5 **6.** Et ideal $\mathfrak{q}$ kaldes *irreducibelt*, hvis $\mathfrak{q}$ er et ægte ideal og $\mathfrak{q}$ ikke kan skrives som fællemængde $\mathfrak{q} = \mathfrak{a} \cap \mathfrak{b}$ af idealer, der er effektivt større end $\mathfrak{q}$. Vis, at et primideal er irreducibelt. Vis, at de irreducible idealer i $\mathbb{Z}$ er (0) og hovedidealerne (p^n) frembragt af en primtalspotens. Vis, at i en noethersk ring er hvert ideal $\mathfrak{a}$ en fællesmængde, $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$, af irreducible idealer $\mathfrak{q}_i$. (Her medregnes fællesmængden af ingen idealer som fremstillingen af R.)

U5 **7.** Lad M være en endeligt frembragt R-modul. Vis, at M er en noethersk modul, hvis og kun hvis kvotientringen $R/\operatorname{Ann} M$ er en noethersk ring.

U6 **8.** Antag, at M er en noethersk R-modul. Vis, for en vilkårlig multiplikativ delmængde S af R, at $S^{-1}M$ er en noethersk $S^{-1}R$-modul. [Vink: Enhver undermodul af $S^{-1}M$ har som bekendt formen $S^{-1}N$ med en undermodul $N \subseteq M$.]

9. Vis for hvert n-sæt $\alpha = (\alpha_1, \dots, \alpha_n)$ i k^n, at idealet $\mathfrak{m}_\alpha := (X_1 - \alpha_1, \dots, X_n - \alpha_n)$ består af de polynomier $f \in k[X_1, \dots, X_n]$ for hvilke $f(\alpha_1, \dots, \alpha_n) = 0$. Vis, når k er et legeme, at $\mathfrak{m}_\alpha$ er et maksimalideal.

10. Antag, at k er et uendeligt legeme. Vis, at hvis $f \in k[X_1, \dots, X_n]$ ikke er nul-polynomiet, så findes et $\alpha = (\alpha_1, \dots, \alpha_n) \in k^n$ med $f(\alpha) \neq 0$.

11. En partielt ordnet mængde $(\mathcal{M}, \preceq)$ kaldes *noethersk ordnet*, hvis der i enhver stigende kæde $x_1 \preceq x_2 \preceq x_3 \preceq \cdots$ gælder „=" fra et vist trin. Formuler en ækvivalent „maksimalitetsbetingelse". Ordningen kaldes *artinsk*, hvis den modsatte ordning er noethersk. Antag, at ordningen er både noethersk og artinsk. Vis, at så findes der i $\mathcal{M}$ en kæde $x_0 \prec x_1 \prec \cdots x_{n-1} \prec x_n$, som er *uforfinelig* i den forstand, at x_0 er minimalt element i $\mathcal{M}$, x_n er maksimalt element i $\mathcal{M}$ og for hvert i findes der intet element x med $x_{i-1} \prec x \prec x_i$. I almindelighed kan man ikke slutte, at der så er en øvre grænse for antallet at elementer i en uforfinelig kæde. Hvilket resultat kan man udlede, når $\mathcal{M}$ er mængden af undermoduler af en given modul M?

U5 **12.** Betragt R-homomorfier $\varphi\colon M \to N$ og $\psi\colon N \to P$. Vis, at $\operatorname{Ker}\varphi \subseteq \operatorname{Ker}\psi\varphi$ og at ψ inducerer en surjektiv homomorfi $\varphi(M) \to \psi\varphi(M)$. Vis, at $\operatorname{Ker}\varphi = \operatorname{Ker}\psi\varphi$, hvis og kun hvis den inducerede homomorfi er en isomorfi $\psi\colon \varphi(M) \to \psi\varphi(M)$.

Vis, at hvis M er noethersk, så er enhver surjektiv homomorfi $M \to M$ automatisk en isomorfi.

U5 **13.** Vis, at enhver noethersk modul $M \neq 0$ har en simpel kvotientmodul.

14. To af de egenskaber, der karakteriserer noetherske moduler ved deres undermoduler, hedder, henholdvis, „den opstigende kædes egenskab", og „maksimalitetsegenskaben". Præciser hvilke! Formuler tilsvarende „den nedstigende kædes egenskab" og „minimalitetsegenskaben", og vis at de to sidste egenskaber er ækvivalente. En modul, der har de to egenskaber, kaldes *artinsk*. Vis, at enhver artinsk modul har en simpel undermodul.

15. Vis, at en R-modul M har endelig længde, hvis og kun hvis M er både noethersk og artinsk.

16. Lad p være et primtal, og lad $C_{p^\infty} \subset \mathbb{C}^*$ være foreningsmængden af undergrupperne:

$$C_1 \subset C_p \subset C_{p^2} \subset \cdots, \qquad (*)$$

Vis, at C_{p^∞} er en gruppe, og at undergrupperne i $(*)$ er de eneste ægte undergrupper af C_{p^∞}. Vis, at C_{p^∞} er artinsk som $\mathbb{Z}$-modul.

17. Vis, for et primtal p, at $M := \mathbb{Z}[1/p]/\mathbb{Z}$ er artinsk som $\mathbb{Z}$-modul. [Vink 1: Vis, at undergrupperne $\mathbb{Z}(1/p)^n/\mathbb{Z}$ for $n = 0, 1, 2, \dots$ er de eneste ægte undergrupper af M. Eller Vink 2: Vis, at M er relateret til gruppen C_{p^∞}.]

18. Antag, at nul-idealet i R er et produkt af maksimalidealer, $(0) = \mathfrak{m}_1 \cdots \mathfrak{m}_r$. Vis, at så er følgende betingelser er ækvivalente: (i) R er noethersk; (ii) R er artinsk; (iii) R har endelig længde. [Vink: I filtrationen af R bestemt ved $F_i := \mathfrak{m}_1 \cdots \mathfrak{m}_i$ har hver af de successive kvotienter formen $F/\mathfrak{m}F$; specielt er hver kvotient en modul over en kvotientring $R/\mathfrak{m}$, altså et vektorrum. Brug nu, at for vektorrum er de tre betingelser trivielt ækvivalente.]

19. Vis, at R (som modul over sig selv) er artinsk, hvis og kun hvis R har endelig længde. [Vink: Antag, at R er artinsk. Det er nok at vise, at (0) er produkt af maksimalidealer. Vælg $\mathfrak{d}$ minimalt blandt de idealer, der er produkter af maksimalidealer, og sæt $\mathfrak{a} = \operatorname{Ann}\mathfrak{d}$. Så er $\mathfrak{a}$ det største ideal med $\mathfrak{a}\mathfrak{d} = 0$. Antag, indirekte, at $\mathfrak{d} \neq (0)$. Så er $1 \notin \mathfrak{a}$, og kvotienten $R/\mathfrak{a}$ er ikke nul. Slut heraf, at $R/\mathfrak{a}$ har en simpel undermodul, svarende til et ideal $\mathfrak{b}$ med $\mathfrak{a} \subset \mathfrak{b}$ og $\mathfrak{b}/\mathfrak{a} = R/\mathfrak{m}$. Nu er $\mathfrak{m}\mathfrak{b} \subseteq \mathfrak{a}$, og dermed er $\mathfrak{m}\mathfrak{b}\mathfrak{d} = 0$. Øjensynlig er $\mathfrak{m}\mathfrak{d} \subseteq \mathfrak{d}$ er produkt af maksimal idealer, så valget af $\mathfrak{d}$ sikrer, at $\mathfrak{m}\mathfrak{d} = \mathfrak{d}$. Altså er $\mathfrak{b}\mathfrak{d} = (0)$, men da $\mathfrak{a} \subset \mathfrak{b}$ er det er i modstrid med definitionen af $\mathfrak{a}$.

20. Vis, at en endeligt frembragt R-modul er artinsk, hvis og kun hvis den har endelig længde.

U6 **21.** Lad M være en R-modul, og betragt den direkte sum $R \oplus M$. Vis, at med kompositionen $(r, x)(s, y) = (rs, ry + sx)$ som multiplikation er $R \oplus M$ en kommutativ ring. (Tænker man på (r, x) som $r + x$, er multiplikationen bestemt ved $xy = 0$ for $x, y \in M$.) Antag, at $R = k$ er et legeme. Vis, at $k \oplus M$ er en lokal ring med kun ét primideal. Hvornår er $k \oplus M$ noethersk? – artinsk? – af endelig længde?

4. Endeligt frembragte algebraer. Hele udvidelser.

(4.1) Algebra og delalgebra. Lad der være givet en ringhomomorfi $\theta\colon R \to A$. Ringen A organiseres da som R-modul med multiplikationen defineret ved

$$ra := \theta(r)a \qquad \text{for } r \in R,\ a \in A.$$

Når ringhomomorfien θ er givet, siges A også at være en *algebra over* R eller en R-algebra. Specielt: hvis R er en delring af A, så kan A opfattes som algebra over R.

Når A er en R-algebra kan enhver delring $B \subseteq A$, som omfatter $\theta(R)$, selv opfattes som R-algebra. En sådan delring kaldes også en *delalgebra* af A.

(4.2) Lemma. *Lad A være en R-algebra, og lad M være en A-modul. Hvis M er endeligt frembragt som A-modul og A er endeligt frembragt som R-modul, så er M endeligt frembragt som R-modul.*

Bevis. Den givne A-modul M opfattes naturligt som R-modul, idet produktet rx for $r \in R$ og $x \in M$ defineres ved $rx := \theta(r)x$.

Antag nu, at n elementer $e_1, \dots, e_n$ i M frembringer M som A-modul, og at p elementer $v_1, \dots, v_p$ i A frembringer A som R-modul. Det påstås, at de np elementer $v_i e_j$ i M frembringer M som R-modul. Lad nemlig x være element i M. Da har x en fremstilling,

$$x = a_1 e_1 + \cdots + a_n e_n, \tag{$*$}$$

som A-linearkombination af e_j'erne. Koefficienterne a_j tilhører A, og hver koefficient a_j har derfor en fremstilling som R-linearkombination af v_i'erne. Indsættes for hvert a_j i $(*)$ en sådan fremstilling, fås en fremstilling af x som R-linearkombination af $v_i e_j$'erne, som ønsket. □

(4.3) Endeligt frembragt algebra. Lad A være en R-algebra. For givne elementer $a_1, \dots, a_m$ i A betegnes da med

$$R[a_1, \dots, a_m]$$

delmængden af A bestående af de elementer, der er R-linearkombinationer af endelig mange af de endelige produkter,

$$a_1^{i_1} a_2^{i_2} \cdots a_m^{i_m}.$$

Øjensynlig er denne delmængde en delring af A, endda den mindste, der indeholder billedringen $\theta(R)$ og alle a_i'erne. Specielt er delmængden selv en R-algebra; den kaldes *delalgebraen frembragt* af a_i'erne.

En given R-algebra A siges at være *endeligt frembragt* (mere udførligt: *endeligt frembragt som R-algebra*), hvis der i A findes endelig mange elementer $a_1, \dots, a_m$, som *frembringer algebraen A*, dvs opfylder at

$$A = R[a_1, \dots, a_m].$$

Algebraen A er specielt en R-modul, men det skal understreges, at en endeligt frembragt algebra ikke nødvendigvis er endeligt frembragt som R-modul.

(4.4) Definition. Polynomiumsringen $R[X_1, \dots, X_m]$ er en R-algebra, idet R kan opfattes som delringen bestående af de konstante polynomier. Polynomiumsringen er endeligt frembragt som R-algebra, nemlig frembragt af de variable $X_1, \dots, X_m$.

For givne elementer $a_1, \dots, a_m$ i en R-algebra A defineres en R-lineær ringhomomorfi $R[X_1, \dots, X_m] \to A$ ved

$$\sum r_{i_1,\dots,i_m} X_1^{i_1} \cdots X_m^{i_m} \quad \mapsto \quad \sum r_{i_1,\dots,i_m} a_1^{i_1} \cdots a_m^{i_m}.$$

Billedet af et polynomium $P \in R[X_1, \dots, X_m]$ ved denne afbildning betegnes også

$$P(a_1, \dots, a_m),$$

og det siges at fremkomme ved at *indsætte* $a_1, \dots, a_m$ i P. Billedet for denne ringhomomorfi er øjensynlig delalgebraen frembragt af a_i'erne. Billedet af det konstante polynomium $r \in R$ er elementet $r1_A = \theta(r)$ i A; hvis misforståelser er udelukkede skrives blot r for dette element i A.

Givne elementer $a_1, \dots, a_m$ i A siges at være *algebraisk uafhængige* over R, eller *transcendente* over R, hvis homomorfien defineret ved indsættelse er injektiv. Hvis homomorfien ikke er injektiv, kaldes elementerne *algebraisk afhængige* over R.

(4.5) Observation. Af definitionerne følger let, at en R-algebra A er endeligt frembragt over R, hvis og kun hvis A er homomorft billede af en polynomiumsring $R[X_1, \dots, X_m]$ for passende m, altså hvis og kun hvis A er isomorf med en kvotient $R[X_1, \dots, X_m]/\mathfrak{A}$, hvor $\mathfrak{A}$ er et ideal.

Specielt følger det, at en algebra, der er endeligt frembragt over en noethersk ring R, selv er en noethersk ring.

(4.6) Sætning. *Lad A være en R-algebra. For hvert element a i A er følgende betingelser ækvivalente:*

(i) *Der findes et normeret polynomium P i $R[X]$ så at $P(a) = 0$. Med andre ord: der findes i A en relation af formen $a^n + r_1a^{n-1} + \cdots + r_n = 0$, hvor r_i'erne tilhører R.*
(ii) *Delalgebraen $R[a]$ af A er endeligt frembragt som R-modul.*
(iii) *Der findes en delalgebra B af A, som er endeligt frembragt som R-modul og indeholder a.*

Bevis. (i)⇒(ii). Antag, at a tilfredsstiller en ligning,

$$a^n + r_1a^{n-1} + \cdots + r_n = 0, \tag{$*$}$$

hvor r_i'erne tilhører R. Det påstås, at elementerne $1, a, \dots, a^{n-1}$ frembringer $R[a]$ som R-modul. Det er øjensynlig nok at vise, at hver potens a^p er en R-linear kombination af $1, \dots, a^{n-1}$. Dette vises ved induktion efter p. For $p < n$ er det klart. Antag, at påstanden gælder for a^p, dvs at der gælder en ligning,

$$a^p = s_n + s_{n-1}a + \cdots + s_1a^{n-1},$$

hvor $s_1, \dots, s_n$ tilhører R. Multipliceres denne ligning med a fås ligningen

$$a^{p+1} = \big(s_n a + s_{n-1}a^2 + \cdots + s_2 a^{n-1}\big) + s_1 a^n. \tag{$**$}$$

Af $(*)$ ses, at $a^n = -r_n - r_{n-1}a - \cdots - r_1 a^{n-1}$. Specielt er a^n en R-linearkombination af $1, \dots, a^{n-1}$. Erstattes a^n på højresiden af $(**)$ med denne linearkombination fås en fremstilling af a^{p+1} som R-linearkombination af $1, \dots, a^{n-1}$, som ønsket.

(ii)⇒(iii). Hvis (ii) gælder, så kan $B := R[a]$ øjensynlig anvendes i (iii).

(iii)⇒(i). Antag, at B er en delalgebra af A, frembragt som R-modul af elementer $b_1, \dots, b_m$, og at $a \in B$. Da B er en delring og $a \in B$, gælder for hvert b i B, at produktet ab tilhører B; produktet ab har altså en fremstilling som en R-linearkombination af b_i'erne. Skrives koefficienterne i en sådan fremstilling som en søjlematrix α, fås altså en matrixligning af formen,

$$ab = (b_1, \dots, b_m)\alpha.$$

Specielt fås for $i = 1, \dots, m$ en sådan ligning for $b = b_i$, og disse ligninger kan under ét skrives som en matrixligning,

$$a(b_1, \dots, b_m) = (b_1, \dots, b_m)\alpha,$$

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

$$(b_1, \dots, b_m)(a1_m - \alpha) = 0,$$

hvor 1_m betegner enhedsmatricen. Betragt nu determinanten $d := \det(a1_m - \alpha)$ i A. Af matrixligningen følger ved hjælp af Cramer's formler, at $(b_1, \dots, b_m)d = 0$. Determinanten d annullerer derfor alle b_i'erne, og dermed også enhver linearkombination af b_i'erne. Da B er frembragt som R-modul af b_i'erne, vil d annullere ethvert element i B. Specielt vil d annullere et-elementet 1_A, som jo tilhører B. Følgelig er $d = 0$. Da matricen α har koefficienter i R, er det på den anden side klart, at $d = \det(a1_m - \alpha)$ har formen,

$$d = a^m + r_1 a^{m-1} + \cdots + r_m,$$

hvor $r_1, \dots, r_m$ tilhører R. Ligningen $d = 0$ viser derfor, at betingelsen (i) er opfyldt.

Hermed er Sætningen bevist. □

(4.7) Definition. Lad A være en R-algebra, givet ved ringhomomorfien $\theta\colon R \to A$. Et element a i A, som opfylder de ækvivalente betingelser i Sætning (4.6), siges at være *helt over* R. Hvis alle elementer i A er hele over R, siges afbildningen θ at være en *hel homomorfi*, og algebraen A siges at være *hel over* R.

Øjensynlig er A hel over R, netop når A er hel over delringen $\theta(R)$.

Hvis R-algebraen A er endeligt frembragt som R-modul, da er A hel over R, dvs hvert element a i A er helt over R. Som delalgebra B i betingelsen (4.6)(iii) kan nemlig i så fald bruges $B = A$.

(4.8) Korollar. *Lad A være en R-algebra. Elementer $a_1, \dots, a_m$ i A er da hele over R, hvis og kun hvis delalgebraen $R[a_1, \dots, a_m]$ er endeligt frembragt som R-modul.*

Bevis. Delalgebraen $R[a_1, \dots, a_m]$ indeholder a_i'erne. Af betingelsen (4.6)(iii) følger derfor, at hvis delalgebraen er endeligt frembragt som R-modul, så er hvert af a_i'erne hele over R.

Den omvendte implikation vises ved induktion efter m. For $m = 1$ følger påstanden direkte af definitionen, jfr betingelsen (4.6)(ii). Antag nu, at elementer $a_1, \dots, a_{m+1}$ i A er hele over R, og at påstanden gælder for m elementer. Sæt $B := R[a_1, \dots, a_m]$. Øjensynlig er $R[a_1, \dots, a_m, a_{m+1}] = B[a_{m+1}]$, og det skal vises, at denne algebra er endeligt frembragt som R-modul. Da a_{m+1} er hel over R, er a_{m+1} også hel over B. Følgelig er $B[a_{m+1}]$ endeligt frembragt som B-modul. Af induktionsforudsætningnen følger, at B er endeligt frembragt som R-modul. Af Lemma (4.2) følger nu, at $B[a_{m+1}]$ er endeligt frembragt som R-modul, som ønsket. □

(4.9) Korollar. *Sum og produkt af hele elementer a, b i A er igen hele. Elementerne i A, som er hele over R, udgør en delalgebra af A.*

Bevis. Ifølge det foregående korollar er $R[a, b]$ endeligt frembragt som R-modul. Da både summen $a + b$ og produktet ab tilhører $R[a, b]$, følger det af betingelsen (4.6)(iii), at $a + b$ og ab er hele over R. Heraf følger videre den sidste påstand, idet elementerne i $\theta(R)$ er hele over R; elementet $a := \theta(r)$ i A opfylder jo ligningen $a - r1_A = 0$. □

(4.10) Korollar. *Antag, at A er hel over R. Lad $A \to C$ være en ringhomomorfi. Hvert element i C, der er helt over A, vil da også være helt over R. Hvis homomorfien $A \to C$ er hel, da er også den sammensatte homomorfi $R \to C$ hel.*

Bevis. Betragt i C et element c, der er helt over A. Det skal vises, at c er hel over R. Da c er hel over A, findes en relation,

$$c^n + a_1 c^{n-1} + \cdots + a_n = 0,$$

hvor a_i'erne tilhører A. Af denne relation fremgår, at c er hel over delalgebraen $B := R[a_1, \dots, a_n]$ af A. Altså er $B[c]$ endeligt frembragt som B-modul. Da A er hel over R og B er en delring af A, er B hel over R. Af Korollar (4.8) følger derfor, at B er endeligt frembragt som R-modul. Altså følger det af Lemma (4.2), at algebraen $B[c]$ er endeligt frembragt som R-modul. Da c tilhører denne delalgebra af C, er c hel over R. Hermed er Korollarets første påstand bevist.

Den sidste påstand følger trivielt af den første. □

(4.11) Sætning. *Lad R være en faktoriel ring. Enhver brøk i brøklegemet for R, som er hel over R, vil da tilhøre R.*

Bevis. Betragt en brøk r/s, hvor $s \neq 0$. Da R er faktoriel, kan r, s vælges primiske. Antag, at r/s er hel over R. Der findes altså i brøklegemet en relation,

$$(r/s)^n + r_1 (r/s)^{n-1} + \cdots + r_n = 0.$$

Multipliceres med s^n fås en ligning i R,

$$s(-r_1r^{n-1} - r_2r^{n-2}s - \cdots - r_ns^{n-1}) = r^n.$$

Af denne ligning følger, at enhver primdivisor i s er divisor i r^n og dermed i r. Følgelig har s ingen primdivisorer, og s er derfor invertibel i R. Altså er $r/s = rs^{-1}$ element i R. ▯

(4.12) Note. Delalgebraen af A beskrevet i (4.9) kaldes den *hele afslutning* af R i A. Hvis den kun består af billedet af R i A, kaldes R *helt afsluttet* i A. Af (4.10) følger, at den hele afslutning er helt afsluttet.

Sætning (4.11) udsiger, at et UFD er helt afsluttet i sit brøklegeme. Sætningen generaliserer i øvrigt en del af følgende sætning kendt fra gymnasiet: Hvis et polynomium med hele koefficienter har en rational rod skrevet som uforkortelig brøk r/s, så går r op i konstantleddet og s går op i højestegradskoefficienten.

(4.13) Noether's Normaliseringslemma. *Lad k være et legeme og lad $A \neq 0$ være en algebra over k frembragt af m elementer $a_1, \dots, a_m$. Da findes i A et sæt af $t \leqslant m$ elementer $x_1, \dots, x_t$, der er algebraisk uafhængige over k og således at A er endeligt frembragt som modul over delalgebraen $k[x_1, \dots, x_t]$.*

Bevis. Påstanden vises ved induktion efter m. For $m = 0$ (forudsætningen er her, at $k \to A$ er surjektiv) er påstanden triviel.

Antag nu at $m > 0$, og at påstanden er vist for algebraer frembragt af færre end m elementer. Hvis de givne elementer $a_1, \dots, a_m$ er algebraisk uafhængige, er påstanden triviel: vi kan bruge $t = m$ og $x_i = a_i$ for $i = 1, \dots, m$. Antag derfor, at a_i'erne er algebraisk afhængige, dvs at der findes en relation,

$$\sum r_{i_1,\dots,i_m} a_1^{i_1} \cdots a_m^{i_m} = 0, \tag{$*$}$$

hvor koefficienterne $r_{i_1,\dots,i_m}$ tilhører k, og hvor ikke alle koefficienterne er 0. Lad nu $g_1, \dots, g_{m-1}$ være et sæt af $m-1$ positive eksponenter, og sæt

$$b_i := a_i - a_m^{g_i} \quad \text{for } i = 1, \dots, m-1.$$

Det er nok at vise, at hvis g_j'erne vælges passende, så er a_m hel over delalgebraen $B := k[b_1, \dots, b_{m-1}]$. Antag nemlig, at a_m er hel over B. Da er $B[a_m]$ endeligt frembragt som B-modul. For $i = 1, \dots, m-1$ er $a_i = b_i + a_m^{g_i}$, og altså er $a_i \in B[a_m]$. Da A er frembragt som k-algebra af a_i'erne, følger det at $A = B[a_m]$. Altså er A endeligt frembragt som B-modul. Videre følger det af induktionsforudsætningen, at der findes $t \leqslant m-1$ elementer i B, der er algebraisk uafhængige over k, og således at B er endeligt frembragt som modul over $k[x_1, \dots, x_t]$. Af Lemma (4.2) følger, at A er endeligt frembragt som modul over $k[x_1, \dots, x_t]$, og så er påstanden vist for algebraen A.

Vi viser nu, at g_j'erne kan vælges passende. Ifølge definitionen er $a_i = b_i + a_m^{g_i}$ for $i = 1, \dots, m-1$. Indsættes disse ligninger i ligningen $(*)$ fremkommer på venstresiden en sum af udtryk af formen,

$$r_{i_1,\dots,i_m}(b_1 + a_m^{g_1})^{i_1} \cdots (b_{m-1} + a_m^{g_{m-1}})^{i_{m-1}} a_m^{i_m}.$$

I dette udtryk kan vi udføre multiplikationerne (binomialformlen), og ordne efter potenser af a_m. Hver potens af a_m kommer da med en koefficient, der afhænger af b_j'erne. Disse koefficienter tilhører altså delalgebraen B. Den højeste eksponent til a_m er øjensynlig $g_1 i_1 + \cdots + g_{m-1} i_{m-1} + i_m$, og den hertil hørende koefficient er blot $r_{i_1,\dots,i_m}$. Udtrykket har altså formen

$$r_{i_1,\dots,i_m} a_m^{g_1 i_1 + \cdots + g_{m-1} i_{m-1} + i_m} + \cdots, \tag{$**$}$$

hvor de tre prikker står for en B-linearkombination af potenser af a_m med lavere eksponent end den første.

I den givne relation $(*)$ er $r_{i_1,\dots,i_m}$'erne kun forskellige fra 0 for endelig mange sæt $i_1, \dots, i_m$. Svarende til disse endelig mange sæt $i_1, \dots, i_m$ vælger vi nu g_j'erne, så at de tilhørende eksponenter $i_1 g_1 + \cdots + i_{m-1} g_{m-1} + i_m$ er indbyrdes forskellige. At et sådant valg er muligt kan indses således: Vi betragter kun endelig mange sæt $i_1, \dots, i_m$, så der findes et naturligt tal g som er skarpt større end hvert af de optrædende i_ν'er. Med dette g vælger vi $g_j := g^{m-j}$. De tilhørende eksponenter er da

$$i_1 g^{m-1} + \cdots + i_{m-1} g + i_m g^0.$$

Exponenterne svarende til de endelig mange sæt $i_1, \dots, i_m$ er da indbyrdes forskellige, thi da $i_\nu \leqslant g - 1$ er sættet simpelthen cifrene, når eksponenten skrives i g-talssystemet.

Med dette valg af g_j'erne opnås det ønskede. For de endelig mange sæt $i_1, \dots, i_m$, for hvilke $r_{i_1,\dots,i_m} \neq 0$, er de tilsvarende eksponenter $i_1 g^m + \cdots + i_{m-1} g + i_m g^0$ nu forskellige, så blandt dem findes èn, der er størst. Lad N være den største eksponent, og lad r være den tilhørende koefficient. Blandt udtrykkene $(**)$ forekommer så udtrykket $r a_m^N + \cdots$, og i alle andre udtryk forekommer a_m med en eksponent mindre end N. Ved addition af udtrykkene $(**)$ og udnyttelse af ligningen $(*)$ får vi derfor en relation,

$$r a_m^N + \cdots = 0,$$

hvor de tre prikker står for en B-linearkombination af potenser af a_m med eksponent mindre end N. Ifølge valget er $r \neq 0$. Da k er et legeme, kan relationen derfor multipliceres med r^{-1}. Det følger af den fremkomne relation, at a_m er hel over B. Hermed er det ønskede opnået, og Normaliseringslemma'et bevist. □

(4.14) Lemma. *Lad A være et integritetsområde, og antag, at A er hel over en delring R. Da er A et legeme, hvis og kun hvis R er et legeme.*

Bevis. Antag først, at A er et legeme. Det skal så vises for hvert element $r \neq 0$ i R, at r er et invertibelt element i R. Da A er et legeme, har r et inverst element a i A. Ifølge antagelsen er elementet a helt over R. Der findes altså en relation i A,

$$a^m + r_1 a^{m-1} + \cdots + r_m = 0,$$

hvor r_i'erne tilhører R. Multiplicer denne relation med r^m. Da $ra = 1$ fås følgende ligninger,

$$0 = 1 + r r_1 + r^2 r_2 + \cdots + r^m r_m = 1 + r(r_1 + \cdots + r_m r^{m-1}).$$

Heraf aflæses, at summen i parentesen, bortset fra fortegnet, er det inverse til r. Da summen tilhører R, aflæses specielt, at det inverse til r er element i R.

Antag dernæst, at R er et legeme. Lad a være et element forskelligt fra 0 i A. Det skal vises, at a er invertibelt i ringen A. Vælg hertil blandt de normerede polynomier i $R[X]$ med a som rod et af lavest grad. At a er rod i polynomiet, kan omskrives til en ligning,

$$a(a^{n-1} + r_1 a^{n-2} + \cdots + r_1) = -r_0, \tag{*}$$

hvor n er graden og $r_0, \dots, r_n \in R$. Ringen R er et integritetsområde og $a \neq 0$. Hvis $r_0 = 0$, kunne det derfor sluttes, at parentesen er 0, altså at a er rod i et normeret polynomium af grad $n-1$, i modstrid med valget. Altså er $r_0 \neq 0$, og derfor har r_0 en invers i legemet R. Multiplikation af ligningen (*) med $-r_0^{-1}$ giver umiddelbart den inverse til a. □

(4.15) Hilbert's Nulpunktssætning, version 1. *Lad k være et legeme, og lad A være en endeligt frembragt algebra over k. Antag, at A er et legeme. Da er A et endeligdimensionalt vektorrum over k.*

Bevis. Ifølge Noether's Normaliseringslemma findes i A elementer $x_1, \dots, x_t$, der er algebraisk uafhængige over k og således at A er endeligt frembragt som modul over delringen $k[x_1, \dots, x_t]$. Da A er et legeme, følger det af Lemma (4.14), at også denne delring er et legeme. Da elementerne $x_1, \dots, x_t$ er algebraisk uafhængige over k, er delringen isomorf med polynomiumsringen over k i t variable. Øjensynlig er en sådan polynomiumsring kun et legeme, hvis $t = 0$. Delringen er altså blot k. Algebraen A er altså endeligt frembragt som modul over legemet k. Med andre ord: A er endeligdimensional over k. □

(4.16) Opgaver.

1. Lad R være et integritetsområde med brøklegeme K, og antag, at K er dellegeme af et legeme L. Hvis $\alpha \in L$ er algebraisk over K, betegnes med $f_{\alpha/K}$ det *minimale polynomium* for α, dvs det normerede polynomium af lavest grad i $K[X]$, der har α som rod. Antag, at R er helt afsluttet i K. Vis, at α er hel over R, hvis og kun hvis α er algebraisk over K og $f_{\alpha/K}$ har koefficienter i R.

2. Gennemfør følgende bevis for Noether's Normaliseringslemma. Lad $A := k[a_1, \dots, a_m]$ være den givne algebra. Antag, at der findes en egentlig relation $F(a_1, \dots, a_m) = 0$, hvor F ikke er nul-polynomiet. Betragt et sæt af $m-1$ skalarer $\lambda_1, \dots, \lambda_{m-1} \in k$, og sæt

$$b_i := a_i - \lambda_i a_m \quad \text{for } i = 1, \dots, m-1.$$

Det skal vises, at skalarerne kan vælges sådan, at a_m er hel over $k[b_1, \dots, b_{m-1}]$ (thi så bliver $k[a_1, \dots, a_m]$ hel over $k[b_1, \dots, b_{m-1}]$). Lad d være graden af F, og altså $F = F_d + \cdots + F_1 + F_0$, hvor F_i er homogen af grad d. Vi har $a_i = b_i + \lambda_i a_m$, og altså ligningen,

$$F(b_1 + \lambda_1 a_m, \dots, b_{m-1} + \lambda_{m-1} a_m, a_m) = 0.$$

Ordnes efter potenser af a_m fås en ligning af grad højst d i a_m, og koefficienten til a_m^d kommer fra F_d. Det bliver en skalar:

$$0 = F(b_1 + \lambda_1 a_m, \dots, b_{m-1} + \lambda_{m-1} a_m, a_m) = F_d(\lambda_1, \dots, \lambda_{m-1}, 1)a_m^d + \dots .$$

Nu var $F_d(X_1, \dots, X_m)$ homogent og ikke nul-polynomiet, og så er $F_d(X_1, \dots, X_{m-1}, 1)$ ikke nul-polynomiet. Vælg nu skalarerne sådan, at koefficienten $F_d(\lambda_1, \dots, \lambda_{m-1}, 1) \neq 0$. Division med denne koefficient giver så en „helhelds"-relation for a_m over $k[b_1, \dots, b_{m-1}]$.

Den væsentlige fordel ved dette bevis er, at den givne algebra bliver hel over algebraisk uafhængige elementer, der er *linearkombinationer* af de givne $a_1, \dots, a_m$. Ulempen er, at beviset kun fungerer, når legemet k er uendeligt. Hvorfor denne sidste indskrænkning?

U9 **3.** Lad k være et legeme, og lad $A := k^{\mathbb{N}}$ være ringen af alle følger $\alpha_1, \alpha_2, \dots$ med $\alpha_i \in k$. Vis, at de følger, der er konstante fra et vist trin, udgør en delring R af A. For en følge (α_i) i R betegnes med α_∞ følgens konstante værdi α_j for $j \gg 0$. Vis, for hvert $i = 1, 2, \dots, \infty$, at følgerne $\alpha \in R$ med $\alpha_i = 0$ udgør et maksimalideal $\mathfrak{m}_i$ i R, og at disse idealer er samtlige primidealer i R. [Vink: Lad $\mathfrak{p}$ være et primideal i R. Betragt, for $i = 1, 2, \dots$, hovedidealet (δ_i) i R (hvor δ_i er Kronecker's delta, $\delta_{ij} = 1$ når $j = i$ og $\delta_{ij} = 0$ når $j \neq i$). Udnyt, at $(\delta_i)\mathfrak{m}_i = (0) \subseteq \mathfrak{p}$.]

Vis, at de følger, der kun antager endelig mange værdier, udgør en delring R' af A [Så $R' = A$, hvis k er et endeligt legeme]. Vis, at R' er den hele afslutning af R i A. Kan du bestemme et maksimalideal i R', der ligger over $\mathfrak{m}_i$? – Også for $i = \infty$?

U9 **4.** Betragt i polynomiumsringen $k[T]$ (k er et legeme) polynomierne $x = T^2$ og $y = T^3$, og delalgebraen $k[x, y]$ af $k[T]$. Vis, at kernen for den naturlige homomorfi $k[X, Y] \to k[x, y]$ (bestemt ved $f \mapsto f(x, y)$) er idealet $\mathfrak{p} := (X^3 - Y^2)$. [Vink: Regn modulo det sidste ideal, dvs at man i monomier kan erstatte X^3 med Y^2 (og omvendt). For hvert $f \in k[X, Y]$ har vi så en kongruens, $f \equiv f_0(X) + f_1(X)Y$ med polynomier $f_0, f_1 \in k[X]$. Det er klart, at $\mathfrak{p}$ er indeholdt i kernen. Antag omvendt, at f tilhører kernen. Så følger det, at $f_0(x) + f_1(x)y = 0$, altså $f_0(T^2) + f_1(T^2)T^3 = 0$, og så må f_0 og f_1 være nul, og altså $f \equiv 0$, dvs $f \in (X^3 - Y^2)$.]

5. *Betragt i polynomiumsringen $k[T]$ (k er et legeme) polynomierne $x = T^3$, $y = T^4$ og $z = T^5$, og delalgebraen $k[x, y, z]$ af $k[T]$. Vis, at kernen for den naturlige homomorfi $k[X, Y, Z] \to k[x, y, z]$ er idealet $\mathfrak{p} := (Y^2 - XZ, X^3 - YZ, X^2Y - Z^2)$. [Vink: Regn modulo det sidste ideal, og vis, at for hvert $f \in k[X, Y, Z]$ er der en kongruens

$$f \equiv X^2 f_1(Z) + XY f_2(Z) + X f_3(Z) + Y f_4(Z) + f_5(Z) \pmod{\mathfrak{p}}.$$

Det er klart, at kernen omfatter $\mathfrak{p}$. Omvendt, hvis f ligger i kernen, så fås $T^6 f_1(T^5) + T^7 f_2(T^5) + T^3 f_3(T^5) + T^4 f_4(T^5) + f_5(T^5)$, og heraf følger $f_1 = f_2 = f_3 = f_4 = f_5 = 0$, og altså $f \in \mathfrak{p}$.]

U9 **6.** Lad $\theta\colon R \to R'$ være en ringhomomorfi, og lad S være en multiplikativ delmængde af R. Brøkmodulen $S^{-1}R'$ kan som bekendt identificeres med brøkringen $\theta(S)^{-1}R'$, og homomorfien $S^{-1}R \to S^{-1}R'$ er en ringhomomorfi. Vis, at hvis R' er hel over R, så er $S^{-1}R'$ hel over $S^{-1}R$.

5. Transcendensgrad.

I denne paragraf betragtes et fast integritetsområde A, og det antages, at ringen R er en delring af A. Specielt er R så et integritetsområde, og A er en R-algebra.

(5.1) Definition. Af definitionen (4.4) fremgår, at et enkelt element a i A er algebraisk afhængigt over R, hvis og kun hvis der findes en relation,

$$r_m a^m + \cdots + r_1 a + r_0 = 0, \tag{5.1.1}$$

hvor r_i'erne tilhører R, og hvor mindst ét af r_i'erne er forskelligt fra 0. Er dette opfyldt siges a også at være *algebraisk over* R.

Delmængden af A bestående af de elementer a, der er algebraiske over R, betegnes $\bar{R}$, og den kaldes den *algebraiske afslutning* af R i A. Bemærk, at betegnelsen $\bar{R}$ er ufuldstændig, idet denne delmængde afhænger af både R og A.

(5.2) Observation. Hvis delringen R er et legeme, så er et element a i A algebraisk over R, hvis og kun hvis a er hel over R. At a er hel over R betyder jo, at der findes en relation af formen (5.1.1), hvor $r_m = 1$. Et helt element er således algebraisk. Omvendt, hvis R er et legeme og a tilfredsstiller en ligning af formen (5.1.1), hvor $r_m \neq 0$, så kan denne ligning multipliceres med r_m^{-1}, hvorved der opnås en ligning med $r_m = 1$.

Hvis brøklegemet K for R er indeholdt i A, så er et element a algebraisk over R, hvis og kun hvis a er algebraisk (og dermed hel) over K. Er der nemlig givet en ligning (5.1.1), hvor koefficienterne r_i er brøker i K, så kan ligningen multipliceres med en fælles nævner for disse brøker, og herved opnås en ligning, hvor koefficienterne tilhører R.

(5.3) Lemma. (1) *Den algebraiske afslutning $\bar{R}$ i A er en delring af A. Hvis A eller R er et legeme, så er $\bar{R}$ et legeme.*

(2) *Lad B være en delring af A således at $R \subseteq B \subseteq A$, og således at hvert element i B er algebraisk over R. Hvert element $a \in A$, som er algebraisk over B, er da algebraisk over R.*

Bevis. (1) Antag først, at R er et legeme. Delmængden $\bar{R}$ af A består da af de elementer, der er hele over R. Af Korollar (4.9) følger derfor, at $\bar{R}$ er en delring af A. Da denne delring er hel over legemet R følger det af Lemma (4.14), at $\bar{R}$ er et legeme. Hermed er (1) vist når R er et legeme.

I det almindelige tilfælde betegnes med Q brøklegemet for A. Legemet Q vil da indeholde brøklegemet K for R, og vi har inklusioner,

$$\begin{array}{ccc} A & \subseteq & Q \\ \cup\!| & & \cup\!| \\ R & \subseteq & K\,. \end{array}$$

Lad $\bar{K}$ betegne den algebraiske afslutning af K i Q. Ifølge det allerede viste er $\bar{K}$ da et legeme. Da K er brøklegemet for R, består $\bar{K}$ af de elementer i Q, der er algebraiske over R. Heraf følger først, at $\bar{R} = A \cap \bar{K}$, hvoraf fremgår, at $\bar{R}$ er en delring af A. Hvis A er et legeme, og altså $A = Q$, så følger det videre, at $\bar{R} = \bar{K}$ er et legeme. Hermed er alle påstandene i (1) bevist.

Beviset for (2) er tilsvarende: Af antagelsen følger, at elementet a er helt over brøklegemet for B, og at brøklegemet for B er helt over K. Af Korollar (4.10) følger, at a er hel over K. Følgelig er a algebraisk over R. $\square$

(5.4) Lemma. *Lad der være givet et sæt af endelig mange elementer $a_1, \dots, a_m$ i A. Da er a_i'erne algebraisk afhængige over R, hvis og kun hvis et af a_i'erne er algebraisk over delalgebraen frembragt af de øvrige.*

Bevis. Elementet a_m er algebraisk over delalgebraen $R[a_1, \dots, a_{m-1}]$ netop hvis der findes en relation, med $N \geqslant 1$,

$$P_N(a_1, \dots, a_{m-1})a_m^N + P_{N-1}(a_1, \dots, a_{m-1})a_m^{N-1} + \dots + P_0(a_1, \dots, a_{m-1}) = 0, \quad (*)$$

med $P_N(a_1, \dots, a_{m-1}) \neq 0$, hvor koefficienterne fås ved indsættelse af $a_1, \dots, a_{m-1}$ i polynomier P_j i $m-1$ variable. Venstresiden i $(*)$ fås øjensynlig ved at indsætte $a_1, \dots, a_m$ i polynomiet

$$P := P_N X_m^N + P_{N-1} X_m^{N-1} + \dots + P_0. \quad (**)$$

Nu følger „hvis“ umiddelbart: Er $(*)$ opfyldt med $P_N(a_1, \dots, a_{m-1}) \neq 0$, så er $P \neq 0$; af $P(a_1, \dots, a_m) = 0$ følger derfor, at a_i'erne er algebraisk afhængige.

„Kun hvis“ vises ved induktion efter m. Det er trivielt for $m = 1$, idet delalgebraen frembragt af den tomme mængde blot er R. Antag, at $m > 1$ og at påstanden gælder for $m-1$ elementer. Betragt m elementer $a_1, \dots, a_m$, som er algebraisk afhængige. Hvis de $m-1$ elementer $a_1, \dots, a_{m-1}$ er algebraisk afhængige, så fås den ønskede konklusion af induktionsforudsætningen. Antag derfor, at de $m-1$ første a_i'er er algebraisk uafhængige. Da alle a_i'erne er algebraisk afhængige, findes et polynomium $P \neq 0$ så at $P(a_1, \dots, a_m) = 0$. Skriv nu polynomiet P på formen $(**)$ med $P_N \neq 0$. Da $(a_1, \dots, a_{m-1})$ er algebraisk uafhængige, følger det, at $N \geqslant 1$ og at $P_N(a_1, \dots, a_{m-1}) \neq 0$. Af $P(a_1, \dots, a_m) = 0$ fås den ønskede ligning (*). Altså er a_m algebraisk over delalgebraen frembragt af de første $m-1$ af a_i'erne. $\square$

(5.5) Definition. Lad V være en delmængde af A. Da siges V at have endelig *algebraisk dimension* over R, hvis der findes endelig mange elementer $a_1, \dots, a_n$ i A, så at hvert element i V er algebraisk over delringen $R[a_1, \dots, a_n]$, dvs så at

$$V \subseteq \overline{R[a_1, \dots, a_n]}. \quad (5.5.1)$$

Hvis relationen (5.5.1) er opfyldt, siges a_i'erne at være et *algebraisk frembringersystem* for V over R. Det mindste (endelige) antal a_i'er, der kan frembringe V, vil vi betegne $\dim_R^{\mathrm{alg}} V$. Hvis V ikke har endelig algebraisk dimension sættes $\dim_R^{\mathrm{alg}} V := \infty$.

Ved *transcendensgraden* for V over R forstås det største antal af algebraisk uafhængige (over R) elementer, der kan udtages fra V. Transcendensgraden betegnes $\operatorname{tdeg}_R V$. Mere præcist, transcendensgraden er ∞, hvis der kan udtages vilkårligt store (endelige) delmængder af V, som er algebraisk uafhængige over R. Hvis transcendensgraden ikke er uendelig, findes et største antal af elementer i V, der er algebraisk uafhængige over R, og dette største antal betegnes $\operatorname{tdeg}_R V$.

Ved en (endelig) *transcendensbasis* for V over R forstås et endeligt sæt af elementer $v_1, \dots, v_t$ i V, som er algebraisk uafhængige over R og som frembringer V algebraisk over R.

Af definitionen følger, at enhver delmængde V af A, der er indeholdt i en endelig frembragt R-delalgebra, har endelig algebraisk dimension over R.

Bemærk videre, at en delmængde V har transcendensgrad 0, hvis og kun hvis hvert element i V er algebraisk over R, og at dette indtræffer hvis og kun hvis den algebraiske dimension af V er lig med 0. I dette tilfælde er den tomme mængde en transcendensbasis for V over R.

(5.6) Lemma. *Lad V være en delmængde af A, og lad der være givet et endeligt sæt af elementer $v_1, \dots, v_t$ i V. Følgende betingelser (over R) er da ækvivalente:*

(i) *Sættet $v_1, \dots, v_t$ er et minimalt algebraisk frembringersystem for V, dvs et frembringersystem hvori intet v_i kan undværes.*
(ii) *Sættet $v_1, \dots, v_t$ er et maksimalt algebraisk uafhængigt system i V, dvs et algebraisk uafhængigt system, der ikke kan udvides med et element fra V til et større algebraisk uafhængigt system.*
(iii) *Sættet $v_1, \dots, v_t$ er en transcendensbasis for V.*

Bevis. „(i)⇒(iii)“: Antag, at v_i'erne er et minimalt algebraisk frembringersystem. For at vise, at de udgør en transcendensbasis, skal vises, at de er algebraisk uafhængige. Antag, indirekte, at v_i'erne er algebraisk afhængige. Det følger da af Lemma (5.4), at et af v_i'erne, fx v_t, er algebraisk over delalgebraen frembragt af de øvrige. Lad B betegne denne delalgebra. Da er

$$R[v_1, \dots, v_t] = R[v_1, \dots, v_{t-1}][v_t] = B[v_t].$$

Da v_t er algebraisk over B følger det Lemma (5.3)(1), at alle elementer i $B[v_t]$ er algebraiske over B. Af Lemma (5.3)(2) følger derfor, at $\overline{B[v_t]} = \bar{B}$. Med andre betegnelser,

$$V \subseteq \overline{R[v_1, \dots, v_t]} = \overline{R[v_1, \dots, v_{t-1}]}.$$

Men dette strider mod at $v_1, \dots, v_t$ var et minimalt frembringersystem for V.

„(iii)⇒(i)“: Antag, at v_i'erne er en transcendensbasis for V. Da er de specielt et algebraisk frembringersystem for V, og det skal vises, at dette frembringersystem er minimalt. Antag, indirekte, at et af v_i'erne, fx v_t, kan undværes. Da gælder inklusionen $V \subseteq \overline{R[v_1, \dots, v_{t-1}]}$. Nu er v_t element i V, og følgelig er v_t element i relationens højreside. Ifølge Lemma (5.4) er dette i modstrid med at v_i'erne er algebraisk uafhængige.

Beviset for „(ii) $\iff$ (iii)“ er analogt, og overlades til læseren. □

(5.7) Bemærkning. Af Lemma'et følger, at en delmængde V af A har en (endelig) transcendensbasis, hvis enten V har endelig transcendensgrad, eller hvis der findes endelig mange elementer i V, der udgør et algebraisk frembringersystem for V over R. I det første tilfælde kan vi nemlig begynde med den tomme mængde, som er en algebraisk uafhængig delmængde af V, og så supplere successivt med elementer fra V indtil vi opnår en maximal algebraisk uafhængig delmængde af V; forudsætningen medfører, at denne proces stopper efter endelig mange skridt. I det andet tilfælde kan vi begynde med en endelig delmængde af V, som udgør et algebraisk frembringersystem, og så successivt bortkaste v_i'er, som kan undværes. Efter endelig mange skridt fås et minimalt algebraisk frembringersystem for V.

(5.8) Lemma. *Lad V være en delmængde af A, og antag at V har en endelig transcendensbasis over R med t elementer. Da gælder ulighederne,*

$$\dim_R^{\mathrm{alg}} V \leqslant t \leqslant \operatorname{tdeg}_R V.$$

Bevis. Lad $v_1, \ldots, v_t$ være en transcendensbasis for V over R. Da er v_i'erne specielt et algebraisk frembringersystem for V, så antallet, t, af v_i'er er større end eller lig med det minimale antal elementer, der kan frembringe V. Videre er v_i'erne et algebraisk uafhængigt sæt fra V, så antallet af v_i'er er mindre end eller lig med det maximale antal (evt ∞) der kan være i et algebraisk uafhængigt sæt udtaget fra V.

Hermed er ulighederne bevist. □

(5.9) Udskiftningssætningen. *Lad V være en delmængde af A. Lad $a_1, \ldots, a_l$ være et sæt af elementer i A, som frembringer V algebraisk over R, og lad $v_1, \ldots, v_t$ være et sæt af elementer i V, som er algebraisk uafhængige over R. Da er $l \geqslant t$, og der findes $l - t$ af a_i'erne som sammen med v_j'erne frembringer V algebraisk over R.*

Bevis. Sætningen vises ved induktion efter t. For $t = 0$ er påstanden triviel (og indholdsløs). Antag, at $t \geqslant 1$, og at påstanden gælder for $t - 1$ elementer v_j. Da de $t - 1$ første v_j'er er algebraisk uafhængige over R, gælder påstanden altså for $v_1, \ldots, v_{t-1}$. Følgelig er $l \geqslant t-1$, og vi kan udskifte $t - 1$ af a_i'erne med disse v_j'er. Vi kan antage, at det er de første $t - 1$ af a_i'erne der kan udskiftes, dvs at elementerne $v_1, \ldots, v_{t-1}, a_t, \ldots, a_l$ frembringer V algebraisk over R. [I dette skridt ved vi kun, at $l \geqslant t-1$; det er altså ikke udelukket, at $l = t-1$, i hvilket tilfælde følgen $a_t, \ldots, a_l$ er tom.] Altså er $V \subseteq \overline{R[v_1, \ldots, v_{t-1}, a_t, \ldots, a_l]}$. Da $v_t \in V$ gælder derfor specielt, at

$$v_t \in \overline{R[v_1, \ldots, v_{t-1}, a_t, \ldots, a_l]}.$$

Af Lemma (5.4) følger nu, at elementerne $v_1, \ldots, v_{t-1}, a_t, \ldots, a_l, v_t$ er algebraisk afhængige over R. Der findes altså en ikke-triviel algebraisk relation mellem disse elementer. Da elementerne $v_1, \ldots, v_t$ er forudsat algebraisk uafhængige, må et af elementerne $a_t, \ldots, a_l$ forekomme i denne relation. Specielt følger det, at $t \leqslant l$. Det kan antages, at det er a_t, der forekommer i relationen, og så får vi, at

$$a_t \in \overline{R[v_1, \ldots, v_t, a_{t+1}, \ldots, a_l]}.$$

Under brug af Lemma (5.3)(2) fås følgende inklusioner,

$$V \subseteq \overline{R[v_1, \ldots, v_{t-1}, a_t, \ldots, a_l]} \subseteq \overline{R[v_1, \ldots, v_t, a_{t+1}, \ldots, a_l]}.$$

Altså er $v_1, \ldots, v_t, a_{t+1}, \ldots, a_l$ et algebraisk frembringersystem for V over R.

Hermed er påstanden vist for t elementer, hvorved induktionsbeviset er fuldført. □

(5.10) Hovedsætning. *For enhver delmængde V af A gælder ligningen,*

$$\operatorname{tdeg}_R V = \dim_R^{\mathrm{alg}} V.$$

Hvis V har endelig transcendensgrad t over R, så findes der endelige transcendensbaser for V over R, og alle sådanne baser indeholder t elementer.

Bevis. Uligheden $\dim_R^{\mathrm{alg}} V \leqslant \operatorname{tdeg}_R V$ gælder, thi hvis højresiden er uendelig gælder den trivielt, og hvis højresiden er endelig, så findes der en transcendensbasis for V, og så følger uligheden af Lemma (5.8).

Ligeledes gælder uligheden $\operatorname{tdeg}_R V \leqslant \dim_R^{\mathrm{alg}} V$. Hvis højresiden er uendelig gælder uligheden nemlig trivielt. Hvis højresiden er endelig, findes et algebraisk frembringersystem $a_1, \dots, a_l$ for V over R med $l = \dim_R^{\mathrm{alg}} V$. Af Udskiftningssætningen (5.9) følger, at der for hvert algebraisk uafhængigt sæt i V med t elementer gælder $t \leqslant l$. Altså er $\operatorname{tdeg}_R V \leqslant l$, hvormed den påståede ulighed er vist.

Altså gælder ligningen anført i sætningen. Sætningens sidste påstand følger nu umiddelbart af Lemma (5.8). □

(5.11) Bemærkning. Begreberne og sætningerne i dette afsnit anvendes ofte i en situation hvor A og/eller R er legemer.

Antag først, at integritetsområdet A er et legeme. For enhver delring B af A vil da også brøklegemet for B være indeholdt i A. For givne elementer $a_1, \dots, a_m$ i A betegnes med

$$R(a_1, \dots, a_m)$$

brøklegemet for delalgebraen $R[a_1, \dots, a_m]$. Øjensynlig er dette dellegeme af A det mindste, der indeholder R og alle a_i'erne; det kaldes *dellegemet frembragt* af R og a_i'erne.

Det givne legeme A siges at være *endeligt frembragt som legeme* over R, hvis der i A findes endelig mange elementer $a_1, \dots, a_m$, som *frembringer legemet* A, dvs opfylder at

$$A = R(a_1, \dots, a_m).$$

I denne situation har altså enhver delmængde V af A en endelig transcendensbasis over R, nødvendigvis med højst m elementer.

Betragt dernæst tilfældet, hvor A er et integritetsområde, endeligt frembragt som algebra over et legeme k af elementer $a_1, \dots, a_m$. Da er $A = k[a_1, \dots, a_m]$, og for brøklegemet af A kan anvendes betegnelsen $k(a_1, \dots, a_m)$. Algebraen A er homomorft billede af en polynomiumsring, altså af formen $A = k[X_1, \dots, X_m]/\mathfrak{P}$, og idealet $\mathfrak{P}$ er et primideal i polynomiusringen, da A er forudsat at være et integritetsområde. Resultaterne i dette kapitel har altså speciel anvendelse på sådanne kvotienter af polynomiumsringen over et legeme k. Ifølge Noether's Normaliseringslemma er en sådan algebra A hel over en delring af formen $k[x_1, \dots, x_t]$, hvor x_i'erne er algebraisk uafhængige over k. Ifølge definitionen udgør x_i'erne en transcendensbasis for A over k. Specielt er antallet t entydigt bestemt, nemlig som $t = \operatorname{tdeg}_k A$.

(5.12) Sætning. *Antag, at A er et integritetsområde, og at legemet k er en delring af A. Lad $\mathfrak{p}$ være et primideal i A. Da gælder uligheden,*

$$\operatorname{tdeg}_k(A/\mathfrak{p}) \leqslant \operatorname{tdeg}_k A.$$

Hvis $\operatorname{tdeg}_k A < \infty$ *og lighed gælder i uligheden ovenfor, da er* $\mathfrak{p} = (0)$.

Bevis. Lad $a \mapsto \hat{a}$ betegne den kanoniske (surjektive) homomorfi $A \to A/\mathfrak{p}$. Betragt i A elementet $P(a_1, \dots, a_t)$, der fås ved at indsætte af a_i'erne i et polynomium P. Det er klart, at billedet i $A/\mathfrak{p}$ af dette element fås ved at indsætte $\hat{a}_i$'erne i P. Det følger, at hvis $\hat{a}_i$'erne er algebraisk uafhængige over k, så er a_i'erne algebraisk uafhængige over k. Heraf følger den påståede ulighed umiddelbart.

Antag nu, at $\operatorname{tdeg}_k A < \infty$ og at lighed gælder i uligheden. Vi kan da vælge a_i'erne, med $t := \operatorname{tdeg}_k(A/\mathfrak{p})$, således, at de udgør en transcendensbasis for $A/\mathfrak{p}$. Da er a_i'erne algebraisk uafhængige over k. Specielt afbildes delringen $B := k[a_1, \dots, a_t]$ derfor isomorft på sit billede $k[\hat{a}_1, \dots, \hat{a}_t]$ i $A/\mathfrak{p}$. Da $t = \operatorname{tdeg}_k A$, er a_i'erne en transcendensbasis for A over k, og hvert element i A er derfor algebraisk over B. Lad nu a være et element forskelligt fra 0 i A. Der findes da en ligning,

$$b_m a^m + \cdots + b_1 a + b_0 = 0, \tag{$*$}$$

hvor koefficienterne b_i tilhører B, og hvor ikke alle b_i'er er lig med 0. I denne relation kan vi antage, at b_0 er forskellig fra 0. Er nemlig b_i den første koefficient forskellig fra 0, så kan a^i sættes uden for parentes på venstresiden; da $a \neq 0$, er parentesen lig med 0, og dette er så en ligning af den ønskede form.

Ligningen $(*)$ medfører følgende ligning i $A/\mathfrak{p}$:

$$\hat{b}_m \hat{a}^m + \cdots + \hat{b}_1 \hat{a} + \hat{b}_0 = 0$$

Nu var afbildningen $b \mapsto \hat{b}$ injektiv på B, og da vi har antaget $b_0 \neq 0$, følger det af den sidste ligning, at $\hat{a} \neq 0$.

Vi har vist, at for $a \neq 0$ er $\hat{a} \neq 0$. Altså er afbildningen $A \to A/\mathfrak{p}$ injektiv. Og det betyder, at kernen $\mathfrak{p}$ er lig med (0). □

(5.13) Bemærkning. Nogle af begreberne og resultaterne i denne paragraf kan generaliseres til tilfældet, hvor algebraen A ikke er et integritetsområde. Algebraisk uafhængighed er defineret for en vilkårlig R-algebra A. Vi vælger her at definere *transcendensgraden* $\operatorname{tdeg}_R A$ som det største antal elementer fra A, algebraisk uafhængige over R. Bemærk, at hvis $x_1, \dots, x_t \in A$ er algebraisk uafhængige over R, dvs hvis $R[X_1, \dots, X_t] \to R[x_1, \dots, x_t]$ er en injektiv homomorfi, så er specielt $R \to A$ injektiv. Hvis homomorfien $R \to A$ ikke er injektiv, er altså ikke engang den tomme delmængde af A algebraisk uafhængig; transcensdensgraden $\operatorname{tdeg}_R A$ sættes så til -1.

Vi vælger her at kalde et element a i A *algebraisk* over R, hvis a er rod i et polynomium $f \neq 0$ i $R[X]$, hvis højestegradskoefficient er regulær i A (i den „store“ ring). (Man kan forestille sig andre definitioner, og ovenstående kunne måske kaldes *regulær-algbraisk*).

Det er let at se, at $a \in A$ er algebraisk over R, hvis og kun hvis der findes et element $s \in R$, regulært i A, således, at sa er hel over R. Heraf følger let, at de algebraiske elementer i A udgør en delalgebra af A.

Sætning. *Antag, at R er et integritetsområde indeholdt i A. Da er*

$$\operatorname{tdeg}_R A = \sup \operatorname{tdeg}_R(A/\mathfrak{p}), \tag{5.13.1}$$

hvor supremum er over alle primidealer $\mathfrak{p}$ i A. Antag yderligere, at A er algebraisk over en delalgebra $B = R[y_1, \dots, y_d]$ frembragt af d elementer. Da er

$$d \geqslant \operatorname{tdeg}_R A, \tag{5.13.2}$$

og lighed gælder, hvis og kun hvis $y_1, \dots, y_d$ er algebraisk uafhængige over R.

Bevis. I beviset bruges gentagne gange tilføjelsen til Eksistenssætningen: Hvis S er en multiplikativ delmængde af A, og $\mathfrak{a}$ er et ideal i A med $\mathfrak{a} \cap S = \emptyset$, så findes et primideal $\mathfrak{p} \supseteq \mathfrak{a}$ med $\mathfrak{p} \cap S = \emptyset$.

Det er klart, at ved en homomorfi $A \to A'$ falder transcendensgraden: elementer $x_1, \dots, x_t$ i A, hvis billeder i A' er algebraisk uafhængige, er selv algebraisk uafhængige. Altså gælder uligheden '$\geqslant$' i (5.13.1). er elementer i A.

For at vise den omvendte ulighed betragtes t algebraisk uafhængige elementer $x_1, \dots, x_t$ i A. Det skal vises, at t højst er lig med supremum på højresiden af (5.13.1), altså at der findes et primideal $\mathfrak{p} \subseteq A$ med $t \leqslant \operatorname{tdeg}_R(A/\mathfrak{p})$. Delalgebraen $C := R[x_1, \dots, x_t]$ er så isomorf med polynomiumsalgebraen $R[X_1, \dots, X_t]$. Da R er et integritetsområde, er C er et integritetsområde. Altså er (0) et primideal i C. Derfor findes et primideal $\mathfrak{p} \subseteq A$ således, at $\mathfrak{p} \cap C = (0)$. Den sidste relation viser, at homomorfien $A \to A/\mathfrak{p}$ afbilder C isomorft på sit billede i $A/\mathfrak{p}$. Derfor er billederne af $x_1, \dots, x_t$ i $A/\mathfrak{p}$ algebraisk uafhængige, og det følger, at $t \leqslant \operatorname{tdeg}_R(A/\mathfrak{p})$, som ønsket.

Antag nu, at A er algebraisk over delalgebraen $B = R[y_1, \dots, y_d]$. For at vise den anførte ulighed, skal det vises, for hvert primideal $\mathfrak{p}$ i A, at

$$d \geqslant \operatorname{tdeg}_R(A/\mathfrak{p}).$$

Lad S være mængden af de elementer i B, der er regulære i A. Da er S en multiplikativ delmængde af B (og dermed af A), og hvert element i A er rod i et polynomium i $B[X]$ med højestegradskoefficient i S. Betragt primidealer $\mathfrak{q}$ i A, der opfylder to betingelser:

$$\mathfrak{q} \subseteq \mathfrak{p} \quad \text{og} \quad \mathfrak{q} \cap S = \emptyset.$$

Den første af de to betingelser betyder, at $\mathfrak{q}$ er disjunkt med komplementærmængden $T := A \setminus \mathfrak{p}$. Under et betyder de to betingelser, at $\mathfrak{q}$ er disjunkt med foreningsmængden $S \cup T$, og for et primideal $\mathfrak{q}$ gælder det præcis, når $\mathfrak{q}$ er disjunt med produktet ST. Da T ikke indeholder 0, og da elementerne i S er regulære i A, er 0 ikke element i ST. Derfor findes et primideal $\mathfrak{q}$ som opfylder betingelserne.

Af den første betingelse følger, at $A/\mathfrak{p}$ er en kvotientring af $A/\mathfrak{q}$; derfor er $\operatorname{tdeg}_R(A/\mathfrak{q}) \geqslant \operatorname{tdeg}_R(A/\mathfrak{p})$. Af den anden betingelse følger, at billedet i $A/\mathfrak{q}$ af et element i S er forskelligt fra 0; billedet er derfor et regulært element i integritetsområdet $A/\mathfrak{p}$. Heraf følger, at $A/\mathfrak{q}$

er algebraisk over billedalgebraen $\widehat{B} = R[\hat{y}_1, \dots, \hat{y}_t]$. Altså er $d \geqslant \dim_R^{\mathrm{alg}}(A/\mathfrak{q})$. Af Hovedsætning (5.10) følger så, at $d \geqslant \mathrm{tdeg}_R(A/\mathfrak{q})$. I alt er altså som ønsket,

$$t \geqslant \mathrm{tdeg}_R(A/\mathfrak{q}) \geqslant \mathrm{tdeg}_R(A/\mathfrak{p}). \tag{5.13.3}$$

For at vise sætningens sidste påstand antages først, at lighed gælder i (5.13.2), altså at der findes et primideal $\mathfrak{p} \subseteq A$ med $d = \mathrm{tdeg}_R(A/\mathfrak{p})$. Vælg $\mathfrak{q} \subseteq \mathfrak{p}$ som ovenfor. Af (5.13.3) fås så ligningen $d = \mathrm{tdeg}_R(A/\mathfrak{q})$. Videre er $A/\mathfrak{q}$ algebraisk over billedalgebraen $R[\hat{y}_1, \dots, \hat{y}_d]$. Derfor er billederne $\hat{y}_1, \dots, \hat{y}_d$ i $A/\mathfrak{q}$ algebraisk uafhængige over R. Følgelig er elementerne $y_1, \dots, y_d$ i A algebraisk uafhængige over R.

Antages omvendt, at elementerne $y_1, \dots, y_d$ er algebraisk uafhængige over R, så følger det umiddelbart, at $d \leqslant \mathrm{tdeg}_R A$; følgelig gælder lighed i (5.13.2). □

(5.14) Opgaver.

1. Lad B være en delring af integritetsområdet A således, at $R \subseteq B \subseteq A$. Vis formlen,

$$\mathrm{tdeg}_R A = \mathrm{tdeg}_B A + \mathrm{tdeg}_R B.$$

2. Lad A og B være algebraer over et legeme k. Diskuter ligningen $\mathrm{tdeg}(A \times B) = \max\{\mathrm{tdeg}\, A, \mathrm{tdeg}\, B\}$.

3. Lad der være givet delringe $R \subseteq B \subseteq A$, hvor A og B ikke nødvendigvis er integritetsområder. Antag, at hvert element $r \neq 0$ i R er regulært i B (Specielt er så R et integritetsområde). Vis, at hvis A er algebraisk over B, og B er algebraisk over R, så er A algebraisk over R.

Moduler over noetherske ringe

1. Ann, Supp og Ass.

(1.1) Definition. Lad M være en R-modul. En skalar $r \in R$ siges da at *annullere* elementet $x \in M$, hvis $rx = 0$. De skalarer, som annullerer et givet element x i M, udgør øjensynlig et ideal i R, kaldet *annullatoren* for elementet x, og betegnet $\operatorname{Ann}(x)$. Ifølge definitionen er altså

$$\operatorname{Ann}(x) = \{ r \in R \mid rx = 0 \}.$$

De skalarer, som annullerer alle elementer i modulen M, udgør ligeledes et ideal i R. Dette ideal kaldes *annullatoren* for modulen M, og det betegnes $\operatorname{Ann} M$, altså

$$\operatorname{Ann} M = \{ r \in R \mid rx = 0 \text{ for alle } x \in M \}.$$

Ved *støtten* for modulen M forstås mængden af de primidealer $\mathfrak{p}$ i R, for hvilke $M_\mathfrak{p} \neq 0$. Støtten betegnes $\operatorname{Supp} M$. Bemærk, at støtten er en mængde af primidealer, og ikke en delmængde af R. Støtten er specielt en partielt ordnet mængde, ordnet ved inklusion; de minimale elementer i denne mængde kaldes *minimale primidealer* for M. Støtten for en kvotient $R/\mathfrak{a}$, hvor $\mathfrak{a}$ er et ideal, består øjensynlig af de primidealer $\mathfrak{p}$, for hvilke $\mathfrak{p} \supseteq \mathfrak{a}$. Et minimalt primideal for $R/\mathfrak{a}$ siges også at være et *isoleret primideal* for $\mathfrak{a}$.

Primidealerne blandt annullatorerne $\operatorname{Ann}(x)$ for x i M siges at være *associerede primidealer* til modulen M. At primidealet $\mathfrak{p}$ i R er associeret til modulen M betyder altså, at der findes et element x i M således, at

$$\mathfrak{p} = \operatorname{Ann}(x).$$

Mængden af primidealer associerede til modulen M betegnes $\operatorname{Ass} M$.

(1.2) Observation. Det følger umiddelbart af definitionen, at modulens annullator $\operatorname{Ann} M$ er fællesmængden af annullatorerne $\operatorname{Ann}(x)$ for $x \in M$.

Betragt et element x i M og et primideal $\mathfrak{p}$. Brøken $x/1$ er da nul-brøken i $M_\mathfrak{p}$, hvis og kun hvis der findes et element $s \notin \mathfrak{p}$ således, at $sx = 0$. Med andre ord gælder der, at

$$x/1 \neq 0 \text{ i } M_\mathfrak{p} \iff \operatorname{Ann}(x) \subseteq \mathfrak{p}.$$

Brøkmodulen $M_\mathfrak{p}$ er øjensynlig forskellig fra 0, hvis og kun hvis en af brøkerne $x/1$, for $x \in M$, er forskellig fra 0. Heraf følger, at primidealet $\mathfrak{p}$ tilhører støtten for M, hvis og kun hvis $\mathfrak{p}$ indeholder en af annullatorerne $\operatorname{Ann}(x)$ for et element x i M.

Specielt følger det, at hvert associeret primideal for modulen tilhører støtten for modulen. Der gælder altså inklusionen,

$$\operatorname{Ass} M \subseteq \operatorname{Supp} M.$$

(1.3) Observation. Et ideal $\mathfrak{a}$ er annullator for et element i modulen M, hvis og kun hvis M indeholder en undermodul isomorf med kvotientmodulen $R/\mathfrak{a}$. Annullatoren $\operatorname{Ann}(x)$ er nemlig kernen for den ved $r \mapsto rx$ bestemte lineære afbildning $R \to M$. Hvis $\mathfrak{a} = \operatorname{Ann}(x)$, så følger det af Isomorfisætningen, at $R/\mathfrak{a}$ er isomorf med afbildningens billede (der er undermodulen Rx). Omvendt, hvis $R/\mathfrak{a}$ er isomorf med en undermodul i M, så svarer restklassen $\hat{1}$ herved til et element x i M, og det er klart, at $\operatorname{Ann}(x) = \operatorname{Ann}(\hat{1}) = \mathfrak{a}$.

Specielt er et primideal $\mathfrak{p}$ associeret til M, hvis og kun hvis M indeholder en undermodul isomorf med $R/\mathfrak{p}$.

(1.4) Eksistenssætning. *Antag, at R-modulen M er forskellig fra 0. Da er støtten* Supp M *ikke tom.*

Bevis. Da $M \neq 0$ findes i M et element $x \neq 0$. Da $x \neq 0$ vil et-elementet 1 ikke tilhøre annullatoren $\operatorname{Ann}(x)$. Følgelig er $\operatorname{Ann}(x) \subset R$. Af Eksistenssætningen for maksimalidealer følger derfor, at der i R findes et maksimalideal $\mathfrak{m}$ således, at $\operatorname{Ann}(x) \subseteq \mathfrak{m}$. Af den sidste relation følger, at $M_{\mathfrak{m}} \neq 0$. Da maksimalidealet $\mathfrak{m}$ således tilhører støtten Supp M, er støtten ikke tom. ∎

(1.5) Sætning. *Lad M være en endeligt frembragt R-modul. For et primideal $\mathfrak{p}$ gælder da, at $M_{\mathfrak{p}} \neq 0$, hvis og kun hvis $\mathfrak{p} \supseteq \operatorname{Ann} M$.*

Bevis. Antag først, at $M_{\mathfrak{p}} \neq 0$. Da findes i M et element x således, at $\operatorname{Ann}(x) \subseteq \mathfrak{p}$. Da $\operatorname{Ann} M \subseteq \operatorname{Ann}(x)$, følger det, at $\operatorname{Ann} M \subseteq \mathfrak{p}$.

For at vise det omvendte bruges, at M er frembragt af endelig mange elementer $x_1, \dots, x_n$. Et element r, der annullerer hvert af x_i'erne, vil også annullere enhver linearkombination af x_i'erne, og dermed ethvert element i M. Altså gælder inklusionen,

$$\operatorname{Ann}(x_1) \cap \dots \cap \operatorname{Ann}(x_n) \subseteq \operatorname{Ann} M$$

(der forøvrigt klart må være en lighed). Antag nu, at $\operatorname{Ann} M \subseteq \mathfrak{p}$. Af inklusionen ovenfor følger så, at fællesmængden af idealerne $\operatorname{Ann}(x_i)$ er indeholdt i primidealet $\mathfrak{p}$. Som bekendt følger heraf, at et af idealerne $\operatorname{Ann}(x_i)$ er indeholdt i $\mathfrak{p}$. Primidealet $\mathfrak{p}$ indeholder altså en annullator for et element i M. Følgelig er $M_{\mathfrak{p}} \neq 0$. ∎

(1.6) Eksempel. Betragt for et ideal $\mathfrak{a}$ kvotienten $R/\mathfrak{a}$ som R-modul. Annullatoren af restklassen $\hat{1}$ er øjensynlig $\operatorname{Ann}(\hat{1}) = \mathfrak{a}$. Omvendt er det klart, at hvert element i $\mathfrak{a}$ annullerer hvert element i $R/\mathfrak{a}$. Altså er $\mathfrak{a} = \operatorname{Ann}(R/\mathfrak{a})$. Heraf følger videre, at støtten for $R/\mathfrak{a}$ består af de primidealer $\mathfrak{p}$, der omfatter $\mathfrak{a}$.

Antag nu, at idealet er et primideal $\mathfrak{q}$. Betragt en restklasse $x \neq 0$ i modulen $R/\mathfrak{q}$. For et element r i R gælder da $rx = \hat{r}x$, hvor $\hat{r}$ er restklassen modulo $\mathfrak{q}$. Da nulreglen gælder i ringen $R/\mathfrak{q}$, følger det, at $\operatorname{Ann}(x) = \mathfrak{q}$. Alle elementer forskellige fra 0 i $R/\mathfrak{q}$ har altså den samme annullator, nemlig $\mathfrak{q}$. Specielt er $\mathfrak{q}$ det eneste primideal associeret til $R/\mathfrak{q}$, dvs,

$$\operatorname{Ass}(R/\mathfrak{q}) = \{\mathfrak{q}\}.$$

(1.7) Lemma. *Lad $N \subseteq M$ være en undermodul. Da gælder relationerne,*

$$\operatorname{Supp} M = \operatorname{Supp} N \cup \operatorname{Supp}(M/N), \tag{1.7.1}$$

$$\operatorname{Ass} N \subseteq \operatorname{Ass} M \subseteq \operatorname{Ass} N \cup \operatorname{Ass}(M/N). \tag{1.7.2}$$

Bevis. Lad $\mathfrak{p}$ være et primideal. Ifølge Isomorfisætning for Brøkmoduler er $N_\mathfrak{p}$ en undermodul i $M_\mathfrak{p}$ og $(M/N)_\mathfrak{p}$ er den tilhørende kvotientmodul. Følgelig er $M_\mathfrak{p}$ forskellig fra 0, hvis og kun hvis en af modulerne $N_\mathfrak{p}$ og $(M/N)_\mathfrak{p}$ er forskellig fra 0. Og det er netop påstanden i ligningen (1.7.1).

Den første inklusion i (1.7.2) er triviel. At $\mathfrak{p}$ er associeret til N betyder jo at der findes et element y i N, så at $\mathfrak{p} = \operatorname{Ann}(y)$. Og denne ligning sikrer at $\mathfrak{p}$ er associeret til M, idet y er element i M.

Betragt nu den anden inklusion i (1.7.2). Antag, at $\mathfrak{p}$ tilhører venstresiden, altså at $\mathfrak{p}$ er et primideal associeret til M. Da findes et element $x \in M$ så at $\mathfrak{p} = \operatorname{Ann}(x)$. Betragt restklassen $\hat{x}$ af x modulo N. Et element, der annullerer x vil også annullere $\hat{x}$. Altså gælder relationerne,

$$\mathfrak{p} = \operatorname{Ann}(x) \subseteq \operatorname{Ann}(\hat{x}).$$

Hvis den sidste inklusion er en lighed, så er $\mathfrak{p} = \operatorname{Ann}(\hat{x})$; følgelig er $\mathfrak{p}$ associeret til M/N, og dermed er $\mathfrak{p}$ element i foreningsmængden på højresiden i (1.7.2). Betragt dernæst tilfældet, hvor den sidste inklusion er skarp, hvor altså $\operatorname{Ann}(x) \subset \operatorname{Ann}(\hat{x})$. Da findes et element $r \in R$ således, at $r\hat{x} = 0$ og $rx \neq 0$. At $r\hat{x} = 0$ i kvotientmodulen M/N betyder, at rx tilhører N. Følgelig gælder relationerne,

$$\mathfrak{p} = \operatorname{Ann}(x) \subseteq \operatorname{Ann}(rx), \quad rx \in N, \quad rx \neq 0.$$

Det er nok at vise, at inklusionen $\operatorname{Ann}(x) \subseteq \operatorname{Ann}(rx)$ er en lighed, thi så er $\mathfrak{p}$ annullator for et element (nemlig rx) i undermodulen N; følgelig er $\mathfrak{p}$ associeret til N, og dermed er $\mathfrak{p}$ element i foreningsmængden på højresiden i (1.7.2).

For at vise, at inklusionen $\operatorname{Ann}(x) \subseteq \operatorname{Ann}(rx)$ er en lighed, betragtes et element $s \in \operatorname{Ann}(rx)$. Da er $srx = 0$, og følgelig er $sr \in \operatorname{Ann}(x)$. Ifølge valget af r er $rx \neq 0$, så $r \notin \operatorname{Ann}(x)$. Da $\operatorname{Ann}(x) = \mathfrak{p}$ er et primideal, sluttes nu, at $s \in \operatorname{Ann}(x)$. Hermed er den påståede lighed vist, og beviset fuldført. □

(1.8) Lemma. *Betragt en R-modul M og et primideal $\mathfrak{p} \subset R$.* (1) *Hvis S er en multiplikativ delmængde disjunkt med $\mathfrak{p}$, gælder:*

$$\mathfrak{p} \in \operatorname{Supp} M \iff S^{-1}\mathfrak{p} \in \operatorname{Supp}(S^{-1}M), \tag{1.8.1}$$

$$\mathfrak{p} \in \operatorname{Ass} M \implies S^{-1}\mathfrak{p} \in \operatorname{Ass}(S^{-1}M); \tag{1.8.2}$$

hvis $\mathfrak{p}$ er endeligt frembragt, så er den sidste implikation en biimplikation.

(2) *Hvis $\mathfrak{a} \subseteq R$ er et ideal, gælder:*

$$\mathfrak{p} \in \operatorname{Supp} M/\mathfrak{a}M \implies \mathfrak{p} \in \operatorname{Supp} M \text{ og } \mathfrak{p} \supseteq \mathfrak{a}; \tag{1.8.3}$$

hvis M er endeligt frembragt, er implikationen en biimplikation.

Bevis. (1) Antag, at $\mathfrak{p}$ er disjunkt med S. Af Lokaliseringsprincippet følger derfor, at $S^{-1}\mathfrak{p}$ er et primideal i brøkringen $S^{-1}R$ og at

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

Af denne ligning følger umiddelbart biimplikationen i (1.8.1).

For at vise implikationen i (1.8.2) antages, at $\mathfrak{p}$ er associeret til M. Da har M en undermodul isomorf med $R/\mathfrak{p}$. Af Isomorfisætningen for Brøkmoduler følger så først, at $S^{-1}M$ har en undermodul isomorf med $S^{-1}(R/\mathfrak{p})$, og videre, at denne sidste modul er isomorf med $S^{-1}R/S^{-1}\mathfrak{p}$. Heraf ses, at $S^{-1}\mathfrak{p}$ er associeret til $S^{-1}M$.

Antag endelig, at $\mathfrak{p}$ er frembragt af endelig mange elementer $p_1, \dots, p_n$. For at vise implikationen mod venstre i (1.8.2) antages, at $S^{-1}\mathfrak{p}$ er associeret til $S^{-1}M$. Der findes da en brøk x/t i $S^{-1}M$ således, at

$$S^{-1}\mathfrak{p} = \mathrm{Ann}(x/t). \tag{$*$}$$

Heraf ses først, at for hvert element $p \in \mathfrak{p}$ vil brøken $p/1$ annullere x/t. Altså findes for hvert $p \in \mathfrak{p}$ et element $s \in S$ således, at $spx = 0$. Specielt findes for hver af frembringerne p_i et element $s_i \in S$ således, at $s_i p_i x = 0$. Sættes $s := s_1 \cdots s_n$ følger det, at $sp_i x = 0$ for alle i, og dernæst videre, at $spx = 0$ for alle $p \in \mathfrak{p}$. Med andre ord gælder inklusionen,

$$\mathfrak{p} \subseteq \mathrm{Ann}(sx).$$

Det er nok at vise, at lighed gælder i denne inklusion, thi da er $\mathfrak{p}$ annullatoren for elementet sx i M, og så er $\mathfrak{p}$ associeret til M. Antag derfor, at r er element i $\mathrm{Ann}(sx)$, altså at $rsx = 0$. Da s tilhører S, følger det at brøken $r/1$ annullerer brøken x/t. Af $(*)$ følger derfor, at $r/1$ tilhører $S^{-1}\mathfrak{p}$. Af Lokaliseringsprincippet følger endelig, at r tilhører $\mathfrak{p}$, som ønsket.

(2) Som bekendt er $(M/\mathfrak{a}M)_{\mathfrak{p}} = M_{\mathfrak{p}}/\mathfrak{a}M_{\mathfrak{p}}$. Derfor er $\mathfrak{p} \in \mathrm{Supp}\, M/\mathfrak{a}M$, hvis og kun hvis $\mathfrak{a}M_{\mathfrak{p}} \subset M_{\mathfrak{p}}$. Det sidste er naturligvis udelukket, hvis $M_{\mathfrak{p}} = 0$; det er også udelukket, hvis $\mathfrak{a} \not\subseteq \mathfrak{p}$, thi så indeholder $\mathfrak{a}R_{\mathfrak{p}}$ et invertibelt element, og så er $\mathfrak{a}M_{\mathfrak{p}} = M_{\mathfrak{p}}$. Altså gælder implikationen i (1.8.3).

Antag endelig, at M er endeligt frembragt, og at $M_{\mathfrak{p}} \neq 0$ og $\mathfrak{a} \subseteq \mathfrak{p}$. Så er $\mathfrak{a}R_{\mathfrak{p}} \subseteq \mathfrak{p}R_{\mathfrak{p}}$, og $\mathfrak{p}R_{\mathfrak{p}}$ er maksimalidealet i $R_{\mathfrak{p}}$. Af Nakayama's lemma følger så, at $\mathfrak{a}M_{\mathfrak{p}} \subset M_{\mathfrak{p}}$. Altså gælder også implikationen fra højre med venstre i (1.8.3). □

(1.9) Lemma. *Lad M være en R-modul. Enhver annullator, der er maksimal blandt annullatorerne* $\mathrm{Ann}(x)$ *med $x \in M \setminus \{0\}$, er et primideal* (*og dermed et associeret primideal for* M). *Lad $\mathfrak{p}$ være et primideal i R. Enhver annullator, der er maksimal blandt annulatorerne* $\mathrm{Ann}(x)$ *med $x \in M$ og* $\mathrm{Ann}(x) \subseteq \mathfrak{p}$, *er et primideal* (*og dermed et associeret primideal for* M).

Bevis. For at vise den anden påstand antages, at annullatoren $\mathrm{Ann}(y)$ er maksimal blandt annullatorerne $\mathrm{Ann}(x)$ med $x \in M$ og $\mathrm{Ann}(x) \subseteq \mathfrak{p}$. Det skal vises, at $\mathrm{Ann}(y)$ er et primideal. Antag hertil, for $r, s \in R$, at $rs \in \mathrm{Ann}(y)$, altså at $rsy = 0$. Det skal vises, at r eller s tilhører $\mathrm{Ann}(y)$. Det er klart, at $\mathrm{Ann}(y) \subseteq \mathrm{Ann}(sy)$. Der er to tilfælde: $\mathrm{Ann}(sy) \subseteq \mathfrak{p}$ og

$\mathrm{Ann}(sy) \not\subseteq \mathfrak{p}$. I det første tilfælde sikrer maksimaliteten af $\mathrm{Ann}(y)$, at $\mathrm{Ann}(y) = \mathrm{Ann}(sy)$; da $r(sy) = 0$ følger det, at $r \in \mathrm{Ann}(y)$, som ønsket. I det andet tilfælde findes et element $u \in R$ med $u \in \mathrm{Ann}(sy)$ og $u \notin \mathfrak{p}$; nu er $\mathrm{Ann}(y) \subseteq \mathrm{Ann}(uy)$, og da $u \notin \mathfrak{p}$ er det klart, at $\mathrm{Ann}(uy) \subseteq \mathfrak{p}$. Maksimaliteten af $\mathrm{Ann}(y)$ sikrer så, at $\mathrm{Ann}(y) = \mathrm{Ann}(uy)$; da $s(uy) = 0$ følger det, at $s \in \mathrm{Ann}(y)$, som ønsket.

Beviset for den første påstand er tilsvarende, men lettere. □

(1.10) Opgaver.

1. Vis, uden noetherske forudsætninger, at for enhver R-modul M gælder formlen,

$$\{ f \in R \mid M_f = 0 \} = \bigcap_{\mathfrak{p} \in \mathrm{Supp}\, M} \mathfrak{p}\,.$$

U6 **2.** Beskriv $\mathrm{Ann}\, M$, $\mathrm{Supp}\, M$ og $\mathrm{Ass}\, M$ for $\mathbb{Z}$-modulen $M = \mathbb{Z}/24\mathbb{Z}$. Og for $M = \mathbb{Z}$.

3. Vis, at en potensrække $f = a_0 + a_1X + a_2X^2 + \cdots \in k[X]$ er invertibel, når blot a_0 er invertibel i k. Vis, at når k er et legeme, så er $k[[X]]$ en lokal ring, og et PID. [Vink: Vis, at idealet (0) og idealerne (X^i) for $i = 0, 1, \ldots$ er samtlige idealer.]

U6 **4.** Lad $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ være idealer i R. Bestem annullatoren for R-modulen $R/\mathfrak{a}_1 \oplus \cdots \oplus R/\mathfrak{a}_n$.

U6 **5.** Mængden af primidealer i ringen R kaldes ringens *primspektrum* og betegnes $\mathrm{Spec}\, R$. Hvornår er primspektret tomt? Beskriv primspektret for et legeme. Bestem for kommutative ringe R_1 og R_2 en naturlig bijektiv afbildning $\mathrm{Spec}(R_1 \times R_2) = \mathrm{Spec}\, R_1 \vee \mathrm{Spec}\, R_2$, hvor højresiden er den disjunkte forening af de to mængder.

U7 **6.** Vis, at en R-lineær afbildning $\varphi\colon M \to Q$ er injektiv (henh. surjektiv, henh. bijektiv), hvis og kun hvis $\varphi_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to Q_{\mathfrak{p}}$ er injektiv (henh. surjektiv, henh. bijektiv) for alle primidealer $\mathfrak{p}$ i R.

7. Antag, at R er et PID. Vis, at hvis M er en endeligt frembragt *torsionsfri* R-modul (dvs $\mathrm{Ann}(x) = (0)$ for $x \neq 0$), så er M fri. [Vink: Lokaliseringen $R_{(0)}$ er brøklegemet for R. Vis, at homomorfien $M \to M_{(0)}$ er injektiv, og benyt det til at vise, at M er undermodul i en fri modul. Slut så til sidst, at M må være fri.]

8. Antag, at $\mathfrak{p} \subset \mathfrak{q}$ er primidealer, og sæt $M := R/\mathfrak{p} \oplus R/\mathfrak{q}$. Bestem $\mathrm{Ann}\, M$ og $\mathrm{Ass}\, M$. Find en modul N som opfylder $\mathrm{Ann}\, M = \mathrm{Ann}\, N$ men $\mathrm{Ass}\, M \supset \mathrm{Ass}\, N$.

U8 **9.** Lad der være givet en endelig mængde af primidealer $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ i R. Angiv en modul M for hvilken $\mathrm{Ass}\, M = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

10. Ligningen $\mathrm{Ass}(M_1 \oplus M_2) = \mathrm{Ass}(M_1) \cup \mathrm{Ass}(M_2)$ er en konsekvens af Noether (1.7.2). Giv, ved at se på annullatorer for elementer (x_1, x_2) i $M_1 \oplus M_2$, et direkte bevis for ligningen.

11. I hvilke af følgende ringe udgør nuldivisorerne et ideal: $\mathbb{Z}$, $\mathbb{Z}/1$, $\mathbb{Z}/8$, $\mathbb{Z}/24$?

12. Vis, at hvis nuldivisorerne udgør et ideal, så er det et primideal.

13. Betragt en ikke nødvendigvis noethersk ring R, som er *reduceret*, dvs opfylder følgende ækvivalente betingelser: (i) 0 er det eneste nilpotente element. (ii) $(0) = \bigcap \mathfrak{p}$, hvor fællesmængden er over alle primidealer $\mathfrak{p}$. (iii) $(0) = \bigcap \mathfrak{n}$, hvor fællesmængden er over alle minimale primidealer $\mathfrak{n}$. (iv) R er delring af et (evt uendeligt) produkt af legemer.

(1) Vis ækvivalensen.

(2) Vis, at enhver annullator $\mathrm{Ann}(a)$ for $a \neq 0$ er indeholdt i et minimalt primideal. [Vink: brug (1)(iii): $a \notin \mathfrak{n} \Rightarrow \mathrm{Ann}(a) \subseteq \mathfrak{n}$.]

(3) Vis, at ethvert minimalt primideal $\mathfrak{n}$ består af nuldivisorer, og slut at mængden $Z(A)$ af nuldivisorer er foreningsmængden $\bigcup \mathfrak{n}$ af minimale primidealer. [Vink: Lad $p \in \mathfrak{n}$. Da $R_{\mathfrak{n}}$ er reduceret, med præcis et primideal (nemlig $\mathfrak{n}R_{\mathfrak{n}}$), er $\mathfrak{n}R_{\mathfrak{n}} = 0$ (og $R_{\mathfrak{n}}$ er et legeme). Af $p/1 = 0$ i $R_{\mathfrak{n}}$ følger, at $sp = 0$ med $s \notin \mathfrak{n}$, hvoraf $p \in \mathrm{Ann}(s)$.]

(4) En modul M kaldes *torsionsfri*, hvis 0 er det eneste torsionselement i M, altså hvis hver annullator $\mathrm{Ann}(m)$ for $m \neq 0$ i M består af nuldivisorer i A, og M kaldes *stærkt torsionsfri* („hjemmelavet“ definition), hvis hver annullator $\mathrm{Ann}(m)$ for $m \neq 0$ i M er indeholdt i et minimalt primideal $\mathfrak{n}$ for A. Vis, at R er stærkt torsionsfri.

(5) Vis at M er stærkt torsionsfri, hvis og kun hvis den kanoniske afbildning $M \to \prod M_{\mathfrak{n}}$ (over minimale primidealer $\mathfrak{n}$) er injektiv.

(6) Vis, at „stærkt torsionsfri“ $\Rightarrow$ „torsionsfri“. Vis, at „(stærk) torsionsfri“ nedarves til undermodul, og bevares ved vilkårlige produkter. Specielt: Ethvert produkt R^I og enhver fri R-modul er stærkt torsionsfri.

(7) Vis, at „stærkt torsionsfri“ $\Leftrightarrow$ „torsionsfri“, når R kun har endelig mange minimale primidealer.

I resten af dette kapitel antages, at R er en noethersk ring.

2. Filtrationsætningen.

(2.1) Sætning. *Lad M være en R-modul. Enhver annullator* $\mathrm{Ann}(y)$*, hvor y er et element forskelligt fra* 0 *i M, er indeholdt i et associeret primideal. Ethvert primideal $\mathfrak{p}$ i støtten for M indeholder et associeret primideal. Specielt eksisterer der associerede primidealer til M, hvis M ikke er nul-modulen.*

Bevis. Sætningens sidste påstand er øjensynlig en konsekvens af den første påstand.

For at vise den første påstand, betragtes mængden af annullatorer $\mathrm{Ann}(x)$ med $x \in M \setminus \{0\}$ og $\mathrm{Ann}(x) \supseteq \mathrm{Ann}(y)$. Da R er noethersk findes en annullator $\mathrm{Ann}(x_0)$, der er maksimal blandt disse annullatorer. Det er klart, at annullatoren $\mathrm{Ann}(x_0)$ er maksimal blandt alle annullatorer $\mathrm{Ann}(x)$ med $x \neq 0$. Af den første påstand i Lemma (1.9) følger, at $\mathrm{Ann}(x_0)$ er et primideal associeret til M, og ifølge valget er $\mathrm{Ann}(y) \subseteq \mathrm{Ann}(x_0)$. Hermed er den første påstand bevist.

Sætningens anden påstand følger tilsvarende af den anden påstand i Lemma (1.9). □

(2.2) Bemærkning. Det følger af Sætning (2.1), at hvert minimalt primideal $\mathfrak{q}$ for M, altså et primideal $\mathfrak{q}$ der er minimalt blandt primidealerne i støtten for M, må være et associeret primideal. For moduler i almindelighed kan man vise, ved hjælp af Zorn's Lemma, at hvert primideal i støtten for M indeholder et minimalt primideal for M. For modulerne behandlet her (endeligt frembragte over en noethersk ring) er det en direkte konsekvens af det efterfølgende resultat.

(2.3) Filtrationssætning. *Lad M være en endeligt frembragt R-modul. Da gælder:* (1) *Der findes i M en filtration,*

$$(0) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = M,$$

hvor de successive kvotienter F_i/F_{i-1}, for $i = 1, \dots, n$, er isomorfe med moduler af formen $R/\mathfrak{p}_i$, hvor $\mathfrak{p}_i$ er et primideal.

(2) *For enhver sådan filtration i M gælder følgende relationer mellem mængder af primidealer,*

$$\mathrm{Ass}\, M \subseteq \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} \subseteq \mathrm{Supp}\, M.$$

Yderligere vil ethvert primideal i støtten for M indeholde et af $\mathfrak{p}_i$'erne, og de tre mængder ovenfor har de samme minimale elementer.

(3) *Lad $\mathfrak{p}$ være et minimalt primideal for M. Da er antallet af gange $R/\mathfrak{p}$ forekommer som kvotient i filtrationen, dvs antallet af i'er for hvilke F_i/F_{i-1} er isomorf med $R/\mathfrak{p}$, entydigt bestemt, idet antallet er lig med længden,* $\mathrm{long}_{R_\mathfrak{p}} M_\mathfrak{p}$*, af $R_\mathfrak{p}$-modulen $M_\mathfrak{p}$.*

Bevis. (1) Sæt $F_0 := (0)$. Hvis $M = 0$, er den ønskede filtration opnået, med $n = 0$ (og ingen kvotienter). Antag derfor, at $M \neq 0$. Af den sidste påstand i Sætning (2.1) følger så, at M har en undermodul F_1 isomorf med $R/\mathfrak{p}$, hvor $\mathfrak{p}$ er et (associeret) primideal. Hvis $F_1 = M$ er den ønskede filtration opnået. Ellers er $M/F_1 \neq 0$. Af Sætning (2.1) følger så igen, at M/F_1 har en undermodul isomorf med $R/\mathfrak{p}_2$, hvor $\mathfrak{p}_2$ er et primideal. Ifølge Noether's anden Isomorfisætning svarer denne undermodul i M/F_1 til en undermodul $F_2 \supseteq F_1$, og F_2/F_1 er isomorf med $R/\mathfrak{p}_2$. Hvis $F_2 = M$ er den ønskede filtration opnået. Ellers fortsættes processen med M/F_2. Da M er endeligt frembragt, og dermed noethersk, stopper processen efter endelig mange skridt, med den ønskede filtration.

(2) Betragt nu en given filtration af formen i (1). Den første inklusion vises ved induktion efter n. Hvis $n = 0$ er venstresiden tom, så inklusionen gælder. Hvis $n > 0$ følger det af Sætning (1.7), at

$$\operatorname{Ass} M \subseteq \operatorname{Ass} F_{n-1} \cup \operatorname{Ass}(M/F_{n-1}).$$

Ifølge induktionsantagelsen er $\operatorname{Ass} F_{n-1}$ indeholdt i $\{\mathfrak{p}_1, \dots, \mathfrak{p}_{n-1}\}$, og ifølge Eksempel (1.6) er $\operatorname{Ass}(M/F_{n-1}) = \operatorname{Ass}(R/\mathfrak{p}_n) = \{\mathfrak{p}_n\}$. Heraf følger den første inklusion.

Betragt nu et vilkårligt primideal $\mathfrak{p}$ i R. Ved lokalisering i $\mathfrak{p}$ fremkommer en filtration i $M_\mathfrak{p}$: Ifølge Isomorfisætningen for brøkmoduler er $(F_{i-1})_\mathfrak{p}$ en undermodul i $(F_i)_\mathfrak{p}$, og den tilsvarende kvotient er $(F_i/F_{i-1})_\mathfrak{p}$. Denne sidste kvotient er ifølge antagelsen isomorf med $(R/\mathfrak{p}_i)_\mathfrak{p}$, som ligeledes kan bestemmes af Isomorfisætningen for brøkmoduler: den er isomorf med $R_\mathfrak{p}/\mathfrak{p}_i R_\mathfrak{p}$. Her gælder ifølge Lokaliseringsprincippet, at kvotienten er lig med 0, hvis og kun hvis $\mathfrak{p}_i \not\subseteq \mathfrak{p}$. Altså er

$$(F_i)_\mathfrak{p}/(F_{i-1})_\mathfrak{p} = \begin{cases} R_\mathfrak{p}/\mathfrak{p}_i R_\mathfrak{p} & \text{hvis } \mathfrak{p}_i \subseteq \mathfrak{p}, \\ 0 & \text{ellers.} \end{cases}$$

Det er klart, at $M_\mathfrak{p} \neq 0$, hvis og kun hvis mindst en af kvotienterne $(F_i)_\mathfrak{p}/(F_{i-1})_\mathfrak{p}$ er forskellig fra 0. Af udregningen ovenfor fremgår, at dette indtræffer, hvis og kun hvis $\mathfrak{p}$ indeholder et af $\mathfrak{p}_i$'erne. Altså er $\mathfrak{p}$ element i støtten $\operatorname{Supp} M$, hvis og kun hvis $\mathfrak{p}$ indeholder et af $\mathfrak{p}_i$'erne. Heraf følger den anden inklusion i (2). Desuden følger det, at mængden af $\mathfrak{p}_i$'er og mængden af primidealer i støtten har de samme minimale elementer.

Det skal endelig godtgøres, at mængden af $\mathfrak{p}_i$'er og mængden af associerede primidealer for M har de samme minimale elementer. Da den første mængde omfatter den anden, er det hertil nok at vise, at hvert $\mathfrak{p}_i$ indeholder et associeret primideal for M. Denne sidste påstand følger af Sætning (2.1), idet hvert $\mathfrak{p}_i$ tilhører støtten for M.

(3) Antag nu, at $\mathfrak{p}$ er et minimalt primideal for M. Da $\mathfrak{p}_i$'erne tilhører støtten for M, er det så udelukket, at $\mathfrak{p}_i \subset \mathfrak{p}$. Det fremgår derfor af udregningen ovenfor, at kvotienten $(F_i)_\mathfrak{p}/(F_{i-1})_\mathfrak{p}$ er forskellig fra 0 præcis når $\mathfrak{p}_i = \mathfrak{p}$. Yderligere ses, at når kvotienten er forskellig fra 0, så er den isomorf med $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$. Denne sidste kvotient er netop den lokale ring $R_\mathfrak{p}$ modulo maksimalidealet $\mathfrak{p}R_\mathfrak{p}$. I den fremkomne filtration af $M_\mathfrak{p}$ er kvotienterne, der er forskellige fra 0, altså simple $R_\mathfrak{p}$-moduler. Følgelig har $M_\mathfrak{p}$ endelig længde, og da antallet af simple kvotienter netop var antallet af i'er for hvilke $\mathfrak{p}_i = \mathfrak{p}$, følger påstanden. □

(2.4) Bemærkning. Af Filtrationssætningen følger for en endeligt frembragt modul M, at der kun er endelig mange associerede primidealer, og dermed specielt kun endelig mange minimale primidealer. Associerede primidealer, der ikke er minimale, siges også at være *indlejrede primidealer* for M.

(2.5) Korollar. *Lad M være en endeligt frembragt R-modul. Da er følgende betingelser ækvivalente:*

(i) *Modulen M har endelig længde.*

(ii) *Alle primidealer i støtten* Supp M *er maksimalidealer.*
(iii) *Alle primidealer, der omfatter* Ann M, *er maksimalidealer.*

Er disse betingelser opfyldt, så består støtten for M af endelig mange maksimalidealer $\mathfrak{m}_1, \dots, \mathfrak{m}_q$, og afbildningen, som afbilder $x \in M$ på q-sættet med brøken $x/1$ i $M_{\mathfrak{m}_j}$ på den j'te plads, er en isomorfi,

$$M \xrightarrow{\sim} M_{\mathfrak{m}_1} \times \cdots \times M_{\mathfrak{m}_q}.$$

Bevis. Betingelserne (ii) og (iii) er ækvivalente ifølge (1.5).

At M har endelig længde betyder, at der i M findes en filtration,

$$(0) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = M, \tag{$*$}$$

hvor de successive kvotienter F_i/F_{i-1} er simple moduler, dvs isomorfe med kvotienter $R/\mathfrak{p}_i$ hvor $\mathfrak{p}_i$'erne er maksimalidealer i R. Hvis (i) er opfyldt, findes altså en filtration som i Filtrationssætningen, hvor $\mathfrak{p}_i$'erne er maksimalidealer. Da ethvert primideal i støtten indeholder et af disse $\mathfrak{p}_i$'er, må hvert primideal i støtten være lig med et af disse $\mathfrak{p}_i$'er. Altså gælder (ii), og yderligere ses, at støtten består af disse endelig mange maksimalidealer.

Antag omvendt, at (ii) gælder, og betragt en filtration af M som i Filtrationssætningen. De tilsvarende $\mathfrak{p}_i$'er tilhører støtten for M, så af antagelsen følger, at $\mathfrak{p}_i$'erne er maksimalidealer. Den betragtede filtration har derfor simple kvotienter. Følgelig har M endelig længde, dvs (i) er opfyldt.

Antag nu at betingelserne er opfyldt, altså at der findes en filtration ($*$) med kvotienter $F_i/F_{i-1} = R/\mathfrak{p}_i$, hvor $\mathfrak{p}_i$'erne er maksimalidealer. Betragt den angivne afbildning. Den er øjensynlig R-lineær.

Først vises, at afbildningen er injektiv. Lad y være et element i kernen, og antag, at $y \neq 0$. Det følger da af Sætning (2.1), at annullatoren $\operatorname{Ann}(y)$ er indeholdt i et associeret primideal til M. De associerede primidealer er netop $\mathfrak{m}_j$'erne, så $\operatorname{Ann}(y)$ er indeholdt i et af $\mathfrak{m}_j$'erne. Men dette strider mod at $y/1 = 0$ i $M_{\mathfrak{m}_j}$ for alle j. Altså er $y = 0$. Følgelig er afbildningen injektiv.

Dernæst vises for hvert maksimalideal $\mathfrak{m}$ i støtten for M, at brøkmodulen $M_{\mathfrak{m}}$, der ifølge Filtrationssætningen er en $R_{\mathfrak{m}}$-modul af endelig længde, også er af endelig længde (og endda af samme længde) som R-modul. Denne påstand følger af, at der ved lokalisering i $\mathfrak{m}$ fremkommer en filtration i $M_{\mathfrak{m}}$ hvor kvotienterne forskellige fra 0 er af formen $R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}}$. Da $\mathfrak{m}$ er et maksimalideal i R, er den sidste kvotient ifølge Lokaliseringsprincippet isomorf med $R/\mathfrak{m}$, så kvotienterne er simple som R-moduler.

Nu kan bijektiviteten af afbildningen vises ved et længde-argument. Længden af venstresiden er længden af M, altså lig med n, hvor n er antallet af kvotienter i filtrationen. På den anden side er $\mathfrak{m}_j$'erne netop de forskellige blandt $\mathfrak{p}_i$'erne, så af Filtrationssætningen følger, at tallet n netop er summen af længderne long $M_{\mathfrak{m}_j}$. Altså har homomorfiens venstre- og højreside samme længde. Da homomorfien er injektiv, følger det at den er en isomorfi. □

(2.6) Opgaver.

U7 **1.** Antag, at R er noethersk og M er endeligt frembragt. Lad $\mathfrak{q}_1, \dots, \mathfrak{q}_k$ være de associerede primidealer for M (i en vilkårlig given rækkefølge). Vis, at der findes en filtration (0) =

$F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = M$, hvor de successive kvotienter har formen $R/\mathfrak{p}_i$ med primidealer $\mathfrak{p}_i$ således, at $\mathfrak{p}_j = \mathfrak{q}_j$ for $j = 1, \dots, k$.

2. Lad M være en endeligt frembragt R-modul. Vis, at hvis $\operatorname{Ann} M$ er et primideal $\mathfrak{p}$, så er $\mathfrak{p}$ associeret til M. [Vink: Hvis $e_1, \dots, e_n$ frembringer M, så er $\mathfrak{p} = \operatorname{Ann}(e_1) \cap \cdots \cap \operatorname{Ann}(e_n)$.]

3. Antag, at M er en endeligt frembragt R-modul. Vis, at hvert primideal associeret til $R/\operatorname{Ann} M$ er associeret til M. [Vink: Lad $r \in R$ og lad $\bar{r}$ være restklassen af r modulo $\operatorname{Ann} M$. Vis, at $\operatorname{Ann}(\bar{r}) = \operatorname{Ann}(rM)$.]

U7 **4.** Lad M være en endeligt frembragt modul over en noethersk ring R, og lad $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ være de associerede primidealer. Vis, at den naturlige homomorfi $M \to M_{\mathfrak{p}_1} \times \cdots \times M_{\mathfrak{p}_n}$ er injektiv. [Vink: Overvej, at intet primideal kan være associeret til homomorfiens kerne.]

3. Dekomposition.

(3.1) Definition. Lad M være en R-modul. En undermodul N i M siges da at være en *primær undermodul*, hvis der er netop ét primideal associeret til kvotientmodulen M/N. At $\mathfrak{p}$ er det eneste primideal associeret til M/N, altså at $\operatorname{Ass}(M/N) = \{\mathfrak{p}\}$, udtrykkes ved at sige, at N er en $\mathfrak{p}$-*primær* undermodul i M.

Betragt en endeligt frembragt R-modul $Q \neq 0$, og de associerede primidealer $\mathfrak{p}_1, \dots, \mathfrak{p}_q$ for Q. Foreningsmængden af idealerne $\mathfrak{p}_i$ er da mængden $Z_R(Q)$ af nuldivisorer på Q:

$$Z_R(Q) = \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_q.$$

De minimale blandt idealerne $\mathfrak{p}_i$ er netop de minimale blandt primidealerne, der omfatter annullatoren for Q. Følgelig er fællesmængden af idealerne $\mathfrak{p}_i$ lig med radikalet af annullatoren:

$$\operatorname{Rad}(\operatorname{Ann} Q) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_q.$$

Fællesmængden er skarpt indeholdt i foreningsmængden med mindre $q = 1$. Med andre ord: Der er netop ét associeret primideal for Q, hvis og kun hvis $Q \neq 0$ og der for enhver nuldivisor f på Q gælder, at en potens af f annullerer Q.

Anvendt med $Q := M/N$, hvor M er endeligt frembragt, følger det: En undermodul N er primær i M, hvis og kun hvis $Z_R(M/N) = \operatorname{Rad}(\operatorname{Ann} M/N)$; er dette opfyldt, så er N en $\mathfrak{p}$-primær undermodul med $\mathfrak{p} = \operatorname{Rad}(\operatorname{Ann} M/N)$ (som automatisk er et primideal).

Specitel for $M = R$ fås følgende:

Karakterisering. *Idealet $\mathfrak{q}$ er et primært ideal i R, hvis og kun hvis følgende betingelse er opfyldt: $\mathfrak{q} \subset R$ og for alle $f, g \in R$ gælder, at hvis $fg \in \mathfrak{q}$ og $g \notin \mathfrak{q}$, så er $f \in \operatorname{Rad}(\mathfrak{q})$; er dette opfyldt, er $\mathfrak{p} = \operatorname{Rad}(\mathfrak{q})$ et primideal, og $\mathfrak{q}$ er $\mathfrak{p}$-primær.*

Betingelserne $fg \in \mathfrak{q}$ og $g \notin \mathfrak{q}$ udtrykker jo netop, at f er nuldivisor på $R/\mathfrak{q}$, og konklusionen, $f \in \operatorname{Rad}(\mathfrak{q})$, udtrykker, at en potens af f annullerer $R/\mathfrak{q}$.

En undermodul N i M siges at være *irreducibel*, hvis $N \subset M$ og N ikke kan skrives som en fællesmængde $N = N_1 \cap N_2$, hvor $N \subset N_1$ og $N \subset N_2$.

(3.2) Lemma. (1) *En irreducibel undermodul er primær.*

(2) *En fællesmængde af to $\mathfrak{p}$-primære undermoduler er selv $\mathfrak{p}$-primær.*

Bevis. (1) Lad N være en irreducibel undermodul i M. Specielt er så $M/N \neq 0$. Der findes derfor associerede primidealer for M/N, jfr Sætning (2.1). Det skal nu vises, at kvotientmodulen M/N kun har ét associeret primideal. Antag, indirekte, at $\mathfrak{p}_1$ og $\mathfrak{p}_2$ er associerede primidealer for M/N, og at de er forskellige. For $i = 1, 2$ har kvotienten M/N da en undermodul $\bar{N}_i$ isomorf med $R/\mathfrak{p}_i$. Specielt er $\mathfrak{p}_i$ det eneste primideal associeret til $\bar{N}_i$. Fællesmængden $\bar{N}_1 \cap \bar{N}_2$ er indeholdt i $\bar{N}_1$. Et primideal, der er associeret til fællesmængden er derfor også associeret til $\bar{N}_1$, jfr Lemma (1.7), og det må følgelig være lig med $\mathfrak{p}_1$. Med samme begrundelse måtte det være lig med $\mathfrak{p}_2$. Da $\mathfrak{p}_1 \neq \mathfrak{p}_2$ konkluderes derfor, at fællesmængden $\bar{N}_1 \cap \bar{N}_2$ ikke har associerede primidealer. Af Sætning (2.1) følger derfor, at $\bar{N}_1 \cap \bar{N}_2 = (0)$.

Ifølge Noether's anden Isomorfisætning svarer undermodulerne $\bar{N}_i$ i M/N til undermoduler $N_i \supseteq N$. Af det viste følger at $N_1 \cap N_2 = N$. Yderligere er $N_i \supset N$, da $\bar{N}_i \neq 0$. Da N var irreducibel, har antagelsen således ført til en modstrid, som ønsket.

(2) Lad $N = N_1 \cap N_2$ være en fællesmængde af $\mathfrak{p}$-primære moduler N_1 og N_2. Det er klart, at $M/N \neq 0$, så det skal vises, at $\mathfrak{p}$ er det eneste associerede primideal for M/N. Lad hertil $\mathfrak{q}$ være et associeret primideal for M/N. Betragt homomorfien

$$M \to M/N_1 \oplus M/N_2, \tag{$*$}$$

der til et element i M knytter parret af restklasser modulo N_1 og modulo N_2. Kernen for denne homomorfi er øjensynlig fællesmængden $N_1 \cap N_2$, altså N, så ifølge Isomorfisætningen er kvotienten M/N isomorf med en undermodul af den direkte sum på højresiden i $(*)$. Primidealet $\mathfrak{q}$ er derfor associeret til en undermodel af den direkte sum, og dermed også associeret til den direkte sum, jfr (1.7.2). Af den anden inklusion i (1.7.2), anvendt på en af summanderne i den direkte sum, følger, at et primideal associeret til summen må være associeret til en af summanderne M/N_i. Ifølge forudsætningen er $\mathfrak{p}$ det eneste primideal associeret til M/N_i. Altså må $\mathfrak{q}$ være lig med $\mathfrak{p}$, som ønsket. □

(3.3) Eksempel. (1) Et primideal $\mathfrak{p}$ er en $\mathfrak{p}$-primær undermodul i R. Som vist i Eksempel (1.6) er nemlig $\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$.

(2) Lad $\mathfrak{m}$ være et maksimalideal. Enhver potens $\mathfrak{m}^m$, hvor $m \geqslant 1$, og mere generelt, ethvert ideal $\mathfrak{a}$ således at

$$\mathfrak{m}^m \subseteq \mathfrak{a} \subseteq \mathfrak{m},$$

vil da være et $\mathfrak{m}$-primært ideal i R. Ifølge Eksempel (1.6) består støtten for $R/\mathfrak{a}$ nemlig af de primidealer $\mathfrak{p}$, som omfatter $\mathfrak{a}$. Af $\mathfrak{a} \subseteq \mathfrak{p}$ følger, at potensen $\mathfrak{m}^m$ er indeholdt i $\mathfrak{p}$. Da $\mathfrak{p}$ er et primideal, følger det videre, at en af faktorerne i produktet $\mathfrak{m}^m$, dvs $\mathfrak{m}$, er indeholdt i $\mathfrak{p}$. Da $\mathfrak{m}$ er et maksimalideal følger det endelig, at $\mathfrak{p} = \mathfrak{m}$. Det er således godtgjort, at støtten for $R/\mathfrak{a}$ består af det ene primideal $\mathfrak{m}$. Og så er $\mathfrak{m}$ også det eneste associerede primideal til $R/\mathfrak{a}$ ifølge Sætning (2.1).

(3.4) Primærdekomposition. Lad N være en undermodul i modulen M. Ved en *primærdekomposition* af N forstås en fremstilling af N som en fællesmængde,

$$N = N_1 \cap \cdots \cap N_q,$$

hvor N_j'erne er primære undermoduler. Antag, at N_j er $\mathfrak{p}_j$-primær. Dekompositionen siges da at være *uforkortelig*, hvis $\mathfrak{p}_j$'erne er forskellige og ingen af N_j'erne i fællesmængden er overflødige.

Det følger af Lemma (3.2), at man ud fra en primærdekompostion af N kan opnå en uforkortelig dekomposition: Først erstattes for hvert primideal $\mathfrak{p}$ de N_j'er, der er $\mathfrak{p}$-primære, med deres fællesmængde, og dernæst bortkastes overflødige N_j'er.

(3.5) Dekompositionssætning. *Lad M være en endeligt frembragt R-modul. Da har hver undermodul N en primærdekomposition,*

$$N = N_1 \cap \cdots \cap N_q. \tag{3.5.1}$$

Antag, at en sådan dekomposition er uforkortelig, og at N_j er $\mathfrak{p}_j$-primær. Da er $\mathfrak{p}_j$'erne netop primidealerne associerede til M/N. Yderligere gælder, at de undermoduler N_j, for hvilke $\mathfrak{p}_j$ er et minimalt primideal for M/N, er entydigt bestemte, idet N_j er kernen for den sammensatte homomorfi $M \to M/N \to (M/N)_{\mathfrak{p}_j}$.

Bevis. For at vise eksistensen af fremstillingen er det ifølge Lemma (3.2) nok at vise, at enhver undermodul N er en endelig fællesmængde af irreducible undermoduler. Denne påstand vises ved noethersk induktion: Antag, indirekte, at påstanden er gal, og betragt mængden $\mathcal{S}$ af de undermoduler i M, der ikke er en endelig fællesmængde af irreducible undermoduler. Ifølge antagelsen er $\mathcal{S}$ ikke tom. Da M er endeligt frembragt over en noethersk ring, er M noethersk. Følgelig findes i $\mathcal{S}$ en undermodul N, der er maksimal blandt undermodulerne i $\mathcal{S}$. Undermodulen N tilhører $\mathcal{S}$, og specielt kan den derfor ikke være irreducibel. Yderligere er $N \subset M$, idet M har en fremstilling af den ønskede form, nemlig som fællesmængde af ingen irreducible moduler. Da $N \subset M$ og N ikke er irreducibel, er N en fællesmængde, $N = N_1 \cap N_2$, af undermoduler $N_i \supset N$. Da N var maksimal blandt undermodulerne i $\mathcal{S}$, kan ingen af undermodulerne N_i tilhøre $\mathcal{S}$. Følgelig er begge undermoduler N_1 og N_2 en endelig fællesmængde af irreducible undermoduler, og så er fællesmængden N det også, i modstrid med at N var element i $\mathcal{S}$.

Antag nu, at fremstillingen (3.5.1) er uforkortelig. Betragt homomorfien,

$$M/N \to M/N_1 \oplus \cdots \oplus M/N_q, \tag{$*$}$$

der afbilder restklassen af x modulo N i q-sættet hvis j'te koordinat er restklassen af x modulo N_j. Denne homomorfi er veldefineret, da $N \subseteq N_j$, og den er injektiv, da N er fællesmængden af N_j'erne. Lad $\mathfrak{p}$ være et primideal associeret med M/N. Af Lemma (1.7) følger nu først, at $\mathfrak{p}$ er associeret med den direkte sum på højresiden af $(*)$, og dernæst at $\mathfrak{p}$ er associeret med en af addenderne M/N_j. Da M/N_j er $\mathfrak{p}_j$-primær, er $\mathfrak{p}_j$ det eneste primideal associeret med M/N_j. Altså er $\mathfrak{p}$ lig med et af $\mathfrak{p}_j$'erne.

Betragt omvendt et af primidealerne $\mathfrak{p}_k$. Lad M_k være fællesmængden af de N_j'er, hvor N_k ikke medtages, og lad Q være kvotientmodulen $Q := M_k/N$. Af Noether's anden Isomorfisætning følger, at $Q = M_k/N$ er isomorf med en undermodul i M/N. På den anden side er øjensynlig $N = M_k \cap N_k$, så af Noether's første Isomorfisætning følger, at $Q = M_k/(M_k \cap N_k)$ er isomorf med en undermodul i M/N_k. Af Lemma (1.7) fås derfor inklusionerne,

$$\operatorname{Ass} Q \subseteq \operatorname{Ass}(M/N), \quad \operatorname{Ass} Q \subseteq \operatorname{Ass}(M/N_k).$$

Modulen M/N_k er $\mathfrak{p}_k$-primær, så mængden på højresiden af den sidste inklusion indeholder ét element, nemlig primidealet $\mathfrak{p}_k$. Modulen M_k opfylder at $M_k \supset N$, thi ellers var jo N_k overflødig i fremstillingen (3.5.1). Kvotienten $Q = M_k/N$ er derfor forskellig fra 0, og $\operatorname{Ass} Q$ er derfor ikke tom ifølge Sætning (2.1). Den anden inklusion ovenfor medfører derfor, at $\operatorname{Ass} Q$ består alene af primidealet $\mathfrak{p}_k$. Den første inklusion ovenfor medfører derfor, at $\mathfrak{p}_k$ er associeret til M/N.

Hermed er det vist, at $\mathfrak{p}_j$'erne er de associerede primidealer til M/N.

For at bevise den sidste del af entydighedsudsagnet betragtes først en vilkårlig endeligt frembragt modul Q, med den egenskab at Ass Q består af netop et primideal $\mathfrak{p}$. Det påstås, at den kanoniske homomorfi,

$$Q \to Q_{\mathfrak{p}},$$

da er injektiv. Antag nemlig, at y er et element forskelligt fra 0 i homomorfiens kerne. Da brøken $y/1$ er lig med 0 i $Q_{\mathfrak{p}}$, er $\mathrm{Ann}(y)$ ikke indeholdt i $\mathfrak{p}$. Men det er i modstrid med at $\mathrm{Ann}(y)$ er indeholdt i et associeret primideal ifølge Sætning (2.1) og $\mathfrak{p}$ er det eneste associerede primideal for Q.

Lad nu $\mathfrak{p}_j$ være et minimalt primideal for M/N. Betragt homomorfien, der fremkommer af $(*)$ ved lokalisering i $\mathfrak{p}_j$. For $k \neq j$ består støtten for M/N_k af de primidealer, der omfatter $\mathfrak{p}_k$, og $\mathfrak{p}_j$ er ikke et sådant primideal, da $\mathfrak{p}_j$ er minimalt blandt $\mathfrak{p}_k$'erne. Altså er $(M/N_k)_{\mathfrak{p}_j} = 0$ for $k \neq j$. Den lokaliserede homomorfi er derfor følgende homomorfi,

$$(M/N)_{\mathfrak{p}_j} \to (M/N_j)_{\mathfrak{p}_j}. \tag{$**$}$$

Homomorfien $(*)$ var injektiv, så det følger af Isomorfisætning for Brøkmoduler, at den lokaliserede homomorfi $(**)$ er injektiv. På den anden side følger det af påstanden ovenfor, anvendt på $Q := M/N_j$ og $\mathfrak{p} := \mathfrak{p}_j$, at homomorfien $M/N_j \to (M/N_j)_{\mathfrak{p}_j}$ er injektiv. Det er klart, at følgende diagram er kommutativt,

$$\begin{tikzcd} M \arrow[r] \arrow[d] & M/N_j \arrow[d] \\ (M/N)_{\mathfrak{p}_j} \arrow[r] & (M/N_j)_{\mathfrak{p}_j}. \end{tikzcd}$$

De to homomorfier, der ender i $(M/N_j)_{\mathfrak{p}_j}$, er ifølge det viste injektive. De to homomorfier, der begynder i M, har derfor samme kerne. Heraf følger øjensynlig Sætningens påstand om entydigheden af N_j. □

(3.6) Eksempel. (1) Lad $\mathfrak{a}$ være en fællesmængde af primidealer,

$$\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_q. \tag{3.6.1}$$

Det følger af Eksempel (3.3)(1), at fremstillingen (3.6.1) er en primærdekomposition. Antag, at der ikke er inklusioner mellem $\mathfrak{p}_j$'erne, altså at intet $\mathfrak{p}_j$ er indeholdt i et af de øvrige. Da er dekompositionen uforkortelig, thi $\mathfrak{p}_j$'erne er specielt forskellige, og var et af $\mathfrak{p}_j$'erne, fx $\mathfrak{p}_k$, overflødigt, så ville primidealet $\mathfrak{p}_k$ indeholde fællesmængden af de øvrige, og heraf følger som bekendt, at $\mathfrak{p}_k$ ville indeholde et af de øvrige. Det følger af Dekompositionssætningen, at $\mathfrak{p}_j$'erne er de associerede primidealer til $R/\mathfrak{a}$.

(2) Lad $\mathfrak{m}_1, \dots, \mathfrak{m}_q$ være forskellige maksimalidealer i R, og betragt en fællesmængde,

$$\mathfrak{a} = \mathfrak{m}_1^{m_1} \cap \cdots \cap \mathfrak{m}_q^{m_q}, \tag{3.6.2}$$

hvor eksponenterne m_j er positive. Da er (3.6.2) en uforkortelig primærdekomposition af $\mathfrak{a}$. Det følger nemlig først af Eksempel (3.3)(2), at idealet $\mathfrak{m}_j^{m_j}$ er $\mathfrak{m}_j$-primært. Videre er ingen af idealerne $\mathfrak{m}_j^{m_j}$ overflødige i fællesmængden. Antag nemlig, indirekte, at fx $\mathfrak{m}_1^{m_1}$ er overflødig. Da vil $\mathfrak{m}_1^{m_1}$ indeholde fællesmængden af de øvrige $\mathfrak{m}_j^{m_j}$'er. Specielt vil primidealet $\mathfrak{m}_1$ indeholde denne fællesmængde. Som bekendt følger heraf, at $\mathfrak{m}_1$ indeholder et af idealerne $\mathfrak{m}_j^{m_j}$ for $j > 1$, og videre, at $\mathfrak{m}_1$ indeholder $\mathfrak{m}_j$. Dette er en modstrid, da $\mathfrak{m}_j$ er et maksimalideal og $\mathfrak{m}_1 \neq \mathfrak{m}_j$.

Af Dekompositionssætningen fremgår nu, at $\mathfrak{m}_j$'erne er de associerede primidealer til $R/\mathfrak{a}$. Af korollaret til Filtrationssætningen følger videre, at $R/\mathfrak{a}$ har endelig længde.

(3) Antag, at ringen R er faktoriel, og betragt et element f med primopløsningen $f = p_1^{m_1} \cdots p_q^{m_q}$ (hvor altså p_j'erne er irreducible og ikke associerede, og m_j'erne positive). Ved brug af den entydige primopløsning ses det let, at

$$(f) = (p_1^{m_1}) \cap \cdots \cap (p_q^{m_q}). \tag{3.6.3}$$

Af Eksempel (3.3)(2) følger, at fremstillingen ovenfor er en uforkortelig primærdekomposition af hovedidealet (f).

(4) Lad $\mathfrak{m}$ være et maksimalideal og lad $\mathfrak{p}$ være et primideal forskelligt fra $\mathfrak{m}$ og således at $\mathfrak{p} \not\subseteq \mathfrak{m}^2$. Betragt fællesmængden,

$$\mathfrak{a} = \mathfrak{p} \cap \mathfrak{m}^2. \tag{3.6.4}$$

Det ses ganske som under (1) eller (2), at (3.6.4) er en uforkortelig primærdekomposition. Primidealerne $\mathfrak{m}$ og $\mathfrak{p}$ er altså de associerede primidealer til $R/\mathfrak{a}$. Hvis $\mathfrak{p} \subseteq \mathfrak{m}$ (og dette er ikke udelukket), så er $\mathfrak{p}$ det eneste minimale primideal for $R/\mathfrak{a}$ og $\mathfrak{m}$ er et indlejret primideal.

(3.7) Bemærkning. Dekompositionssætningen kan specielt anvendes på et ideal $\mathfrak{a}$ i R. Som konsekvens fås en uforkortelig primærdekomposition,

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_q,$$

hvor idealet $\mathfrak{q}_j$ er $\mathfrak{p}_j$-primært. De minimale primidealer $\mathfrak{p}$ for $R/\mathfrak{a}$ er de minimale blandt primidealerne, der omfatter $\mathfrak{a}$, jfr Eksempel (1.6). Hvis $\mathfrak{p}_j$ er et sådant primideal, så er $\mathfrak{q}_j$ entydigt bestemt, nemlig som kernen for den sammensatte homomorfi $R \to R/\mathfrak{a} \to (R/\mathfrak{a})_{\mathfrak{p}_j}$. Her er kvotienten $(R/\mathfrak{a})_{\mathfrak{p}_j}$ ifølge Lokaliseringsprincippet lig med $R_{\mathfrak{p}_j}/\mathfrak{a}R_{\mathfrak{p}_j}$. Heraf ses, at $\mathfrak{q}_j$ er kontraktionen af ekstensionen $\mathfrak{a}R_{\mathfrak{p}_j}$.

Specielt ses, at hvis $\mathfrak{q}$ er et $\mathfrak{p}$-primært ideal, så er homomorfien $R/\mathfrak{q} \to R_\mathfrak{p}/\mathfrak{q}R_\mathfrak{p}$ injektiv. Hvis $\mathfrak{p} = \mathfrak{m}$ er et maksimalideal, følger det endda af Korollar (2.5), at denne homomorfi er en isomorfi. Specielt fremhæves for en potens $\mathfrak{m}^i$, at lokalisering i $\mathfrak{m}$ inducerer en isomorfi,

$$R/\mathfrak{m}^i \xrightarrow{\sim} R_\mathfrak{m}/\mathfrak{m}^i R_\mathfrak{m}.$$

(3.8) Opgaver.

U7 **1.** Antag, at $\mathfrak{q}$ er et $\mathfrak{p}$-primært ideal i R. Vis for idealer $\mathfrak{a}$ og $\mathfrak{b}$, at hvis $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{q}$ og $\mathfrak{a} \not\subseteq \mathfrak{q}$, så er $\mathfrak{b} \subseteq \mathfrak{p}$.

U7 **2.** Antag, at R er et PID. Antag, at $a \in R$ har primopløsningen $a = up_1^{\nu_1} \cdots p_r^{\nu_r}$, hvor $u \in R^*$ og elementerne $p_1, \dots, p_r$ er ikke-associerede. Bestem $\mathrm{Rad}(a)$. Bestem de primære idealer i R.

U7 **3.** Antag, at R er et integritetsområde og at $p \in R$ er et primelement, dvs at $p \neq 0$ og hovedidealet (p) er et primideal. Vis, at potenserne (p^m), hvor $m \geqslant 1$, er (p)-primære idealer.

4. Betragt polynomiumsringen $R = k[X, Y]$, hvor k er et legeme, og idealet $\mathfrak{m} = (X, Y)$ som R-modul. Vis, at $\operatorname{Ass}(\mathfrak{m}) = \{(0)\}$. Vis, at i følgende filtration af $\mathfrak{m}$,

$$(0) \subset (Y) \subset (X^2, Y) \subset (X, Y) = \mathfrak{m}$$

har de successive kvotienter formen $R/\mathfrak{p}_i$ med primidealer $\mathfrak{p}_i$. Vis, at i enhver filtration af $\mathfrak{m}$, hvor de successive kvotienter er af denne form, vil der forekomme primidealer ud over primidealet (0). [Vink: i modsat fald ville $\mathfrak{m}$ være en fri R-modul, hvad der ikke kan være tilfældet; eller: Overvej, at der må være mere end 1 kvotient, og at antallet af gange $R/(0)$ forekommer er lig med 1.]

U7 **5.** Betragt polynomiumsringen $R = k[X, Y, Z]$, hvor k er et legeme. Vis, at idealerne $\mathfrak{m} = (X, Y, Z)$, $\mathfrak{p} = (X, Z)$ og $\mathfrak{q} = (Y, Z)$ er primidealer. Vis for $M := R/\mathfrak{p}\mathfrak{q}$, at $\operatorname{Ass} M = \{\mathfrak{p}, \mathfrak{q}, \mathfrak{m}\}$. Vis, at den naturlige homomorfi $M \to M_{\mathfrak{p}} \times M_{\mathfrak{q}}$ ikke er injektiv.

6. Lad R være en noethersk ring. Vis, at R er et endeligt produkt af integritetsområder, hvis og kun hvis $R_{\mathfrak{m}}$ er et integritetsområde for alle maksimalidealer $\mathfrak{m}$ (og dermed for alle primidealer $\mathfrak{m}$). [Vink til „hvis“: Vis først, at $\operatorname{Rad}(0) = (0)$ og udled, at $(0) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$, hvor fremstillingen kan antages uforkortelig. Vis dernæst, at den naturlige ringhomomorfi $R \to R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_n$ er en isomorfi (lokaliser i $\mathfrak{m}$!).]

U8 **7.** Vis i $\mathbb{Z}[X]$, at idealet $\mathfrak{m} := (2, X)$ er et maksimalideal og at idealet $(4, X)$ er $\mathfrak{m}$-primært og ikke en potens af $\mathfrak{m}$.

8. *For et ideal $\mathfrak{a}$ i R betegnes med $\mathfrak{a}[X]$ ekstensionen af $\mathfrak{a}$ til $R[X]$. Vis, at hvis $\mathfrak{p}$ er et primideal i R, så er $\mathfrak{p}[X]$ et primideal i $R[X]$. Vis, at hvis $\mathfrak{q}$ er et $\mathfrak{p}$-primært ideal i R, så er $\mathfrak{q}[X]$ et $\mathfrak{p}[X]$-primært ideal i $R[X]$.

9. Antag, at R er noethersk og M er endeligt frembragt. Betragt følgende *betingelse* på M: nuldivisorerne på M udgør et ideal. Vis, at hvis N er en primær undermodul af M, så er betingelsen opfyldt for M/N. Vis, at hvis betingelsen er opfyldt, så udgør nuldivisorerne et associeret primideal. Vis, at hvis $N \subseteq M$ er en irreducibel undermodul, så er betingelsen opfyldt for M/N. [Vink til det sidste: vis det indirekte!]

U8 **10.** Betragt i $R = k[X, Y]$ (hvor k er et legeme) maksimalidealet $\mathfrak{m} = (X, Y)$. Gør rede for, at $\mathfrak{m}^2 = (X^2, XY, Y^2)$ er $\mathfrak{m}$-primært. Vis, at $\mathfrak{m}^2$ ikke er irreducibelt. [Vink: Vis, at $\mathfrak{m}^2$ er en fællesmængde $\mathfrak{a}_1 \cap \mathfrak{a}_2$, hvor $\mathfrak{a}_1 = (X^2, Y)$ og $\ldots$.]

U8 **11.** Vis i $\mathbb{Z}[X]$, at delringen $R := \mathbb{Z}[2X, X^2, X^3]$ består af de polynomier $f = a_0 + a_1 X + \cdots$, hvor koefficienten a_1 (altså koefficienten til X) er lige. Vis at idealet $\mathfrak{p}$, bestående af de polynomier $f \in R$ for hvilke $f(0) = 0$, er et primideal, og vis, at $\mathfrak{p} = (2X, X^2, X^3)$. Vis, at idealet $\mathfrak{p}^2$ ikke er $\mathfrak{p}$-primært. [Vink: $\mathfrak{p}^2 = (4X^2, 2X^3, X^4, X^5, X^6)$, og $4X^2 \in \mathfrak{p}^2$, men $4 \notin \mathfrak{p}$ og $X^2 \notin \mathfrak{p}^2$.]

U8 **12.** Betragt i $R = k[X, Y]$ (hvor k er et legeme) idealerne $\mathfrak{p} = (X)$ og $\mathfrak{m} = (X, Y)$. Vis, at $\mathfrak{p} \subseteq \mathfrak{m}$ er primidealer. Sæt $\mathfrak{a} := \mathfrak{p}\mathfrak{m}$. Vis, at $\operatorname{Rad}(\mathfrak{a})$ er primidealet $\mathfrak{p}$ og at $\mathfrak{a}$ ikke er $\mathfrak{p}$-primært.

U8 **13.** Betragt i $k[X,Y]$ (hvor k er et legeme) idealerne $\mathfrak{p} = (X)$, $\mathfrak{m} = (X,Y)$, $\mathfrak{q} = (X^2, Y)$, og $\mathfrak{a} := \mathfrak{p}\mathfrak{m}$. Vis, at $\mathfrak{a} = (X^2, XY)$. Vis, at $\mathfrak{q}$ er $\mathfrak{m}$-primært. Eftervis følgende ligninger: $\mathfrak{a} = \mathfrak{p} \cap \mathfrak{m}^2 = \mathfrak{p} \cap \mathfrak{q}$, og vis, at begge bestemmer uforkortelige primærdekompositioner af $\mathfrak{a}$.

14. Antag, at R er noethersk og M er endeligt frembragt. Lad $\mathfrak{a}$ være et ideal i R, og betragt undermodulen $N := \bigcap \mathfrak{a}^n M$ i M. Vis, at $N = \mathfrak{a}N$, idet følgende påstande skal eftervises: Da $\mathfrak{a}N \subseteq N$, er det nok at vise, at for hver primær undermodul Q af M med $\mathfrak{a}N \subseteq Q$ er $N \subseteq Q$. Antag hertil, indirekte, at der findes $x \in N$ med $x \notin Q$, og betragt restklassen $\bar{x} \in M/Q$. Da er $\mathfrak{a} \subseteq \mathrm{Ann}(\bar{x})$. Da M/Q er primær, følger det, at hvert $a \in \mathfrak{a}$ har en potens, der annullerer M/Q. Derfor findes en eksponent k således, at $\mathfrak{a}^k M \subseteq Q$. Da $N \subseteq \mathfrak{a}^k M$, følger det at $N \subseteq Q$, – som ønsket.

15. Antag, at nuldivisorerne på M udgør et ideal $\mathfrak{q}$ i R. Vis, at så er $\mathfrak{q}$ et primideal. Vis, at hvis R er noethersk og M er endeligt frembragt, så er $\mathfrak{q}$ et associeret primideal for M.

16. Betragt en kvadratisk talring $R = \mathbb{Z}[\xi]$, hvor ξ er rod i $f = X^2 + bX + c \in \mathbb{Z}[X]$. Bestem en isomorfi $\mathbb{Z}[X]/(f) \xrightarrow{\sim} R$. Udled for hvert primtal p en naturlig isomorfi $\mathbb{F}_p[X]/(f) \xrightarrow{\sim} R/(p)$, idet f opfattes som polynomium i $\mathbb{F}_p[X]$. Vis, at der er følgende tre muligheder: 1° (p) er et maksimalideal i R; 2° (p) er en fællesmængde $(p) = \mathfrak{m}_1 \cap \mathfrak{m}_2$ af to forskellige maksimalidealer; 3° (p) er et kvadrat $(p) = \mathfrak{m}^2$ på et maksimalideal. Vis, at de tre muligheder indtræffer, henholdsvis, når f i $\mathbb{F}_p$ har ingen rødder; to forskellige rødder; en dobbeltrod.

4. Valuationsringe og Dedekindringe.

(4.1) Lemma. *Antag, at R er et (noethersk) integritetsområde. Da har hvert element a i R, som ikke er nul eller en enhed, en irreducibel opløsning, dvs der findes en fremstilling af a som et produkt af irreducible elementer,*

$$a = q_1 \cdots q_n. \tag{$*$}$$

Bevis. Beviset er indirekte, ved noethersk induktion. Antag, at der findes elementer b, som ikke er nul og ikke er enheder og ikke kan skrives som produkt af irreducible elementer. Lad $\mathcal{S}$ betegne mængden af hovedidealer (b) frembragt af sådanne elementer b. Der findes da i $\mathcal{S}$ et hovedideal (b), der er maksimalt blandt hovedidealerne i $\mathcal{S}$. Elementet b kan specielt ikke være irreducibelt, og det er forskelligt fra nul og ikke en enhed. Følgelig er b et produkt $b = b_1 b_2$, hvor faktorerne b_i ikke er enheder. Nu er $(b) \subset (b_2)$. Ellers ville lighed nemlig gælde, og så ville b_2 kunne skrives $b_2 = ab = ab_1 b_2$; da nul-reglen gælder, ville det følge, at $1 = ab_1$, i modstrid med at b_1 ikke er en enhed. Tilsvarende er $(b) \subset (b_1)$.

Af $(b) \subset (b_i)$ følger, at hovedidealerne (b_i) ikke tilhører $\mathcal{S}$. Heraf følger videre, at b_i er et produkt af irreducible elementer. Men det er i modstrid med at $b = b_1 b_2$ og b ikke er et produkt af irreducible elementer. □

(4.2) Sætning. *Lad R være en lokal (noethersk) ring med maksimalidealet $\mathfrak{m}$. Antag, at R er et integritetsområde, men ikke et legeme. Da er følgende betingelser ækvivalente:*

(i) *Maksimalidealet $\mathfrak{m}$ er et hovedideal.*
(ii) *Idealerne i R er totalt ordnede ved inklusion.*
(iii) *Ringen R er et hovedidealområde.*

Bevis. „(i)⇒(ii)“. Antag, at $\mathfrak{m} = (p)$ er hovedidealet frembragt af et element p i R. Da R ikke er et legeme, er $p \neq 0$. Videre er (p) et maksimalideal, og dermed et primideal. Altså er p et primelement. Specielt er p et irreducibelt element. Det påstås, at p, på nær multiplikation med en enhed, er det eneste irreducible element. Betragt nemlig et irreducibelt element q. Specielt er q da ikke en enhed, og følgelig er q element i den lokale rings maksimalideal. Med andre ord er $q \in (p)$, så q kan skrives $q = rp$. Da q er irreducibelt, er r en enhed.

Det følger af Lemma (4.1), at hvert element a, som ikke er nul og som ikke er en enhed, har en fremstilling som produkt af irreducible elementer. Af det allerede viste følger, at denne fremstilling har formen,

$$a = up^n, \tag{4.2.1}$$

hvor u er en enhed og $n \geqslant 1$. For enhederne i R fås en fremstilling (4.2.1) med $n = 0$.

Det påstås nu, at samtlige idealer i R er følgende:

$$(0) \subset \cdots \subset (p^{n+1}) \subset (p^n) \subset \cdots \subset (p) \subset (1).$$

Af denne påstand følger øjensynlig (ii). For at vise påstanden betragtes et vilkårligt ideal $\mathfrak{a} \neq (0)$ i R. Der findes da elementer a i $\mathfrak{a}$ som er forskellige fra 0. Vælg nu blandt alle sådanne elementer a et, for hvilket fremstillingen (4.2.1) har det mindst mulige n. Da a er valgt i $\mathfrak{a}$, er $p^n = u^{-1}a$ element i $\mathfrak{a}$. Følgelig er

$$(p^n) \subseteq \mathfrak{a}.$$

Omvendt har ethvert element $b \neq 0$ i $\mathfrak{a}$ en fremstilling af formen (4.2.1), dvs af formen $b = vp^m$; valget af n sikrer, at $m \geqslant n$, og så er $b = vp^{m-n}p^n$ element i (p^n). Altså er $\mathfrak{a} = (p^n)$. Hermed er den ønskede påstand, og specielt betingelsen (ii) eftervist.

„(ii)⇒(iii)". Antag, at idealerne i R er totalt ordnede. Heraf følger først, at ethvert ideal (a, b) frembragt af 2 elementer er et hovedideal. Af hovedidealerne (a) og (b) vil nemlig et, fx (b), omfatte det andet, og af $(a) \subseteq (b)$ følger, at summen $(a, b) = (a) + (b)$ er lig med (b). I almindelighed er $(a_1, \dots, a_n) = (a_1, \dots, a_{n-1}) + (a_n)$, så ved induktion følger, at hvert endeligt frembragt ideal er et hovedideal. Da R er noethersk, er betingelsen (iii) altså opfyldt.

Implikationen „(iii)⇒(i)" er triviel. Hermed er ækvivalensen bevist. □

(4.3) Definition. En lokal (noethersk) ring, som er et integritetsområde og ikke et legeme og opfylder de ækvivalente betingelser i Sætning (4.2), kaldes en *(diskret) valuationsring*.

(4.4) Note. Betingelsen (ii) har mening for enhver ikke nødvendigvis noethersk ring, og en ring, der opfylder denne betingelse, kaldes ofte en valuationsring. Adjektivet „diskret" går essentielt på forudsætningen om at ringen i Definition (4.3), ligesom ellers i dette kapitel, forudsættes at være noethersk.

(4.5) Bemærkning. Antag, at R er lokal, med maksimalidealet $\mathfrak{m}$, og lad $k := R/\mathfrak{m}$ betegne restklasselegemet. Kvotienten $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ er da en modul over kvotientringen $R/\mathfrak{m}$, dvs et vektorrum over k. Hvis R er en valuationsring, så er

$$\dim_k \mathfrak{m}^i/\mathfrak{m}^{i+1} = 1 \text{ for alle } i,$$

thi potensen $\mathfrak{m}^i$ er hovedidealet (p^i), og det er klart, at $r \mapsto rp^i$ inducerer en isomorfi af $R/(p)$ på $(p^i)/(p^{i+1})$. Det følger i øvrigt af Nakayama's Lemma, at dimensionen $\dim_k \mathfrak{m}^i/\mathfrak{m}^{i+1}$ er lig med det minimale antal frembringere for idealet $\mathfrak{m}^i$. Betingelsen (i) Sætning (4.2) kan således udtrykkes ved ligningen $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$.

(4.6) Eksempel. Antag, at R er en faktoriel ring. For hvert irreducibelt element p er hovedidealet (p) da et primideal. Brøkringen $R_{(p)}$, der fås ved lokalisering i primidealet (p), er en valuationsring, thi maksimalidealet i brøkringen er ekstensionen af hovedidealet (p), og det er derfor et hovedideal. Betingelsen (4.2)(i) er således opfyldt.

Specielt gælder for hvert primtal p, at den lokale ring $\mathbb{Z}_{(p)}$, der består af rationale tal af formen a/s, hvor s ikke er delelig med p, er en valuationsring.

Potensrækkeringen $R[[X]]$ består af uendelige følger $f = (a_0, a_1, a_2, \dots)$ organiseret som ring med addition og multiplikation svarende til det, der kendes for polynomier. Ofte skrives $f = a_0 + a_1X + a_2X^2 + \cdots$, hvor man bedst kan opfatte X^i som en „pladsholder". Det er ikke svært at vise, at potensrækkeringen $k[[X]]$ med koefficienter i et legeme k er en valuationsring.

(4.7) Sætning. *Antag, som i Sætning* (4.2) *at R er et lokalt (noethersk) integritetsområde. Da er R en diskret valuationsring, hvis og kun hvis følgende betingelse er opfyldt:*

(iv) *R har præcis to primiealer, nemlig* (0) *og $\mathfrak{m}$, og R er helt afsluttet i sit brøklegeme.*

Bevis. Med betingelserne i (4.2) viser vi først, at (iii) $\Rightarrow$ (iv): Da R er et PID, er primidealerne forskellige fra (0) netop hovedidealerne (p), hvor (p) er irreducibel, og de er alle maksimalidealer. Da R er lokal, og ikke et legeme, er $\mathfrak{m}$ det eneste primideal $\neq (0)$. Yderligere er R er UFD, og dermed som bekendt helt afsluttet i sit brøklegeme.

Beviset for Sætningen fuldføres nu ved at vise (iv) $\Rightarrow$ (i). Vælg hertil et element $a \in \mathfrak{m}$ med $a \neq 0$. Så er $\mathfrak{m} \supseteq (a)$, og af (iv) fremgår, at $\mathfrak{m}$ er det eneste primideal med denne egenskab. Derfor er $\mathrm{Rad}(a) = \mathfrak{m}$, og heraf følger videre, at der findes en potens $\mathfrak{m}^n \subseteq (a)$. Vælg n mindst mulig, eller rettere, lad $k \geqslant 0$ være bestemt ved at $\mathfrak{m}^k \not\subseteq (a)$ og $\mathfrak{m}^{k+1} \subseteq (a)$. Vi kan så vælge $b \in \mathfrak{m}^k$ med $b \notin (a)$, og så har vi

$$b \notin (a), \qquad \text{og} \qquad b\mathfrak{m} \subseteq (a). \tag{*}$$

Vi kan betragte brøken b/a i brølegemet. Den sidste inklusion betyder, at $\frac{b}{a}\mathfrak{m} \subseteq R$. Det er klart, at $\frac{b}{a}\mathfrak{m}$ så er et ideal i R. Da R er lokal, er der to muligheder:

$$\tfrac{b}{a}\mathfrak{m} \subseteq \mathfrak{m} \quad \text{eller} \quad \tfrac{b}{a}\mathfrak{m} = R. \tag{†}$$

Vi udelukker den første mulighed med et standard argument:

Antag, at $\frac{b}{a}\mathfrak{m} \subseteq \mathfrak{m}$. Multiplikation med brøken $\alpha = \frac{b}{a}$ er så en R-lineær endomorfi $\mathfrak{m} \to \mathfrak{m}$. Vælges frembringere, $\mathfrak{m} = (p_1, \dots, p_r)$, fås for hver frembringer p_i en fremstilling af αp_i som R-linearkombination af $p_1, \dots, p_r$. Med disse koefficientsæt som søjler fås en matrix $A \in \mathrm{Mat}_n(R)$ og en matrixligning $\alpha(p_1, \dots, p_n) = (p_1, \dots, p_n)A$, eller

$$(p_1, \dots, p_n)(\alpha - A) = (0, \dots, 0).$$

Matricen $\alpha - A$ har koefficienter i brøklegemet. Multipliceres matricen med sin kofaktormatrix fås diagonalmatricen med $\det(\alpha - A)$ i diagonalen. Følgelig annulerer $\det(\alpha - A)$ alle frembringerne p_i. For mindst en frembringer p_i gælder $p_i \neq 0$, og ligningen $p_i \det(\alpha - A) = 0$ (i brøklegemet) medfører så, at $\det(\alpha - A) = 0$. Men $\det(\alpha - A)$ fås ved at indsætte α i det karakteristiske polynomium for A. Det karakteristiske polynomium er normeret. Af ligningen $\det(\alpha - A) = 0$ følger derfor, at α er hel over R. Af forudsætningerne i (iv) følger, at $\alpha \in R$, altså at $b \in (a)$, i modstrid med (*).

Altså gælder den anden mulighed i (†), dvs $\frac{b}{a}\mathfrak{m} = R$. Specielt kan vi så skrive $\frac{b}{a}\, p = 1$ med $p \in \mathfrak{m}$, og nu følger det umiddelbart af $\frac{b}{a}\mathfrak{m} = R$, at $\mathfrak{m} = (p)$. Altså er betingelsen (i) eftervist. $\square$

(4.8) Definition. En noethersk ring R kaldes en *Dedekindring*, hvis R er et integritetsomoråde og hvis der for hvert maksimalideal $\mathfrak{m}$ i R gælder, at den lokale ring $R_{\mathfrak{m}}$ er en valuationsring.

Et hovedidealområde, der ikke er et legeme, er en Dedekindring. I et hovedidealområde, der ikke er et legeme, er maksimalidealerne nemlig hovedidealerne (p) frembragt af de irreducible elementer p, og maksimalidealet i den lokale ring $R_{(p)}$ er derfor et hovedideal, jfr Eksempel (4.6).

(4.9) Sætning. *Lad R være en Dedekindring. Da har hvert ideal $\mathfrak{a} \neq (0)$ en entydig fremstilling,*

$$\mathfrak{a} = \mathfrak{m}_1^{n_1} \cap \cdots \cap \mathfrak{m}_q^{n_q}, \tag{4.9.1}$$

som en fællesmængde af potenser af maksimalidealer.

Bevis. Ifølge Dekompositionssætningen (3.5), jfr Eksempel (3.6)(2), er det nok at vise, at de primære idealer $\mathfrak{q} \neq (0)$ i R netop er potenserne $\mathfrak{m}^n$ af maksimalidealer $\mathfrak{m}$ (og at eksponenten n er entydigt bestemt).

Antag altså, at $\mathfrak{q} \neq (0)$ er et $\mathfrak{p}$-primært ideal. Det følger af Eksistenssætningen, at $\mathfrak{p}$ er indeholdt i et maksimalideal $\mathfrak{m}$. Yderligere er $(0) \subset \mathfrak{q} \subseteq \mathfrak{p}$. Følgelig gælder inklusionerne,

$$(0) \subset \mathfrak{p} \subseteq \mathfrak{m}. \tag{$*$}$$

Det følger af forudsætningen, at den lokale ring $R_\mathfrak{m}$ er en valuationsring. I $R_\mathfrak{m}$ findes derfor netop 2 primidealer, nemlig maksimalidealet og (0). På den anden side svarer de tre primidealer i $(*)$ ifølge Lokaliseringsprincippet bijektivt til tre primidealer i den lokaliserede ring $R_\mathfrak{m}$. Af disse må de to sidste altså være ens. Følgelig er $\mathfrak{p} = \mathfrak{m}$. Hermed er vist, at $\mathfrak{q}$ er $\mathfrak{m}$-primært.

Af entydighedsdelen i Dekompositionssætningen følger nu, at $\mathfrak{q}$ er kernen for den sammensatte homomorfi $R \to R_\mathfrak{m} \to (R/\mathfrak{q})_\mathfrak{m}$. Idealet $\mathfrak{q}$ er med andre ord kontraktionen af ekstensionen $\mathfrak{q}R_\mathfrak{m}$. Ekstensionen er et ideal forskelligt fra nul i valuationsringen $R_\mathfrak{m}$, og det er derfor en potens af maksimalidealet i $R_\mathfrak{m}$. Ekstensionen har derfor formen $\mathfrak{m}^n R_\mathfrak{m}$ med en entydig betemt eksponent n. Det givne ideal $\mathfrak{q}$ er altså kontraktionen af $\mathfrak{m}^n R_\mathfrak{m}$. Med samme argument er denne kontraktion lig med $\mathfrak{m}^n$. Følgelig er $\mathfrak{q} = \mathfrak{m}^n$, som påstået. □

(4.10) Note. Det er en konsekvens af den såkaldte kinesiske restklassesætning, at fællesmængden af potenserne i (4.9.1) er lig med produktet. I den forstand udtrykker resultatet i Sætning (4.9), at Dedekindringe tillader en faktoriseringsteori, der på mange måder er en naturlig generalisation af teorien i hovedidealområder.

Det skal bemærkes, at det her givne resultat kun er et hjørne af teorien for Dedekindringe.

(4.11) Eksempel. Det helt basale eksempel er følgende: Lad K være et algebraisk tallegeme, dvs et dellegeme $K \subseteq \mathbb{C}$ af endelig dimension over $\mathbb{Q}$. Hvert elelement i K er så algebraisk over $\mathbb{Q}$, altså rod i et normeret polynomium med koefficienter i $\mathbb{Q}$, eller, ækvivalent, rod i et polynomium $\neq 0$ med koeffcienter i $\mathbb{Z}$. Lad R være den hele afslutning af $\mathbb{Z}$ i K. Da er R er en Dedekindring.

Denne påstand bevises ved at eftervise: (1) R er en noethersk ring (ikke så svært), og (2) hvert primideal $\mathfrak{p} \neq (0)$ i R er et maksimalideal (det beviser vi senere).

Antag dette er vist, og betragt et maksimalideal $\mathfrak{m}$ i R. Af definitionen på R som den hele afslutning følger let, at R er helt afsluttet i sit brøklegme K, og så gælder det samme for lokaliseringen $R_\mathfrak{m}$. Af (1) følger, at også lokaliseringen $R_\mathfrak{m}$ er noethersk. Primidealerne i $R_\mathfrak{m}$ svarer til primidealer $\mathfrak{p}$ i R med $\mathfrak{p} \subseteq \mathfrak{m}$; af (2) følger, at der er præcis 2. Altså er betingelsen (iv) i Sætning (4.7) opfyldt for $R_\mathfrak{m}$.

5. Artin–Rees' sætninger.

(5.1) Definition. Lad $\mathfrak{a}$ være et fast ideal i R. Det er klart, at polynomierne i $R[T]$ af formen,

$$a_0 + a_1T + \cdots + a_nT^n, \text{ hvor } a_i \in \mathfrak{a}^i \text{ for alle } i,$$

udgør en delring. Denne delring kaldes *Rees-ringen* for idealet $\mathfrak{a}$, og den betegnes i det følgende $\tilde{R}$. Idet monomierne af formen aT^i, hvor $a \in \mathfrak{a}^i$, udgør undergruppen $\mathfrak{a}^iT^i$ af $R[T]$, er altså

$$\tilde{R} = R \oplus \mathfrak{a}T \oplus \mathfrak{a}^2T^2 \oplus \cdots .$$

Rees-ringen $\tilde{R}$ er øjensynlig en positivt gradueret ring med $(\tilde{R})_0 = R$.

Lad M være en R-modul. Det er klart hvorledes den direkte sum,

$$M^* := M \oplus M \oplus M \oplus \cdots ,$$

kan organiseres som en gradueret modul over polynomiumsringen $R[T]$. Multiplikation med T i M^* forskyder blot graden: elementet $x \in M$ opfattet som homogent element af grad i i M^* afbildes på sig selv opfattet som homogent element af grad $i+1$ i M^*.

Den graduerede modul M^* kan specielt opfattes som en gradueret modul over delringen $\tilde{R}$. Videre er det klart, at følgende undergruppe i M^*:

$$\tilde{M} := M \oplus \mathfrak{a}M \oplus \mathfrak{a}^2M \oplus \cdots$$

er en homogen $\tilde{R}$-modul. Den kaldes også *Rees-modulen* for M (mht det faste ideal $\mathfrak{a}$ i R).

(5.2) Lemma. *Hvis idealet $\mathfrak{a}$ er frembragt af endelig mange elementer $a_1, \dots, a_d$, så er Rees-ringen $\tilde{R}$ frembragt som R-algebra af elementerne $a_1T, \dots, a_dT$ (der er homogene af grad 1 i $\tilde{R}$). Hvis R-modulen M er frembragt af elementer $v_1, \dots, v_n$, så er Rees-modulen $\tilde{M}$ frembragt som $\tilde{R}$-modul af $v_1, \dots, v_n$ opfattet som homogene elementer af grad 0 i $\tilde{M}$.*

Bevis. Begge påstande eftervises umiddelbart. □

(5.3) Observation. Den første påstand udsiger, at algebra-homomorfien

$$R[T_1, \dots, T_d] \to \tilde{R},$$

defineret ved $f \mapsto f(a_1T, \dots, a_dT)$, er surjektiv. Denne homomorfi er øjensynlig en homogen homomorfi af graduerede ringe, og resultatet medfører derfor at Rees-ringen R er isomorf med en kvotient af polynomiumsringen $R[T_1, \dots, T_d]$ modulo et homogent ideal.

(5.4) Bemærkning. Ingen af de foregående definitioner og resultater har udnyttet den stiltiende forudsætning, at R er en noethersk ring. Indrages denne forudsætning, følger det af Hilbert's Basissætning og det første resultat i Lemma (5.2), at Rees-ringen $\tilde{R}$ er en noethersk ring, og af det andet resultat, at Rees-modulen for en endeligt frembragt R-modul er en noethersk $\tilde{R}$-modul.

(5.5) Artin–Rees' Lemma. *Lad $\mathfrak{a}$ være et ideal i R og lad M være en endeligt frembragt R-modul. Lad videre N være en undermodul i M. Da findes et naturligt tal d, således at*

$$\mathfrak{a}^n M \cap N = \mathfrak{a}^{n-d}\bigl(\mathfrak{a}^d M \cap N\bigr) \text{ for alle } n \geqslant d.$$

Specielt er $\mathfrak{a}^n M \cap N \subseteq \mathfrak{a}^{n-d} N$ for alle $n \geqslant d$.

Bevis. Ifølge definitionen er Rees-modulen $\tilde{M}$ en homogen undermodul i $\tilde{R}$-modulen M^*. Det er klart, at også N^* er en homogen undermodul i M^*. Fællesmængden af disse to undermoduler er øjensynlig den homogene undermodul,

$$\mathcal{N} = \mathcal{N}_0 \oplus \mathcal{N}_1 \oplus \mathcal{N}_2 \oplus \cdots, \text{ hvor } \mathcal{N}_n := \mathfrak{a}^n M \cap N.$$

Af Lemma (5.2), jfr Bemærkning (5.4), følger, at $\tilde{M}$ er en noethersk $\tilde{R}$-modul. Da $\mathcal{N}$ er en undermodul i $\tilde{M}$, følger det, at $\mathcal{N}$ er en endeligt frembragt $\tilde{R}$-modul. Heraf følger, at $\mathcal{N}$ er frembragt som $\tilde{R}$-modul af endelig mange homogene elementer. Videre er $\tilde{R}$ ifølge Lemma (5.2) frembragt som R-algebra af homogene elementer af grad 1. Vælges d større end eller lig med graderne af de homogene elementer, der frembringer $\mathcal{N}$, kan man derfor slutte, at den homogene undermodul $\mathcal{N}_{\geqslant d}$ er frembragt som $\tilde{R}$-modul af elementerne i $\mathcal{N}_d$. Med andre ord: hvert homogent element i $\mathcal{N}_n$ for $n \geqslant d$ er en sum af produkter he, hvor $h \in \tilde{R}_{n-d}$ og $e \in \mathcal{N}_d$. Da $\mathcal{N}_n = \mathfrak{a}^n M \cap N$, gælder altså for $n \geqslant d$ ligningen,

$$\mathfrak{a}^n M \cap N = \mathfrak{a}^{n-d}(\mathfrak{a}^d M \cap N).$$

Hermed er Lemma'ets første påstand bevist. Den anden påstand er øjensynlig en konsekvens af den første. □

(5.6) Krull's Snitsætning. *Antag, at R er lokal med maksimalideal $\mathfrak{m}$. Da gælder for enhver endeligt frembragt R-modul M, at*

$$\bigcap_n \mathfrak{m}^n M = 0.$$

Bevis. Lad N betegne fællesmængden ovenfor. Ifølge Artin–Rees' Lemma findes et naturligt tal d således at inklusionen,

$$\mathfrak{m}^n M \cap N \subseteq \mathfrak{m}^{n-d} N,$$

er opfyldt for $n \geqslant d$. Undermodulerne $\mathfrak{m}^n M$ er en dalende følge af undermoduler i M, med fællesmængde N. Fællesmængden, for $n > d$, af modulerne på venstresiden af inklusionen, er derfor er lig med N. Højresiden af inklusionen, for $n > d$, er øjensynlig indeholdt i $\mathfrak{m}N$. Det følger derfor, at $N \subseteq \mathfrak{m}N$. Altså er $N = \mathfrak{m}N$. Af Nakayama's Lemma følger derfor, at $N = 0$. □

Dimensionsteori

1. Krull-dimension.

(1.1) Bemærkning. Dimensionen, $\dim P$, af en partielt ordnet mængde $(P, <)$ kan defineres som det største antal skarpe ulighedstegn i en kæde $p_0 < p_1 < \cdots < p_h$ af elementer fra P. Hvis der ikke findes en øvre grænse for antallet af ulighedstegn, sættes $\dim P := \infty$. Det er en konvention, at den tomme mængde tillægges dimensionen $-\infty$, og den medregnes blandt de partielt ordnede mængder af endelig dimension (dvs af dimension mindre end ∞). Med denne konvention betyder $\dim P = 0$, at P ikke er tom og at to forskellige elementer i P ikke kan sammenlignes.

For eksempel kan længden af en R-modul M defineres som dimensionen af den partielt ordnede mængde af undermoduler i M.

(1.2) Definition. Ved *Krull-dimensionen*, i det følgende blot kaldet *dimensionen*, af en R-modul M forstås dimensionen,

$$\dim M := \dim \operatorname{Supp} M,$$

hvor støtten $\operatorname{Supp} M$, bestående af primidealer $\mathfrak{p}$ i R således at $M_{\mathfrak{p}} \neq 0$, er partielt ordnet ved sædvanlig inklusion. Dimensionen er med andre ord det største antal skarpe inklusionstegn i en kæde af primidealer i støtten for M:

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_h. \tag{1.2.1}$$

Et primideal $\mathfrak{p}$ tilhører som bekendt støtten $\operatorname{Supp} M$, hvis og kun hvis der findes et element x i M, således at $\mathfrak{p} \supseteq \operatorname{Ann}(x)$. Specielt gælder, når $\mathfrak{p}$ tilhører støtten for M og $\mathfrak{q}$ er et primideal der omfatter $\mathfrak{p}$, at også $\mathfrak{q}$ tilhører støtten for M. Det er således i (1.2.1) nok at kræve, at $\mathfrak{p}_0 \in \operatorname{Supp} M$.

For nul-modulen er støtten tom, så nul-modulen har ifølge konventionen fra (1.1) dimensionen $-\infty$. En modul $M \neq 0$ har som bekendt en ikke-tom støtte, og dermed er $\dim M \geqslant 0$. Ligningen $\dim M = 0$ udtrykker øjensynlig, at $M \neq 0$ og at ethvert primideal i støtten for M er et maksimalideal.

Dimensionen af R som R-modul kaldes også *Krull-dimensionen* af ringen R.

(1.3) Bemærkning. Lad $\mathfrak{a}$ være et ideal i R. Kvotienten $R/\mathfrak{a}$ kan da opfattes som en ring og som en R-modul. Mere generelt kan en kvotient $M/\mathfrak{a}M$ opfattes både som modul over R og som modul over $R/\mathfrak{a}$. Dimensionen af $M/\mathfrak{a}M$ er uafhængig heraf. Det er nemlig klart, at hvert primideal i støtten for R-modulen $M/\mathfrak{a}M$ vil omfatte $\mathfrak{a}$. Primidealer $\mathfrak{p}$, der omfatter $\mathfrak{a}$, svarer ifølge Kvotientprincippet til samtlige primidealer i $R/\mathfrak{a}$, og der findes en isomorfi $(M/\mathfrak{a}M)_\mathfrak{p} \simeq (M/\mathfrak{a}M)_{\mathfrak{p}/\mathfrak{a}}$. Heraf ses, at når $\mathfrak{p} \supseteq \mathfrak{a}$, så vil $\mathfrak{p}$ tilhøre støtten for R-modulen $M/\mathfrak{a}M$, hvis og kun hvis primidealet $\mathfrak{p}/\mathfrak{a}$ tilhører støtten for $R/\mathfrak{a}$-modulen $M/\mathfrak{a}M$. Kæder af primidealer (1.2.1) i støtten for R-modulen $M/\mathfrak{a}M$ svarer altså bijektivt til kæder af primidealer i støtten for $R/\mathfrak{a}$-modulen $M/\mathfrak{a}M$. Heraf følger, at de to dimensioner er den samme.

Et tilsvarende resultat om dimension af brøkmoduler gælder ikke. Hvis S er en multiplikativ delmængde af R, så er brøkmodulen $S^{-1}M$ en modul over brøkringen $S^{-1}R$, og $S^{-1}M$ kan derfor specielt opfattes som R-modul. Primidealerne i brøkringen $S^{-1}R$ svarer ifølge Lokaliseringsprincippet bijektivt til primidealer $\mathfrak{p}$ der er disjunkte med S, og der findes en isomorfi $(S^{-1}M)_{S^{-1}\mathfrak{p}} = M_\mathfrak{p}$. Støtten for $S^{-1}R$-modulen $S^{-1}M$ kan derfor identificeres med den delmængde af støtten for R-modulen M, der består af primidealer disjunkte med S, og dimensionen af $S^{-1}R$-modulen $S^{-1}M$ er altså dimensionen af denne delmængde. Men det skal understreges, at det også for primidealer $\mathfrak{p}$, der ikke er disjunkte med S, kan indtræffe, at $(S^{-1}M)_\mathfrak{p} \neq 0$, altså at $\mathfrak{p}$ tilhører støtten for R-modulen $S^{-1}M$; dimensionen af $S^{-1}M$ som R-modul kan altså være større end dimensionen som $S^{-1}R$-modul. Med mindre andet udtrykkeligt er fremhævet, vil $\dim S^{-1}M$ altid betegne dimensionen af $S^{-1}M$ som modul over brøkringen $S^{-1}R$.

(1.4) Observation. For enhver R-modul M gælder uligheden $\dim M \leqslant \dim R$, idet støtten for M er en delmængde af mængden af primidealer i R. Tilsvarende gælder for en undermodul M' i M og kvotienten $M'' = M/M'$, at $\dim M' \leqslant \dim M$ og $\dim M'' \leqslant \dim M$, idet både M' og M'' har støtte indeholdt i støtten for M. Yderligere gælder ligningerne,

$$\dim M = \sup_{\mathfrak{p} \in \operatorname{Supp} M} \dim R/\mathfrak{p} = \sup_{\mathfrak{p}} \dim M_\mathfrak{p},$$

hvor det sidste supremum fx tages over alle primidealer (eller maksimalidealer) (i $\operatorname{Supp} M$). Den første lighed indses således: Dimensionen af M er supremum af de tal h, for hvilke der findes en kæde (1.2.1) med $\mathfrak{p}_0 \in \operatorname{Supp} M$, eller omskrevet, supremum over $\mathfrak{p} \in \operatorname{Supp} M$ af supremum af de tal h for hvilke der findes en kæde (1.2.1) med $\mathfrak{p}_0 = \mathfrak{p}$. Når $\mathfrak{p}$ er givet, så svarer kæder (1.2.1) med $\mathfrak{p}_0 = \mathfrak{p}$ ifølge Kvotientprincippet bijektivt til kæder af primidealer i kvotienten $R/\mathfrak{p}$. Heraf følger den påståede lighed.

At dimensionen af M også er bestemt ved det andet supremum indses tilsvarende: Da hvert primideal er indeholdt i et maksimalideal, er det klart, at vi i definitionen på $\dim M$ kun behøver at betragte kæder (1.2.1), hvor $\mathfrak{p}_i$ tilhører støtten for M og $\mathfrak{p}_h = \mathfrak{m}$ er et maksimalideal. Videre er det klart, at vi i supremum kun behøver at medregne bidrag svarende til primidealer $\mathfrak{p}$ med $M_\mathfrak{p} \neq 0$, idet de øvrige primidealer $\mathfrak{p}$ kun bidrager med $\dim M_\mathfrak{p} = -\infty$ til supremum. Det følger af definitionen, at dimensionen af M er supremum over primidealer $\mathfrak{p}$ i $\operatorname{Supp} M$ af supremum af de tal h, for hvilke der findes en kæde (1.2.1) af primidealer i $\operatorname{Supp} M$ med $\mathfrak{p}_h = \mathfrak{p}$. Når $\mathfrak{p}$ er givet, så svarer sådanne kæder ifølge Lokaliseringsprincippet bijektivt til kæder af primidealer i støtten for $M_\mathfrak{p}$ (som modul over den lokale ring $R_\mathfrak{p}$), som ender med maksimalidealet $\mathfrak{p}R_\mathfrak{p}$. Heraf følger den anden lighed.

For $M = R$ udsiger de to ligheder, at

$$\dim R = \sup \dim R/\mathfrak{p} = \sup \dim R_{\mathfrak{p}}.$$

Lad M være en endeligt frembragt R-modul. Da består støtten for M som bekendt af de primidealer, der omfatter annullatoren $\operatorname{Ann} M$. I kæden (1.2.1) ligger primidealerne $\mathfrak{p}_i$ altså i støtten for M, netop hvis alle $\mathfrak{p}_i$'erne omfatter $\operatorname{Ann} M$. Sådanne kæder svarer altså bijektivt til kæder af primidealer i kvotientringen $R/\operatorname{Ann} M$, og følgelig gælder ligningen,

$$\dim M = \dim(R/\operatorname{Ann} M).$$

(1.5) Bemærkning. Dimensionen af en R-modul kan være ∞. Den er naturligvis ∞, hvis der i støtten for M findes en uendelig kæde $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots$, eller en uendelig kæde $\mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \cdots$. Sådanne kæder findes ikke hvis ringen R er noethersk (det er klart, at der i en noethersk ring ikke findes uendelige kæder af den første type, og det vil fremgå af senere resultater, at der heller ikke findes uendelige kæder af den anden type). Men også for noetherske ringe kan dimensionen være ∞, idet $\dim M = \infty$ kun betyder, at der findes vilkårligt lange kæder (1.2.1).

Antag, at dimensionen $\dim M$ er endelig. Da findes i støtten for M en kæde (1.2.1), hvor $h = \dim M$ er det maksimale antal skarpe inklusioner. Det er klart, at en sådan kæde er *maksimal* i den forstand, at $\mathfrak{p}_0$ er et minimalt primideal for M, $\mathfrak{p}_h$ er et maksimalideal i R, og kæden (1.2.1) er uforfinelig: mellem to på hinanden følgende $\mathfrak{p}_i$'er findes ingen primidealer. Det skal understreges, at der ikke gælder omvendt, at hvis en kæde (1.2.1) er maksimal i denne forstand, så er $h = \dim M$. Der findes et eksempel på en ring R, der er et noethersk, lokalt integritetsområde med to uforfinelige kæder af primidealer,

$$(0) \subset \mathfrak{p} \subset \mathfrak{m}, \qquad (0) \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \mathfrak{m}.$$

(1.6) Eksempel. Nul-ringen har dimension $-\infty$. Et legeme k har øjensynlig dimension 0. Ringen $\mathbb{Z}$ har dimension 1, idet $(0) \subset (p)$, hvor p er et primtal, er den maksimalt opnåelige kæde af primidealer i $\mathbb{Z}$. Mere generelt gælder, at et hovedidealområde, der ikke er et legeme, er af dimension 1.

I polynomiumsringen $R = k[X_1, \ldots, X_n]$ over et legeme k er kæden,

$$(0) \subset (X_1) \subset (X_1, X_2) \subset \cdots \subset (X_1, \ldots, X_n),$$

en kæde af primidealer i R. Heraf følger, at $\dim R \geqslant n$. På den anden side er det velkendt, at man ved at inddrage transcendensgrad kan vise, at ingen kæde af primidealer i R kan indeholde flere end n skarpe inklusioner. Der gælder altså ligheden $\dim R = n$.

(1.7) Definition. For et primideal $\mathfrak{p}$ i R defineres *højden* af $\mathfrak{p}$ som det største antal skarpe inklusioner i en kæde af primidealer,

$$\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_h = \mathfrak{p}. \tag{1.7.1}$$

Højden af $\mathfrak{p}$ betegnes $\operatorname{ht}\mathfrak{p}$. Højden af et primideal kan være ∞, men den er altid ikke-negativ. At $\operatorname{ht}\mathfrak{p} = 0$ betyder, at $\mathfrak{p}$ er et minimalt primideal i R. Primidealer $\mathfrak{q} \subseteq \mathfrak{p}$ svarer som bekendt bijektivt til samtlige primidealer i brøkringen $R_\mathfrak{p}$. Kæder (1.7.1) svarer derfor bijektivt til kæder af primidealer i $R_\mathfrak{p}$. Følgelig er $\operatorname{ht}\mathfrak{p} = \dim R_\mathfrak{p}$.

Det er praktisk at definere højden af et vilkårligt ideal $\mathfrak{a}$ som infimum af højderne af de primidealer, der omfatter $\mathfrak{a}$, altså

$$\operatorname{ht}\mathfrak{a} = \inf_{\mathfrak{p}\supseteq\mathfrak{a}} \operatorname{ht}\mathfrak{p} = \inf_{\mathfrak{p}\supseteq\mathfrak{a}} \dim R_\mathfrak{p}.$$

For det uægte ideal $\mathfrak{a} = R$ tages infimum over den tomme mængde, og idealet R tillægges højden ∞. Hvis $\mathfrak{a}$ er et ægte ideal, findes der altid primidealer (endda maksimalidealer), der omfatter $\mathfrak{a}$, så infimum tages over en ikke-tom mængde. Men også her kan højden være ∞, nemlig når alle primidealer, der omfatter $\mathfrak{a}$, har uendelig højde. Vi skal senere vise, at for noetherske ringe er højden af ægte idealer altid endelig.

(1.8) Observation. For et ægte ideal $\mathfrak{a}$ i R gælder uligheden,

$$\operatorname{ht}\mathfrak{a} + \dim R/\mathfrak{a} \leqslant \dim R.$$

Uligheden gælder trivielt, hvis højresiden er ∞. Antag, at $\dim R < \infty$. Dimensionen af $R/\mathfrak{a}$ bestemmes ved at betragte kæder af primidealer,

$$\mathfrak{a} \subseteq \mathfrak{p}'_0 \subset \cdots \subset \mathfrak{p}'_k. \tag{1.8.1}$$

Da $\dim R < \infty$, er $\dim R/\mathfrak{a} < \infty$, så vi kan finde en kæde af primidealer (1.8.1), hvor $k = \dim R/\mathfrak{a}$. Da $\dim R < \infty$ er $\operatorname{ht}\mathfrak{p}'_0 < \infty$, så vi kan finde en kæde af primidealer (1.7.1) med $\mathfrak{p} = \mathfrak{p}'_0$, hvor $h = \operatorname{ht}\mathfrak{p}'_0$. Da højden af $\mathfrak{a}$ er et infimum, er $\operatorname{ht}\mathfrak{a} \leqslant h$. Kombineres de to kæder (1.7.1) og (1.8.1) fås i R en kæde af primidealer med $h + k$ skarpe inklusioner. Altså har vi $\operatorname{ht}\mathfrak{a} + \dim R/\mathfrak{a} \leqslant h + k \leqslant \dim R$, og dermed den søgte ulighed.

(1.9) Definition. Det er ofte bekvemt at generalisere definitionerne i (1.7) til moduler. For en R-modul M og et ideal $\mathfrak{a}$ defineres *codimensionen*, $\operatorname{codim} M$, og *M-højden*, $\operatorname{ht}_M \mathfrak{a}$, ved ligningerne,

$$\operatorname{codim} M := \inf_{\mathfrak{p}\in\operatorname{Supp} M} \dim R_\mathfrak{p} \qquad \text{og} \qquad \operatorname{ht}_M \mathfrak{a} := \inf_{\mathfrak{p}\in\operatorname{Supp} M,\ \mathfrak{p}\supseteq\mathfrak{a}} \dim M_\mathfrak{p}.$$

Hvis M er endeligt frembragt, følger det af Nakayama's Lemma, at det sidste infimum ækvivalent kan tages over primidealer i støtten for $M/\mathfrak{a}M$. For et primideal $\mathfrak{p}$ følger det let af definitionen, at $\operatorname{ht}_M \mathfrak{p} = \dim M_\mathfrak{p}$.

Det er let at se, at $\operatorname{codim} R/\mathfrak{a} = \operatorname{ht}\mathfrak{a}$. Følgende to uligheder:

$$\operatorname{codim} M + \dim M \leqslant \dim R, \quad \text{når } M \neq 0,$$
$$\operatorname{ht}_M \mathfrak{a} + \dim M/\mathfrak{a}M \leqslant \dim M, \quad \text{når } \mathfrak{a}M \subset M,$$

generaliserer begge uligheden i (1.8), og de vises ved et tilsvarende bevis.

(1.10) Definition. Lad M være en R-modul af endelig dimension, og antag $M \neq 0$. Som nævnt i (1.4) er $\dim M = \sup \dim R/\mathfrak{p}$, hvor supremum tages over primidealer i støtten for M. Da dimensionen er endelig, er supremum et maksimum, og det er klart, at den maksimale værdi $\dim R/\mathfrak{p}$ antages i et minimalt primideal $\mathfrak{p}$ for M, dvs i et primideal $\mathfrak{p}$, der er minimalt i støtten for M. Hvis der for alle minimale primidealer $\mathfrak{q}$ for M gælder, at $\dim R/\mathfrak{q} = \dim M$, siges M at være *equidimensional*. Bemærk, at en modul med kun ét minimalt primideal, specielt et integritetsområde opfattet som modul over sig selv, er equidimensional.

Tilsvarende er $\dim M = \sup \dim M_\mathfrak{p}$, og den maksimale værdi $\dim M_\mathfrak{p}$ antages i et maksimalideal i støtten for M. Hvis der for alle maksimalidealer $\mathfrak{m}$ i støtten for M gælder, at $\dim M_\mathfrak{m} = \dim M$, siges M at være *co-equidimensional*. Bemærk, at en modul over en lokal ring er co-equidimensional.

Lad $\mathfrak{q} \subseteq \mathfrak{p}$ være primidealer i støtten for M. Da dimensionen af M er endelig, findes der uforfinelige kæder,

$$\mathfrak{q} = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_h = \mathfrak{p}, \tag{*}$$

og endda sådanne kæder hvor $h = \operatorname{ht} \mathfrak{p}/\mathfrak{q}$. Hvis der for enhver sådan uforfinelig kæde gælder at $h = \operatorname{ht} \mathfrak{p}_h/\mathfrak{p}_0$, siges M at være *katernær*. Hvis der for alle maksimale kæder (*) i støtten for M, dvs kæder som er uforfinelige og således at $\mathfrak{p}_0$ er et minimalt primideal for M og $\mathfrak{p}_h$ er et maksimalideal i R, gælder at $h = \dim M$, siges M at være *bi-equidimensional*. Det er klart, at en bi-equidimensional modul er equidimensional, co-equidimensional og katernær.

Specielt siges *ringen* R at være *equidimensional*, *co-equidimensional*, ... , når R som modul over sig selv er equidimensional, co-equidimensional, ...

(1.11) Definition. En (endelig eller uendelig) følge $(f_1, f_2, \dots)$ af elementer i ringen R kaldes en *M-højdefølge*, hvis følgende betingelse er opfyldt for alle i:

($*$) For hvert primideal $\mathfrak{p}$, som tilhører støtten for M og omfatter $(f_1, \dots, f_i)$ gælder, at $\dim M_\mathfrak{p} \geqslant i$.

Betingelsen kan også udtrykkes ved ulighederne $\operatorname{ht}_M(f_1, \dots, f_i) \geqslant i$ for $i = 1, 2, \dots$. For $M = R$ er betingelsen, at der for alle primidealer $\mathfrak{p}$ som omfatter $(f_1, \dots, f_i)$ gælder, at $\operatorname{ht} \mathfrak{p} \geqslant i$. Er dette opfyldt, kaldes følgen blot en *højdefølge*.

(1.12) Sætning. *Antag, at R indeholder et legeme k og at R er af endelig transcendensgrad over k. Da gælder uligheden,*

$$\dim R \leqslant \operatorname{tdeg}_k R.$$

Bevis. Transcendesgraden er som bekendt det største antal algebraisk uafhængige (over k) elementer, der kan udtages fra R. Øjensynlig gælder for en kvotient $\overline{R} = R/\mathfrak{a}$, at $\operatorname{tdeg}_k \overline{R} \leqslant \operatorname{tdeg}_k R$. Yderligere er det velkendt, at hvis R er et integritetsområde og $\mathfrak{a} = \mathfrak{p}$ er et primideal forskelligt fra (0), så gælder endda $\operatorname{tdeg}_k \overline{R} < \operatorname{tdeg}_k R$. Af disse overvejelser følger let for enhver kæde (1.2.1), at $\operatorname{tdeg}_k R/\mathfrak{p}_h + h \leqslant \operatorname{tdeg}_k R/\mathfrak{p}_0 \leqslant \operatorname{tdeg}_k R$, hvoraf påstanden. $\square$

2. Dimension af lokale ringe.

(2.1) Setup. I resten af dette kapitel betragtes en noethersk ring R, et ideal $\mathfrak{a}$ i R, og en endeligt frembragt R-modul M. I visse af resultaterne forudsættes, at ringen R er lokal; i disse resultater betegner $\mathfrak{m}$ maksimalidealet i R.

(2.2) Lemma. *Antag, at R er lokal. Da har M endelig længde, hvis og kun hvis der findes et naturligt tal n således, at $\mathfrak{m}^n M = (0)$.*

Bevis. Det er let at se, at påstanden er et korollar til Filtrationssætningen. Her er et mere direkte bevis: Antag først, at $\mathfrak{m}^n M = (0)$. Da defineres ved $F_i := \mathfrak{m}^i M$ en filtration i M,

$$(0) = F_n \subseteq \cdots \subseteq F_1 \subseteq F_0 = M. \tag{2.2.1}$$

Øjensynlig er $F_{i+1} = \mathfrak{m}F_i$, så de successive kvotienter er $F_i/\mathfrak{m}F_i$ for $i = 0, \dots, n-1$. Undermodulen F_i i M er endeligt frembragt over R, og kvotienten $F_i/\mathfrak{m}F_i$ er derfor endeligt frembragt som modul over restklasselegemet $R/\mathfrak{m}$. De successive kvotienter er altså vektorrum af endelig dimension over $R/\mathfrak{m}$, og de har derfor endelig længde som R-moduler. Følgelig har også M endelig længde.

Antag omvendt, at M har endelig længde. Da har M en filtration (2.2.1), hvor de successive kvotienter F_i/F_{i+1} er isomorfe med $R/\mathfrak{m}$. Modulen $R/\mathfrak{m}$ annulleres af $\mathfrak{m}$, og følgelig gælder for hvert i, at $\mathfrak{m}F_i \subseteq F_{i+1}$. Ved gentagen anvendelse heraf fås, at $\mathfrak{m}^n M = \mathfrak{m}^n F_0 \subseteq F_n = (0)$. $\square$

(2.3) Hovedsætning. *Antag, at R er lokal og $M \neq 0$. Betragt følgende tre tal:*

$\dim(M)$ *er Krull-dimensionen,*
$d_\mathfrak{m}(M)$ *er graden af den polynomiale funktion $n \mapsto \operatorname{long} M/\mathfrak{m}^n M$,*
$s(M)$ *er det mindste antal s af elementer $f_1, \dots, f_s$ i maksimalidealet $\mathfrak{m}$ således, at kvotientmodulen $M/(f_1, \dots, f_s)M$ har endelig længde.*

Da gælder, at $\dim(M) = d_\mathfrak{m}(M) = s(M)$. Specielt er Krull-dimensionen $\dim(M)$ endelig.

Bevis. Det er antaget, at $M \neq 0$, så støtten for M er ikke tom; derfor er $\dim(M) \geqslant 0$. Af Nakayma's Lemma følger, at $\operatorname{long} M/\mathfrak{m}^n M > 0$, når $n \geqslant 1$. Polynomiet svarende til $n \mapsto \operatorname{long} M/\mathfrak{m}^n M$ er altså ikke nul-polynomiet, og derfor er $d_\mathfrak{m}(M) \geqslant 0$. Endelig skal det bemærkes, at tallet $s(M)$ er veldefineret, idet der findes endelig mange elementer $f_1, \dots, f_s$ i $\mathfrak{m}$ således, at $M/(f_1, \dots, f_s)M$ har endelig længde. Fx er dette opfyldt, hvis $(f_1, \dots, f_s)$ er et frembringersystem for maksimalidealet $\mathfrak{m}$, idet $M/(f_1, \dots, f_s)M$ så er en endelig frembragt modul over restklasselegemet $R/\mathfrak{m}$, og dermed af endelig længde. For $s = 0$ består undermodulen $(f_1, \dots, f_s)M$ blot af nul-elementet i M og kvotienten $M/(f_1, \dots, f_s)M$ er altså M. Betingelsen $s(M) = 0$ udtrykker altså, at M har endelig længde.

Vi viser først, at hver af betingelserne, $\dim(M) = 0$, $d_\mathfrak{m}(M) = 0$, og $s(M) = 0$, er ækvivalente med, at M har endelig længde. Som nævnt ovenfor følger denne påstand for $s(M)$ af definitionen. Tallet $\dim(M)$ er dimensionen af M. Betingelsen $\dim(M) = 0$ betyder således, at alle primidealer i støtten for M er maksimalidealer, og dette gælder som bekendt netop, hvis M har endelig længde. For $d_\mathfrak{m}(M)$ indses påstanden således: betingelsen $d_\mathfrak{m}(M) = 0$ betyder, at funktionen long $M/\mathfrak{m}^n M$ er konstant når $n \gg 0$. Da denne funktion er voksende, er dette opfyldt hvis og kun hvis der findes et naturligt tal n således, at $\mathfrak{m}^n M = \mathfrak{m}^{n+1} M$. Ifølge Nakayama's Lemma er $\mathfrak{m}^n M = \mathfrak{m}^{n+1} M$, hvis og kun hvis $\mathfrak{m}^n M = (0)$. Lemma (2.2) viser, at dette indtræffer netop, når M har endelig længde.

Af det viste følger, at ligningerne $\dim(M) = d_\mathfrak{m}(M) = s(M)$ gælder, hvis et af de tre tal er 0. Vi efterviser ligningerne i almindelighed ved at bevise hver af ulighederne $\dim(M) \leqslant d_\mathfrak{m}(M)$, $d_\mathfrak{m}(M) \leqslant s(M)$, og $s(M) \leqslant \dim(M)$.

Uligheden $\dim(M) \leqslant d_\mathfrak{m}(M)$: Krull-dimensionen $\dim(M)$ er et supremum, så uligheden er ækvivalent med følgende påstand: For enhver endeligt frembragt R-modul M og enhver kæde af primidealer,

$$\operatorname{Ann} M \subseteq \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_h,$$

er $h \leqslant d_\mathfrak{m}(M)$. Denne påstand vises ved fuldstændig induktion efter $d := d_\mathfrak{m}(M)$. Hvis $d = 0$ gælder endda $\dim(M) = d_\mathfrak{m}(M)$ ifølge det allerede viste. Vi kan derfor antage, at $d \geqslant 1$. I kæden kan vi øjensynlig antage, at $\mathfrak{p}_0$ er et minimalt primideal for M. Heraf følger, at $\mathfrak{p}_0$ er et associeret primideal for M, og M indeholder derfor en undermodul N, der er isomorf med $R/\mathfrak{p}_0$. Det er nok at vise, at $h \leqslant d_\mathfrak{m}(N)$, thi da N er en undermodul i M følger det af et velkendt resultat om Samuel-polynomier, at $d_\mathfrak{m}(N) \leqslant d_\mathfrak{m}(M)$. Vi kan derfor erstatte M med N, dvs vi kan antage, at M er isomorf med $R/\mathfrak{p}_0$. Uligheden $h \leqslant d_\mathfrak{m}(M)$ er opfyldt, hvis $h = 0$, så vi kan antage, at $h \geqslant 1$. Vælg nu et element f i overskudsmængden $\mathfrak{p}_1 \backslash \mathfrak{p}_0$, og betragt kvotientmodulen M/fM. Da $M = R/\mathfrak{p}_0$ og f ikke tilhører $\mathfrak{p}_0$, er multiplikation med f injektiv på M. Af et velkendt resultat om Samuel-polynomier følger derfor, at $d_\mathfrak{m}(M/fM) < d_\mathfrak{m}(M)$. Den anførte påstand gælder derfor for modulen M/fM.

Nu var $M = R/\mathfrak{p}_0$, så $M/fM = R/(\mathfrak{p}_0 + (f))$. Specielt er $\operatorname{Ann} M/fM = \mathfrak{p}_0 + (f)$. Da f var valgt i $\mathfrak{p}_1$, udgør $\mathfrak{p}_i$'erne for $i > 0$ en kæde af primidealer, som omfatter $\operatorname{Ann} M/fM$. Der er $h - 1$ skarpe inklusioner i denne kæde, så da påstanden gælder for M/fM sluttes, at $h - 1 \leqslant d_\mathfrak{m}(M/fM)$. Da $d_\mathfrak{m}(M/fM) < d_\mathfrak{m}(M)$ følger det, at $h \leqslant d_\mathfrak{m}(M)$, hvilket var påstanden for M.

Uligheden $d_\mathfrak{m}(M) \leqslant s(M)$: Tallet $s(M)$ er et infimum, så uligheden udsiger, at der for vilkårlige s elementer $f_1, \dots, f_s$ i $\mathfrak{m}$ således at $M/(f_1, \dots, f_s)M$ har endelig længde gælder, at $d_\mathfrak{m}(M) \leqslant s$. Lad $\mathfrak{a} = (f_1, \dots, f_s)$ være idealet frembragt af $f_1, \dots, f_s$. Da er $\mathfrak{a} \subseteq \mathfrak{m}$. Følgelig er long $M/\mathfrak{a}^n M \geqslant$ long $M/\mathfrak{m}^n$ for alle n. Funktionen long $M/\mathfrak{a}^n M$ er ifølge et resultat om Samuel-polynomier polynomial af grad $\leqslant s$. Graden $d_\mathfrak{m}(M)$ af den mindre funktion long $M/\mathfrak{m}^n M$ er derfor højst lig med s, som påstået.

Uligheden $s(M) \leqslant \dim(M)$: Denne ulighed vises ved fuldstændig induktion efter $h := \dim(M)$ (som er endelig ifølge det allerede viste). Betragt kæder af primidealer med h inklusioner,

$$\operatorname{Ann} M \subseteq \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_h.$$

Disse kæder er maksimale i den forstand, at $h = \dim M$. Vi kan antage, at $h \geqslant 1$, idet den påståede ulighed er vist at være en lighed, hvis $h = 0$. I sådanne maksimale kæder må $\mathfrak{p}_0$ nødvendigvis være et minimalt primideal for M. Specielt er der kun endelig mange primidealer, der kan forekomme som $\mathfrak{p}_0$ i en sådan kæde. Da $h \geqslant 1$ kan intet af disse mulige $\mathfrak{p}_0$ være lig med $\mathfrak{m}$. Det er et velkendt resultat om primidealer, at foreningsmængden af de mulige $\mathfrak{p}_0$ så heller ikke kan være lig med $\mathfrak{m}$. Altså findes et element f i $\mathfrak{m}$ således, at f ikke tilhører de mulige $\mathfrak{p}_0$'er. Betragt nu kvotienten M/fM. Dimensionen af kvotienten er mindre end eller lig med dimensionen af modulen, fordi støtten for kvotienten er en delmængde af støtten for modulen. Valget af f sikrer ydermere, at intet af de mulige $\mathfrak{p}_0$'er kan tilhøre støtten for M/fM. Altså er $\dim(M/fM) < \dim(M)$. Induktionsforudsætningen medfører derfor, at $s(M/fM) \leqslant \dim(M/fM)$. På den anden side følger det klart af definitionen på s, at der for hvert element f i $\mathfrak{m}$ gælder, at $s(M) \leqslant s(M/fM) + 1$. Vi har således vist ulighederne $s(M) \leqslant s(M/fM) + 1 \leqslant \dim(M/fM) + 1 \leqslant \dim(M)$, og dermed uligheden $s(M) \leqslant \dim(M)$.

Hermed er de tre uligheder eftervist og beviset for hovedsætningen afsluttet. ∎

(2.4) Tilføjelse. *Under forudsætningerne i Hovedsætningen gælder for ethvert ideal* $\mathfrak{a} \subseteq \mathfrak{m}$ *således at* $M/\mathfrak{a}M$ *har endelig længde, at*

$$d_{\mathfrak{a}}(M) = \dim M.$$

Bevis. Af Lemma (2.2), anvendt på modulen $M/\mathfrak{a}M$, følger, at der findes et naturligt tal k således, at $\mathfrak{m}^k M \subseteq \mathfrak{a}M$. Ifølge antagelsen er $\mathfrak{a}M \subseteq \mathfrak{m}M$. Ved gentagen anvendelse af disse inklusioner ses, at $\mathfrak{m}^{kn} M \subseteq \mathfrak{a}^n M \subseteq \mathfrak{m}^n M$. Vi får derfor følgende uligheder mellem længder:

$$\operatorname{long} M/\mathfrak{m}^{kn} M \geqslant \operatorname{long} M/\mathfrak{a}^n M \geqslant \operatorname{long} M/\mathfrak{m}^n M.$$

Heraf ses, at når $n \gg 0$, er polynomiet $\chi_{\mathfrak{a},M}(n)$ klemt mellem polynomierne $\chi_{\mathfrak{m},M}(kn)$ og $\chi_{\mathfrak{m},M}(n)$. De to sidste polynomier har øjensynlig samme grad, nemlig graden $d_{\mathfrak{m}}(M) = \dim M$. Altså har også det første polynomium denne grad, dvs $d_{\mathfrak{a}}(M) = \dim M$, som påstået. ∎

(2.5) Korollar. *Antag, at* R *er lokal, og lad* $k := R/\mathfrak{m}$ *være restklasselegemet. Krull-dimensionen* $\dim R$ *er da lig med det mindste antal* s *af elementer i* $\mathfrak{m}$, *som frembringer et* $\mathfrak{m}$*-primært ideal. Specielt gælder uligheden,*

$$\dim R \leqslant \operatorname{rk}_k \mathfrak{m}/\mathfrak{m}^2,$$

hvor rangen på højresiden er dimensionen af $\mathfrak{m}/\mathfrak{m}^2$ *som vektorrum over* k.

Bevis. Et ideal $\mathfrak{q} = (f_1, \dots, f_s)$ er som bekendt $\mathfrak{m}$-primært, hvis og kun hvis $\mathfrak{q}$ indeholder en potens af $\mathfrak{m}$, eller ækvivalent, hvis og kun hvis kvotienten $R/\mathfrak{q}$ har endelig længde. Den første påstand i Korollaret er altså blot ligningen $\dim R = s(R)$ fra Hovedsætningen. Lad r være rangen på ulighedens højreside. Da er r, ifølge Nakayama's lemma, lig med det minimale antal elementer, der frembringer $\mathfrak{m}$. Altså er $r \geqslant s(R)$. Uligheden følger derfor af ligningen $s(R) = \dim R$. ∎

(2.6) Parametersystem. Når R er lokal og $M \neq 0$ siges et system af elementer $f_1, \dots, f_s$ af elementer i $\mathfrak{m}$ at være et *parametersystem* for M, hvis $s = \dim M$ og $M/(f_1, \dots, f_s)M$ har endelig længde. Eksistensen af parametersystemer følger af ligningen $s(M) = \dim M$ fra Hovedsætning (2.3).

Specielt er et parametersystem for R et system af $s = \dim R$ elementer $f_1, \dots, f_s$ som frembringer et $\mathfrak{m}$-primært ideal.

(2.7) Korollar. *Antag, at R er lokal og at $M \neq 0$. Der findes da primidealer $\mathfrak{q}$, som tilhører støtten for M og opfylder, at $\dim M = \dim R/\mathfrak{q}$. Ethvert sådant primideal er et minimalt primideal for M. Specielt er der kun endelig mange sådanne primidealer. Lad f være et element i maksimalidealet $\mathfrak{m}$. Hvis f tilhører et af disse primidealer, så er $\dim M/fM = \dim M$. I modsat fald er*

$$\dim M/fM = \dim M - 1.$$

Bevis. Den første påstand følger af Observation (1.5): Dimensionen $\dim M$ er supremum over $\mathfrak{p}$ i støtten for M af $\dim R/\mathfrak{p}$, og da dimensionerne er endelige, er supremum et maximum. Mere præcist findes der kæder,

$$\operatorname{Ann} M \subseteq \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_h,$$

hvor $h = \dim M$, og kravet til $\mathfrak{q}$ er netop, at $\mathfrak{q}$ indgår som $\mathfrak{p}_0$ i en sådan kæde. I en sådan kæde er $\mathfrak{p}_0$ et minimalt primideal for M, thi ellers ville der findes et primideal $\mathfrak{p}$ med $\operatorname{Ann} M \subseteq \mathfrak{p} \subset \mathfrak{p}_0$, og dermed en kæde med $h + 1$ skarpe inklusioner, i modstrid med at $h = \dim M$ var det maksimale antal skarpe inklusioner. Som bekendt findes der kun endelig mange minimale primidealer for M. Heraf følger den tredie påstand.

Lad nu f være element i $\mathfrak{m}$. Støtten for M/fM består af de primidealer $\mathfrak{p}$ i støtten for M, for hvilke $f \in \mathfrak{p}$. Det er altså klart, at $\dim M/fM \leqslant \dim M$, og at lighedstegnet gælder, hvis og kun hvis f tilhører et af de primidealer $\mathfrak{q}$ i støtten for M, for hvilke $\dim R/\mathfrak{q} = \dim M$. Det er således korollarets essentielle påstand, at hvis $\dim M/fM < \dim M$, så gælder $\dim M/fM = \dim M - 1$. Denne påstand følger af ligningen $\dim M = s(M)$ fra Hovedsætningen, idet der øjensynlig altid gælder $s(M) - 1 \leqslant s(M/fM) \leqslant s(M)$. □

(2.8) Bemærkning. Antag, at R er lokal og at $M \neq 0$. Det følger at Korollar (2.7), at når $f \in \mathfrak{m}$, så gælder ulighederne $\dim M - 1 \leqslant \dim M/fM \leqslant \dim M$. Ved gentagen anvendelse af disse uligheder sluttes, at for en vilkårlig følge $(f_1, \dots, f_s)$ af elementer i $\mathfrak{m}$ gælder ulighederne,

$$\dim M - s \leqslant \dim M/(f_1, \dots, f_s) \leqslant \dim M,$$

og yderligere, at hvis uligheden til venstre er en lighed, altså hvis

$$\dim M/(f_1, \dots, f_s)M = \dim M - s, \tag{2.8.1}$$

så er $\dim M/(f_1, \dots, f_i)M = \dim M - i$ for $i = 1, \dots, s$.

Hvis den givne følge er et parametersystem for M, dvs hvis $s = \dim M$ og kvotienten $M/(f_1, \dots, f_s)M$ har endelig længde, så har kvotienten dimension 0, og lighed gælder i (2.8.1). Heraf aflæses, at lighed gælder i (2.8.1) hvis den givne følge er delfølge af et parametersystem.

Antag omvendt, at lighed i (2.8.1) er opfyldt for den givne følge. Da er $s \leqslant \dim M$ og kvotienten $\overline{M} = M/(f_1, \dots, f_s)M$ dimensionen $t := \dim M - s$. Lad $(g_1, \dots, g_t)$ være et parametersystem for $\overline{M}$. Da har

$$M/(f_1, \dots, f_s, g_1, \dots, g_t)M = \overline{M}/(g_1, \dots, g_t)\overline{M}$$

endelig længde og $s + t = \dim M$. Følgen $(f_1, \dots, f_s, g_1, \dots, g_t)$ er derfor et parametersystem for M.

Heraf aflæses, at lighed gælder i (2.8.1), hvis og kun hvis følgen $(f_1, \dots, f_s)$ er delfølge af et parametersystem.

(2.9) Opgaver.

1. I $R := k[X, Y]$ (k er et legeme) betragtes primidealerne $\mathfrak{q} = (0)$, $\mathfrak{p} := (Y)$ og $\mathfrak{m} := (X, Y)$, og kvotienten $M := R/\mathfrak{p}$ som R-modul. Bestem brøkmodulerne $M_\mathfrak{q}$, $M_\mathfrak{p}$, og $M_\mathfrak{m}$, og deres Krull-dimensioner.

3. Dimension af noetherske ringe.

(3.1) Krull's Idealsætning. *Et primideal* $\mathfrak{p} \subseteq R$, *der er isoleret for et ideal frembragt af* s *elementer* $f_1, \dots, f_s$, *har højde mindre end eller lig med* s. *Mere generelt gælder for et primideal* $\mathfrak{p}$, *der er minimalt primideal for en kvotient* $M/(f_1, \dots, f_s)M$, *at* $\dim M_{\mathfrak{p}} \leqslant s$.

Bevis. Højden $\operatorname{ht} \mathfrak{p}$ er lig med dimensionen $\dim R_{\mathfrak{p}}$ af den lokale ring $R_{\mathfrak{p}}$, så den første påstand er et specialtilfælde af den anden. Den anden påstand følger af Hovedsætningen om dimension af lokale ringe. Antag nemlig, at $\mathfrak{p}$ er minimalt primideal for $M/(f_1, \dots, f_s)M$. Da har kvotienten $M_{\mathfrak{p}}/(f_1, \dots, f_s)M_{\mathfrak{p}}$ endelig længde som $R_{\mathfrak{p}}$-modul, og følgelig er $s \geqslant \dim M_{\mathfrak{p}}$. ∎

Bemærkning. Tilfældet $s = 1$ i sætningen (altså følgende resultat: Hvis $\mathfrak{p}$ er isoleret primideal for et hovedideal, så er $\operatorname{ht} \mathfrak{p} \leqslant 1$) kaldes også *Krull's Hovedidealsætning*.

(3.2) Korollar. *Ethvert ægte ideal* $\mathfrak{a}$ *i* R *har endelig højde. Mere generelt gælder, at hvis* $M/\mathfrak{a}M \neq 0$, *så er* M*-højden* $\operatorname{ht}_M \mathfrak{a}$ *endelig og mindre end eller lig med det minimale antal frembringere for* $\mathfrak{a}$.

Bevis. M-højden er infimum af $\dim M_{\mathfrak{p}}$ over alle primidealer $\mathfrak{p}$ i støtten for $M/\mathfrak{a}M$. Det er klart, at infimum antages i et primideal $\mathfrak{p}$, der er minimalt for $M/\mathfrak{a}M$. Påstanden følger derfor af Idealsætningen. ∎

(3.3) Lemma. *Lad* $\mathfrak{b} \subseteq \mathfrak{a}$ *være idealer således at* $\operatorname{ht}_M \mathfrak{b} < \operatorname{ht}_M \mathfrak{a}$. *Da findes i* $\mathfrak{a}$ *et element* f, *således at*

$$\operatorname{ht}_M \mathfrak{b} < \operatorname{ht}_M(\mathfrak{b}, f).$$

Bevis. Af den antagne skarpe ulighed følger specielt, at M-højden $h := \operatorname{ht}_M \mathfrak{b}$ er endelig. Tallet h er infimum af $\dim M_{\mathfrak{p}}$ over primidealer $\mathfrak{p}$ i støtten for $M/\mathfrak{b}M$. For alle primidealer $\mathfrak{p}$ i støtten for $M/\mathfrak{b}M$ gælder altså uligheden,

$$h \leqslant \dim M_{\mathfrak{p}}, \tag{*}$$

og det er klart, at lighed i denne ulighed medfører, at $\mathfrak{p}$ er minimalt primideal for $M/\mathfrak{b}M$. Ligheden $h = \dim M_{\mathfrak{p}}$ gælder derfor kun for endelig mange primidealer $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ i støtten for $M/\mathfrak{b}M$. Det følger af den antagne skarpe ulighed, at intet af $\mathfrak{p}_i$'erne omfatter $\mathfrak{a}$. Heraf følger som bekendt at $\mathfrak{a}$ ikke er indeholdt i foreningsmængden af $\mathfrak{p}_i$'erne. Altså findes et element $f \in \mathfrak{a}$ således at $f \notin \mathfrak{p}_i$ for $i = 1, \dots, r$.

Det påstås, at $\operatorname{ht}_M \mathfrak{b} < \operatorname{ht}_M(\mathfrak{b}, f)$. For et vilkårligt primideal $\mathfrak{p}$ i støtten for $M/(\mathfrak{b}, f)M$ skal det altså vises, at $h < \dim M_{\mathfrak{p}}$. Primidealet $\mathfrak{p}$ tilhører specielt støtten for $M/\mathfrak{b}M$, så uligheden (*) er opfyldt. Yderligere er $f \in \mathfrak{p}$, så valget af f sikrer, at $\mathfrak{p}$ ikke er et af $\mathfrak{p}_i$'erne. Altså er uligheden (*) skarp, hvormed det ønskede er vist. ∎

(3.4) Korollar. *Lad* $(f_1, \dots, f_r)$ *være en højdefølge i et ægte ideal* $\mathfrak{a}$. *Da er*

$$\operatorname{ht}(f_1, \dots, f_i) = i \quad \text{for } i = 0, 1, \dots r.$$

Yderligere er $r \leqslant \operatorname{ht} \mathfrak{a}$, *og følgen kan suppleres til en højdefølge i* $\mathfrak{a}$ *med* $\operatorname{ht} \mathfrak{a}$ *elementer.*

Et tilsvarende resultat gælder når højde erstattes med M-højde.

Bevis. Vi viser resultatet for en M-højdefølge $(f_1, \dots, f_r)$ i et ideal $\mathfrak{a}$, hvor $M/\mathfrak{a}M \neq 0$. At følgen er en M-højdefølge betyder, at uligheden $\operatorname{ht}_M(f_1, \dots, f_i) \geqslant i$ er opfyldt for $i = 1, \dots, r$. Da idealet $(f_1, \dots, f_i)$ er frembragt at i elementer, gælder den modsatte ulighed, og dermed den ønskede lighed, ifølge Korollar (3.2).

Da idealet $(f_1, \dots, f_r)$ er indeholdt i $\mathfrak{a}$, er det klart, at

$$r = \operatorname{ht}_M(f_1, \dots, f_r) \leqslant \operatorname{ht}_M \mathfrak{a}.$$

Hvis uligheden er skarp, findes ifølge Lemma (3.3) et element $f \in \mathfrak{a}$, således at $r < \operatorname{ht}_M(f_1, \dots, f_r, f)$. Altså er $r + 1 \leqslant \operatorname{ht}_M(f_1, \dots, f_r, f)$, og følgen $(f_1, \dots, f_r, f)$ er derfor en M-højdefølge. Gentagen anvendelse af dette argument viser, at følgen kan suppleres til en M-højdefølge i $\mathfrak{a}$ med $\operatorname{ht}_M \mathfrak{a}$ elementer. ▯

(3.5) Korollar. *Et primideal $\mathfrak{p}$ af højde s er isoleret primideal for et ideal frembragt af s elementer.*

Bevis. Ifølge Korollar (3.4) findes i $\mathfrak{p}$ en højdefølge $(f_1, \dots, f_s)$ med $s = \operatorname{ht} \mathfrak{p}$ elementer. Idealet $\mathfrak{p}$ omfatter idealet $(f_1, \dots, f_s)$ og dermed også et isoleret primideal $\mathfrak{q}$ for $(f_1, \dots, f_s)$. Hvis inklusionen $\mathfrak{p} \supseteq \mathfrak{q}$ var skarp, ville højden af $\mathfrak{q}$ være mindre end højden s af $\mathfrak{p}$, og følgelig ville højden af $(f_1, \dots, f_s)$ være mindre end s, i modstrid med at følgen var en højdefølge. Altså er $\mathfrak{p} = \mathfrak{q}$ isoleret primideal for idealet $(f_1, \dots, f_s)$ frembragt af s elementer. ▯

(3.6) Højdeuligheden. *Lad $\theta \colon R \to R'$ være en homomorfi mellem noetherske ringe. Lad $\mathfrak{p}'$ være et primideal i R' og lad $\mathfrak{p} := R \cap \mathfrak{p}'$ være kontraktionen. Ekstensionen $\mathfrak{p}R'$ er da indeholdt i $\mathfrak{p}'$, så $\mathfrak{p}'$ svarer til et primideal $\mathfrak{p}'/\mathfrak{p}R'$ i kvotientringen $R'/\mathfrak{p}R'$. Herom gælder uligheden,*

$$\operatorname{ht} \mathfrak{p}' \leqslant \operatorname{ht} \mathfrak{p} + \operatorname{ht} \mathfrak{p}'/\mathfrak{p}R'.$$

Bevis. Sæt $h := \operatorname{ht} \mathfrak{p}$ og $k := \operatorname{ht} \mathfrak{p}'/\mathfrak{p}R'$. Ifølge Korollar (3.5) findes da h elementer $f_1, \dots, f_h$ i $\mathfrak{p}$ så at $\mathfrak{p}$ er isoleret primideal for idealet i R frembragt af f_i'erne, og k-elementer $g_1, \dots, g_k$ i $\mathfrak{p}'$ så at $\mathfrak{p}'/\mathfrak{p}R'$ er isoleret primideal for idealet i $R'/\mathfrak{p}R'$ frembragt af restklasserne modulo $\mathfrak{p}R'$ af g_j'erne. Det er nok at vise, at $\mathfrak{p}'$ er isoleret primideal for idealet $\mathfrak{a}' := (\theta f_1, \dots, \theta f_h, g_1, \dots, g_k)$, thi så fås den ønskede ulighed $\operatorname{ht} \mathfrak{p}' \leqslant h + k$ af „hvis"-delen af Idealsætningen. Valget af f_i'erne og g_j'erne sikrer, at $\mathfrak{a}' \subseteq \mathfrak{p}'$. Antag derfor, at vi for et primideal $\mathfrak{q}'$ i R' har inklusionerne,

$$\mathfrak{a}' \subseteq \mathfrak{q}' \subseteq \mathfrak{p}'. \tag{3.6.1}$$

Det skal vises, at $\mathfrak{q} = \mathfrak{p}$. For kontraktionerne af de tre idealer i (3.6.1) fås, med oplagte betegnelser, at $\mathfrak{a} \subseteq \mathfrak{q} \subseteq \mathfrak{p}$. Det er klart, at kontraktionen $\mathfrak{a}$ indeholder idealet $(f_1, \dots, f_h)$. Da $\mathfrak{p}$ var isoleret primideal for $(f_1, \dots, f_h)$, følger det, at $\mathfrak{q} = \mathfrak{p}$. Idealet $\mathfrak{q}'$ indeholder altså ekstensionen $\mathfrak{p}R'$. Altså svarer $\mathfrak{q}'$ til et primideal $\mathfrak{q}'/\mathfrak{p}R'$ i kvotienten $R'/\mathfrak{p}R'$. Betragt billederne i $R'/\mathfrak{p}R'$ af de tre idealer i (3.6.1). Billederne af de to sidste er primidealerne $\mathfrak{q}'/\mathfrak{p}R' \subseteq \mathfrak{p}'/\mathfrak{p}R'$ og billedet af det første vil indeholde idealet frembragt af restklasserne af g_i'erne. Da $\mathfrak{p}'/\mathfrak{p}R'$ var isoleret primideal for det sidste ideal, følger det, at $\mathfrak{q}'/\mathfrak{p}R' = \mathfrak{p}'/\mathfrak{p}R'$. Heraf fås den ønskede lighed $\mathfrak{q}' = \mathfrak{p}'$. ▯

(3.7) Bemærkning. En ringhomomorfi $\theta\colon R \to R'$ som i Højdeuligheden (3.6) giver en afbildning $\tilde\theta$ „den modsatte vej" mellem mængderne af primidealer i de to ringe. Elementet $\mathfrak{p}'$, i mængden af primidealer i R', afbildes ved $\tilde\theta$ på kontraktionen $\tilde\theta(\mathfrak{p}') = R \cap \mathfrak{p}'$, opfattet som element i mængden af primidealer i R. Afbildningens *fiber* over et givet primideal $\mathfrak{p}$, dvs originalmængden $\tilde\theta^{-1}(\mathfrak{p})$, består af de primidealer $\mathfrak{p}'$ i R', hvis kontraktion er det givne ideal $\mathfrak{p}$. En fiber er, som delmængde af mængden af samtlige primidealer i R', en partielt ordnet mængde. Hvert primideal $\mathfrak{p}'$ i R' ligger i én fiber, nemlig i fiberen $\tilde\theta^{-1}(\mathfrak{p})$, hvor $\mathfrak{p} := \tilde\theta(\mathfrak{p}')$. Primidealerne, der indgår i bestemmelsen af $\operatorname{ht}\mathfrak{p}'/\mathfrak{p}R'$ på højresiden i Højdeuligheden, dvs primidealerne $\mathfrak{q}'$ i R' som opfylder at $\mathfrak{p}R' \subseteq \mathfrak{q}' \subseteq \mathfrak{p}'$, svarer netop til de primidealer, der er indeholdt i $\mathfrak{p}'$ og ligger i samme fiber som $\mathfrak{p}'$. Højden $\operatorname{ht}\mathfrak{p}'/\mathfrak{p}R'$ angiver altså højden af $\mathfrak{p}'$ *i sin fiber*. Specielt er denne højde højst lig med dimensionen af fiberen gennem $\mathfrak{p}'$, og dermed højst lig med den maximale fiberdimension. Videre er højden $\operatorname{ht}\mathfrak{p}$ højst lig med dimensionen af R. Højresiden i Højdeuligheden er derfor højst lig med $\dim R + e$, hvor e er den maksimale fiberdimension. Af Højdeuligheden fås derfor uligheden,

$$\dim R' \leqslant \dim R + e.$$

Hvis homomorfien i (3.6) er en såkaldt *lokal homomorfi*, dvs en ringhomomorfi mellem lokale ringe, hvorved maksimalidealet $\mathfrak{m}$ i R afbildes ind i maksimalidealet $\mathfrak{m}'$ i R', kan højdeuligheden anvendes på maksimalidealet $\mathfrak{m}'$. Kontraktionen af $\mathfrak{m}'$ bliver da maksimalidealet $\mathfrak{m}$ i R, og kvotienten $R'/\mathfrak{m}R'$ bliver en lokal ring med $\mathfrak{m}'/\mathfrak{m}R'$ som maksimalideal. De tre højder i højdeuligheden bliver derfor dimensionerne af disse lokale ringe, så højdeuligheden har formen,

$$\dim R' \leqslant \dim R + \dim R'/\mathfrak{m}R'.$$

Bemærk, at primidealerne i $R'/\mathfrak{m}R'$ svarer til samtlige primidealer i fiberen over $\mathfrak{m}$.

(3.8) Opgaver.

1. Antag, at R er et integritetsområde. Vis, at et ikke-konstant polynomium $f \in R[X]$ ikke kan være helt over R. Antag, at k er et legeme, og at $f_1, \dots, f_r$ er polynomier i $k[T]$. Hvad kan du sige om dimensionen af $k[f_1, \dots, f_r]$?

4. Dimension af endeligt frembragte algebraer.

(4.1) Setup. Vi betragter stadig en noethersk ring R. For et ideal $\mathfrak{a}$ i R betegnes med $\mathfrak{a}[X]$ ekstensionen af $\mathfrak{a}$ til polynomiumsringen $R[X]$. Ekstensionen $\mathfrak{a}[X]$ består øjensynlig af de polynomier, hvor alle koefficienterne tilhører $\mathfrak{a}$, og kvotienten $R[X]/\mathfrak{a}[X]$ er derfor isomorf med polynomiumsringen $(R/\mathfrak{a})[X]$. Specielt gælder for et primideal $\mathfrak{p}$ i R, at ekstensionen $\mathfrak{p}[X]$ er et primideal i $R[X]$.

(4.2) Lemma. *Lad $\mathfrak{P}$ være et primideal i polynomiumsringen $R[X]$, og lad $\mathfrak{p} := R \cap \mathfrak{P}$ betegne kontraktionen. Hvis $\mathfrak{P} \supset \mathfrak{p}[X]$, så er $\operatorname{ht} \mathfrak{P}/\mathfrak{p}[X] = 1$. Specielt gælder, når kontraktionen $\mathfrak{p}$ er et maksimalideal i R, at $\mathfrak{P}$ er et maksimalideal i $R[X]$, hvis og kun hvis $\mathfrak{P} \supset \mathfrak{p}[X]$.*

Bevis. Den sidste påstand følger af den første. For at indse dette bemærkes først, at kvotienten $R[X]/\mathfrak{p}[X]$ er polynomiumsringen $(R/\mathfrak{p})[X]$, og specielt er kvotienten ikke et legeme. Hvis $\mathfrak{P} = \mathfrak{p}[X]$, er $\mathfrak{P}$ derfor ikke et maksimalideal. Antag omvendt, at $\mathfrak{P}$ ikke er et maksimalideal. Da findes et maksimalideal $\mathfrak{M} \supset \mathfrak{P}$. Nu er $R \cap \mathfrak{M} \supseteq \mathfrak{p}$, og her må lighed gælde, da $\mathfrak{p}$ er antaget at være et maksimalideal. Altså kan lemmaets første påstand anvendes på $\mathfrak{M}$ og $\mathfrak{p}$. Det følger, at der i kæden $\mathfrak{p}[X] \subseteq \mathfrak{P} \subset \mathfrak{M}$ kun kan være ét skarpt inklusionstegn. Altså er $\mathfrak{P} = \mathfrak{p}[X]$.

Nu vises lemmaets første påstand. Lad S betegne komplementærmængden til $\mathfrak{p}$ i R. Ved lokalisering af R mht S fås den lokale ring $R_\mathfrak{p}$, med maksimalidealet $\mathfrak{m} := \mathfrak{p}R_\mathfrak{p}$, og ved lokalisering af $R[X]$ mht S fås øjensynlig polynomiumsringen $R_\mathfrak{p}[X]$. Da $\mathfrak{p}$ er kontraktionen af $\mathfrak{P}$, er $\mathfrak{P}$ disjunkt med S. Ved den bijektive forbindelse mellem primidealer i $R[X]$ disjunkte med S og samtlige primidealer i brøkringen $R_\mathfrak{p}[X]$ svarer $\mathfrak{P}$ altså til sin ekstension $S^{-1}\mathfrak{P}$, og $\mathfrak{p}[X]$ svarer øjensynlig til ekstensionen $\mathfrak{m}[X]$. For at bevise påstanden i Lemmaet kan vi altså erstatte R med $R_\mathfrak{p}$ og $\mathfrak{P}$ med $S^{-1}\mathfrak{P}$. Specielt kan vi altså antage, at kontraktionen $\mathfrak{p}$ er et maksimalideal i R.

Nu er polynomiumsringen $(R/\mathfrak{p})[X]$ et hovedidealområde, fordi koefficientringen $R/\mathfrak{p}$ er et legeme. I et hovedidealområde er øjensynlig ethvert primideal forskelligt fra (0) af højde 1. Ifølge forudsætningen er $\mathfrak{P}/\mathfrak{p}[X]$ ikke (0). Altså er højden af $\mathfrak{P}/\mathfrak{p}[X]$ lig med 1. Hermed er også lemmaets første påstand bevist. □

(4.3) Sætning. *Lad $\mathfrak{P}$ være et primideal i polynomiumsringen $R[X]$, og lad $\mathfrak{p} := R \cap \mathfrak{P}$ betegne kontraktionen. Da gælder ligningerne,*

$$\operatorname{ht} \mathfrak{P} = \operatorname{ht} \mathfrak{p} + \operatorname{ht} \mathfrak{P}/\mathfrak{p}[X] = \begin{cases} \operatorname{ht} \mathfrak{p}, & \textit{hvis}\ \mathfrak{P} = \mathfrak{p}[X] \\ \operatorname{ht} \mathfrak{p} + 1, & \textit{hvis}\ \mathfrak{P} \supset \mathfrak{p}[X] \end{cases}$$

Bevis. Den anden ligning følger umiddelbart af Lemma (4.2). For at bevise den første ligning bemærkes, at venstresiden er mindre end eller lig med højresiden ifølge Højdeuligheden (3.6). Omvendt er det klart, at højresiden er mindre end eller lig med venstresiden, idet enhver kæde af primidealer $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_h$ i R giver en kæde af primidealer i $R[X]$:

$$\mathfrak{p}_0[X] \subset \cdots \subset \mathfrak{p}_h[X] = \mathfrak{p}[X] \subseteq \mathfrak{P}, \tag{4.3.1}$$

og denne kæde kan suppleres med en kæde af primidealer fra $\mathfrak{p}[X]$ til $\mathfrak{P}$. □

(4.4) Korollar. *Når R ikke er nul-ringen, så er* $\dim R[X] = \dim R + 1$.

Bevis. Uligheden $\dim R[X] \leqslant \dim R + 1$ følger umiddelbart af Sætningen. For at vise ligheden bemærkes, at en kæde af primidealer $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_h$ i R med h skarpe inklusioner i R giver kæden (4.3.1) af primidealer i $R[X]$ med h skarpe inklusioner. Det sidste primideal $\mathfrak{p}_h[X]$ i denne kæde er ikke et maksimalideal, idet kvotienten $(R/\mathfrak{p}_0)[X]$ er en polynomiumsring og derfor ikke et legeme. Kæden (4.3.1) kan derfor suppleres med et maksimalideal, der omfatter $\mathfrak{p}_h[X]$ til en kæde med $h + 1$ skarpe inklusioner.

(4.5) Observation. Induktivt følger det af Korollar (4.4), at ringen $R[X_1, \dots, X_n]$ af polynomier i n variable har dimension $\dim R + n$. Specielt har polynomiumsringen $k[X_1, \dots, X_n]$ over et legeme k dimension n, og ringen $\mathbb{Z}[X_1, \dots, X_n]$ har dimension $n + 1$.

(4.6) Eksempel. Betragt den lokale ring $\mathbb{Z}_{(p)}$, der fremkommer ved at lokalisere $\mathbb{Z}$ i primidealet (p) frembragt af et primtal p. Maksimalidealet i $\mathbb{Z}_{(p)}$ er hovedidealet frembragt af p, og det eneste andet primideal i $\mathbb{Z}_{(p)}$ er det trivielle ideal (0). Altså er $\dim \mathbb{Z}_{(p)} = 1$. Polynomiumsringen $\mathbb{Z}_{(p)}[X]$ har altså dimension 2. For eksempel er følgende to kæder maksimale:

$$(0) \subset (X) \subset (X, p) \quad \text{og} \quad (0) \subset (p) \subset (X, p).$$

Primidealerne (X) og (p) har højde 1, og maksimalidealet (X, p) har højde 2. Bemærk imidlertid, at hovedidealet $(pX - 1)$ også er et maksimalideal. Den tilhørende kvotient er nemlig et legeme:

$$\mathbb{Z}_{(p)}[X]/(pX - 1) = \mathbb{Z}_{(p)}[1/p] = \mathbb{Q}.$$

Ringen $\mathbb{Z}_{(p)}[X]$ har altså dimension 2, men der findes maksimalidealer, der kun har højde 1. Denne ring er altså ikke co-equidimensional.

(4.7) Dimensionsformlen for polynomiumsringe. *Lad $R' := R[X_1, \dots, X_n]$ være polynomiumsringen, lad $\mathfrak{P}$ være et primideal i R', og lad $\mathfrak{p} = R \cap \mathfrak{P}$ betegne kontraktionen. Da gælder formlen,*

$$\operatorname{ht} \mathfrak{P} = \operatorname{ht} \mathfrak{p} + n - \operatorname{tdeg}_{R/\mathfrak{p}}(R'/\mathfrak{P})$$

Bevis. Kontraktionen $\mathfrak{p}$ er kernen for den sammensatte homomorfi $R \to R' \to R'/\mathfrak{P}$. Integritetsområdet $R'/\mathfrak{P}$ indeholder derfor integritetsområdet $R/\mathfrak{p}$. Idet x_i betegner restklassen af X_i modulo $\mathfrak{P}$, er det klart, at $R'/\mathfrak{P} = (R/\mathfrak{p})[x_1, \dots, x_n]$. Den optrædende transcendensgrad er altså endelig, og mindre end eller lig med n.

For $n = 1$ er formlen blot resultatet fra Sætning (4.3). Kvotienten $R'/\mathfrak{P}$ er nemlig $(R/\mathfrak{p})[x]$. Antag først, at $\mathfrak{P} = \mathfrak{p}[X]$. Så er $R'/\mathfrak{P} = (R/\mathfrak{p})[X]$ og transcendensgraden er derfor 1. Formlen reduceres altså til ligningen $\operatorname{ht} \mathfrak{P} = \operatorname{ht} \mathfrak{p}$. Antag dernæst, at $\mathfrak{P} \supset \mathfrak{p}[X]$. Så findes et polynomium F, som tilhører $\mathfrak{P}$, men ikke $\mathfrak{p}[X]$. Restklassen $\bar{F}$ af F modulo $\mathfrak{p}[X]$ er altså ikke nulpolynomiet i $(R/\mathfrak{p})[X]$, og da $F \in \mathfrak{P}$ gælder $\bar{F}(x) = 0$. Restklassen x er altså algebraisk over $R/\mathfrak{p}$, og følgelig er transcendensgraden lig med 0. Formlen reduceres altså her til ligningen $\operatorname{ht} \mathfrak{P} = \operatorname{ht} \mathfrak{p} + 1$. Det ses, at formlen i begge tilfælde reduceres til resultatet fra (4.3).

Formlen i det almindelige tilfælde vises ved induktion efter n. Polynomiumsringen R' indeholder polynomiumsringen $R_0 = R[X_1, \dots, X_{n-1}]$ i $n-1$ variable, og $R' = R[X_n]$. Lad $\mathfrak{P}_0 = R_0 \cap \mathfrak{P}$ være kontraktionen til R_0. Anvend formlen for $n = 1$ på $\mathfrak{P}$ og R_0, og anvend (induktivt) formlen for $n-1$ på $\mathfrak{P}_0$ og R. Herved fremkommer ligningerne,

$$\operatorname{ht}\mathfrak{P} = \operatorname{ht}\mathfrak{P}_0 + 1 - \operatorname{tdeg}_{R_0/\mathfrak{P}_0}(R'/\mathfrak{P}),$$
$$\operatorname{ht}\mathfrak{P}_0 = \operatorname{ht}\mathfrak{p} + (n-1) - \operatorname{tdeg}_{R/\mathfrak{p}}(R_0/\mathfrak{P}_0).$$

Den søgte formel for n variable fås nu ved en simpel addition, idet summen af de to transcendensgrader som bekendt er transcendensgraden $\operatorname{tdeg}_{R/\mathfrak{p}}(R'/\mathfrak{P})$. □

(4.8) En speciel egenskab. Lad I være et integritetsområde. Vi kan da betragte følgende betingelse:

(*) I ringen I findes et element $f \neq 0$, således at f tilhører alle primidealer forskellige fra (0) i I.

Som bekendt er der en bijektiv forbindelse mellem primidealer, der ikke omfatter f og samtlige primidealer i brøkringen $I_f = I[1/f]$. At et element $f \neq 0$ har egenskaben i (*) betyder altså, at primidealet (0) er det eneste primideal i brøkringen I_f eller, med andre ord, at brøkringen I_f er et legeme (og dermed lig med brøklegemet for I).

Det er klart, at ethvert legeme opfylder betingelsen (*). Øjensynlig vil ringen $\mathbb{Z}$ ikke opfylde (*). Ringen $\mathbb{Z}_{(p)}$ fra Eksempel (4.6) vil derimod opfylde (*): Det eneste primideal forskelligt fra (0) er (p), så betingelsen i (*) er fx opfyldt med $f = p$ (i overensstemmelse med at brøklegemet for $\mathbb{Z}_{(p)}$ er $\mathbb{Q} = \mathbb{Z}_{(p)}[1/p]$).

I det følgende vil vi (kortvarigt) møde primidealer $\mathfrak{p}$ i R med den egenskab, at betingelsen (*) er opfyldt for kvotientringen $R/\mathfrak{p}$. I mangel af et fornuftigt navn vil vi, helt usystematisk, kalde sådanne primidealer for **primidealer*. Begrebet bruges kun i forberedelserne til beviset for (4.11). Det er klart, at ethvert maksimalideal er et *primideal. I ringen $\mathbb{Z}$ er det kun maksimalidealerne, der er *primidealer. I ringen $\mathbb{Z}_{(p)}$ er også primidealet (0) et *primideal.

(4.9) Lemma. *Lad $\mathfrak{P}$ være et primideal i polynomiumsringen $R[X]$, og lad $\mathfrak{p} := R \cap \mathfrak{P}$ betegne kontraktionen. Antag, at $\mathfrak{P}$ er et *primideal. Da er $\mathfrak{P} \supseteq \mathfrak{p}[X]$ og $\mathfrak{p}$ er et *primideal.*

Bevis. Ved eventuelt at erstatte R med $R/\mathfrak{p}$ kan det antages, at $\mathfrak{p} = (0)$. Ringen R er så et integritetsområde, og den eneste konstant, der tilhører $\mathfrak{P}$ er 0. Den sammensatte homomorfi $R \to R[X] \to R[X]/\mathfrak{P}$ er altså injektiv, så vi kan opfatte R som delring af integritetsområdet $I := R[X]/\mathfrak{P}$. Idet x betegner restklassen af X modulo $\mathfrak{P}$ gælder så, at $I = R[x]$.

Da $\mathfrak{P}$ er et *primideal, findes i I et element $f \neq 0$, som opfylder betingelsen i (*). Det skal vises, at $\mathfrak{P} \neq (0)$ og at kontraktionen (0) i R er et *primideal, altså at betingelsen (*) er opfyldt for R.

Antag, indirekte, at $\mathfrak{P} = (0)$. Da er I polynomiumsringen $R[X]$, og f er et polynomium. Af betingelsen i (*) følger, at f tilhører primidealet (X). Specielt er f ikke et konstant polynomium. Følgelig er også $f+1$ et ikke-konstant polynomium. Altså findes et maksimalideal $\mathfrak{M}$ som omfatter $f+1$. Det er klart, at der så gælder $f \notin \mathfrak{M}$, i modstrid med at f tilhører alle primidealer forskellige fra (0).

Dernæst skal det vises, at betingelsen (*) er opfyldt for R. Da $\mathfrak{P} \neq 0$, findes et polynomium $P \neq 0$ i $\mathfrak{P}$, og da $R \cap \mathfrak{P} = (0)$, er P et ikke-konstant polynomium. Modulo $\mathfrak{P}$ er $P = 0$, dvs $P(x) = 0$. Restklassen x er altså algebraisk over R. Alle elementer i $I = R[x]$ og i I's brøklegeme K er derfor algebraiske over R. Da f opfylder betingelsen i (*), er brøklegemet lig med $I[1/f]$. Med $y := 1/f$ har vi altså

$$K = I[y] = R[x, y],$$

og både x og y er algebraiske over R. Legemet K indeholder R, og dermed også brøklegemet for R. Da x og y er algebraiske over R følger det, at der findes et element $g \neq 0$ i R, således at x og y er hele over brøkringen R_g. Altså er K hel over delringen R_g. Det er velkendt, at når et legeme er helt over en delring, så er også delringen et legeme. Altså er R_g et legeme. Men det betyder netop, at elementet g i R opfylder betingelsen i (*), jfr (4.8).

Hermed er begge lemmaets påstande bevist. □

(4.10) Lemma. *Lad R være en ring med egenskaben, at kun maksimalidealerne er *primidealer. Da har polynomiumsringen $R[X]$ den samme egenskab, og for hvert maksimalideal i $R[X]$ er kontraktionen til R et maksimalideal. Hvis desuden alle maksimalidealer i R har samme højde h, så har alle maksimalidealer i $R[X]$ højden $h + 1$.*

Bevis. Den første påstand fås umiddelbart af Lemma (4.9) og den sidste del af Lemma (4.2). Den anden påstand følger nu af den første del af Lemma (4.2). □

(4.11) Hilbert's Nulpunktssætning. *Betragt over et legeme k polynomiumsringen $A = k[X_1, \dots, X_n]$. For alle maksimalidealer $\mathfrak{M}$ i A gælder da, at $\operatorname{ht}\mathfrak{M} = n$ og at legemet $A/\mathfrak{M}$ er algebraisk over k (og dermed af endelig dimension over k).*

Betragt polynomiumsringen $A = \mathbb{Z}[X_1, \dots, X_n]$. For alle maksimalidealer $\mathfrak{M}$ i A gælder da, at $\operatorname{ht}\mathfrak{M} = n + 1$ og at legemet $A/\mathfrak{M}$ er et endeligt legeme.

Bevis. Det er umiddelbart at generalisere Lemma (4.10) til polynomiumsringen i n variable. Anvendt på et maksimalideal $\mathfrak{M}$ i $A = k[X_1, \dots, X_n]$ følger det, at $\operatorname{ht}\mathfrak{M} = n$. Af Dimensionsformlen (4.7) følger nu, at legemet $A/\mathfrak{M}$ er algebraisk over k. Da dette legeme er frembragt som k-algebra af de n restklasser af X_i modulo $\mathfrak{M}$, er det af endelig dimension over k.

Generaliseringen anvendes på et maksimalideal $\mathfrak{M}$ i ringen $A = \mathbb{Z}[X_1, \dots, X_n]$. Her følger det, at $\operatorname{ht}\mathfrak{M} = n + 1$ og at kontraktionen $\mathfrak{m} := \mathbb{Z} \cap \mathfrak{M}$ er et maksimalideal i $\mathbb{Z}$. Kvotienten $\mathbb{Z}/\mathfrak{m}$ er altså et endeligt legeme $\mathbb{F}_p$. Af Dimensionsformlen følger nu, at legemet $A/\mathfrak{M}$ er algebraisk over $\mathbb{F}_p$. Da legemet $A/\mathfrak{M}$ er frembragt som $\mathbb{F}_p$-algebra af de n restklasser af X_i modulo $\mathfrak{M}$, er det af endelig dimension over det endelige legeme $\mathbb{F}_p$, og dermed selv et endeligt legeme. □

(4.12) Bemærkning. Hvis ringen R har endelig dimension, findes i R en kæde,

$$\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_h, \tag{4.12.1}$$

hvor $h = \dim R$. En sådan kæde må være maksimal i den forstand, at idealet $\mathfrak{p}_0$ må være et minimalt primideal i R, idealet $\mathfrak{p}_h$ må være et maksimalideal i R, og kæden er uforfinelig (mellem to på hinanden følgende $\mathfrak{p}_i$'er findes ingen primidealer). Det er ikke udelukket, at der i R kan findes kæder (4.12.1) med $h < \dim R$, der er maksimale i denne forstand.

For det første er det nemt at give et eksempel på en ring, der har et minimalt primideal $\mathfrak{p}_0$, hvor $\dim R/\mathfrak{p}_0 < \dim R$. I en kæde (4.12.1), der begynder i et sådant $\mathfrak{p}_0$ må der altid gælde $h < \dim R$. Dette er naturligvis udelukket, hvis der i R kun findes ét minimalt primideal, fx hvis R er et integritetsområde.

For det andet er det nemt, jfr Eksempel (4.6), at give et eksempel på en ring med et maksimalideal $\mathfrak{p}_h$, hvor $\operatorname{ht}\mathfrak{p}_h < \dim R$. I en kæde (4.12.1), der ender med et sådant $\mathfrak{p}_h$, må der altid gælde $h < \dim R$. Dette er naturligvis udelukket, hvis der i R kun findes ét maksimalideal, dvs hvis R er lokal.

For det tredie findes der eksempler på (noetherske) ringe, hvori der findes to primidealer $\mathfrak{q} \subset \mathfrak{p}$ som tillader to uforfinelige kæder fra $\mathfrak{q}$ til $\mathfrak{p}$ med et forskelligt antal skarpe inklusioner. En sådan patologisk opførsel er som bekendt udelukket, hvis ringen er *katernær*.

(4.13) Dimensionsformlen for endeligt frembragte algebraer. *Lad R' være en R-algebra, der er frembragt som R-algebra af n elementer i R'. Lad $\mathfrak{q}' \subseteq \mathfrak{p}'$ være primidealer i R', og lad $\mathfrak{q} := R \cap \mathfrak{q}'$ og $\mathfrak{p} := R \cap \mathfrak{p}'$ betegne kontraktionerne. Da gælder uligheden,*

$$\operatorname{ht}\mathfrak{p}'/\mathfrak{q}' \leqslant \operatorname{ht}\mathfrak{p}/\mathfrak{q} + \operatorname{tdeg}_{R/\mathfrak{q}}(R'/\mathfrak{q}') - \operatorname{tdeg}_{R/\mathfrak{p}}(R'/\mathfrak{p}'), \tag{4.13.1}$$

og lighed gælder, hvis polynomiumsringen $R[X_1, \dots, X_n]$ er katernær.

Bevis. Den sammmensatte homomorfi $R \to R' \to R'/\mathfrak{q}'$ har kernen $\mathfrak{q}$, så $R/\mathfrak{q}$ er en del ring af integritetsområdet $R'/\mathfrak{q}'$. Primidealerne $\mathfrak{q}'$ og $\mathfrak{p}'$ svarer i kvotientringen $R'/\mathfrak{q}'$ til primidealerne (0) og $\mathfrak{p}'/\mathfrak{q}'$, og de sidste primidealer kontraheres til delringen $R/\mathfrak{q}$ til primidealerne (0) og $\mathfrak{p}/\mathfrak{q}$. Det følger af Noether's anden Isomorfisætning, at størrelserne i uligheden (4.13.1) ikke ændres, hvis de indgående primidealer erstattes med deres tilsvarende i kvotienterne $R'/\mathfrak{q}'$ og $R/\mathfrak{q}$. Yderligere er det klart, at hvis polynomiumsringen $R[X_1, \dots, X_n]$ er katernær, så er også kvotienten $(R/\mathfrak{q})[X_1, \dots, X_n]$ katernær. Vi kan derfor antage, at R' er et integritetsområde og $\mathfrak{q}' = (0)$, og at R er en delring. Specielt er de to højder, der indgår i uligheden (4.13.1), så blot højderne $\operatorname{ht}\mathfrak{p}'$ og $\operatorname{ht}\mathfrak{p}$.

Ifølge forudsætningen er R' en kvotient af polynomiumsringen $R[X_1, \dots, X_n]$. Igen ses det ved hjælp af Noether's anden Isomorfisætning, at vi kan antage, at R' er denne polynomiumsring. Nu er $\mathfrak{q}'$ så igen (i almindelighed) forskellig fra (0), men kontraktionen $\mathfrak{q}$ er primidealet (0) i integritetsområdet R.

Nu anvendes Dimensionsformlen (4.7) på primidealerne $\mathfrak{q}'$ og $\mathfrak{p}'$. Idet $\operatorname{ht}\mathfrak{q} = 0$ følger det, at differensen $\operatorname{ht}\mathfrak{p}' - \operatorname{ht}\mathfrak{q}'$ netop er højresiden i uligheden (4.13.1). Uligheden er altså ensbetydende med følgende ulighed:

$$\operatorname{ht}\mathfrak{p}'/\mathfrak{q}' \leqslant \operatorname{ht}\mathfrak{p}' - \operatorname{ht}\mathfrak{q}'.$$

Denne sidste ulighed gælder øjensynlig i enhver ring. Da polynomiumsringen R' er et integritetsområde, er denne ulighed en lighed (og dermed også uligheden (4.13.1) en lighed), når polynomiumsringen R' er katernær. $\square$

(4.14) Bemærkning. Vi skal senere se, at polynomiumsringen $k[X_1, \dots, X_n]$ er katernær, når k er et legeme og når $k = \mathbb{Z}$.

Antag, at k er et legeme. Da gælder altså lighed i uligheden (4.13.1). Når A er et integritetsområde, endeligt frembragt som algebra over k, fås af (4.13.1) anvendt med $\mathfrak{q}' = (0)$, at $\operatorname{ht}\mathfrak{p}' = \operatorname{tdeg}_k A - \operatorname{tdeg}_k(A/\mathfrak{p}')$. Den sidste ligning, anvendt når $\mathfrak{p}'$ er et maksimalideal, kombineret med Hilbert's Nulpunktssætning (4.11), viser, at $\dim A = \operatorname{tdeg}_k A$. Indsættes dette resultat i (4.13.1) fås følgende resultat:

(4.15) Dimensionsformel for algebraer over et legeme. *Lad A være integritetsområde, der er endeligt frembragt som algebra over legemet k. For hvert primideal $\mathfrak{p}$ i A gælder da formlen,*

$$\operatorname{ht}\mathfrak{p} + \operatorname{tdeg}_k(A/\mathfrak{p}) = \dim A. \tag{4.15.1}$$

Bemærk, at denne formel indeholder alle de tidligere fundne resultater om polynomiumsringen $k[X_1, \dots, X_n]$. For det første, anvendt med $\mathfrak{p} = (0)$, viser formlen for et integritetsområde A, at

$$\dim A = \operatorname{tdeg}_k A. \tag{*}$$

Når A specielt er polynomiumsringen, genfinder vi resultatet, at $\dim k[X_1, \dots, X_n] = n$. Yderligere genfinder vi, når A er et legeme, Hilbert's Nulpunktssætning.

Betragt nu en vilkårlig endelig frembragt algebra A over k, og i A en maksimal kæde af primidealer,

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_h.$$

Da kæden er uforfinelig, er $\operatorname{ht}\mathfrak{p}_i/\mathfrak{p}_{i-1} = 1$. Anvendelse af formlen med $A := A/\mathfrak{p}_{i-1}$ og $\mathfrak{p} := \mathfrak{p}_i/\mathfrak{p}_{i-1}$ og ligningen (*) med $A := A/\mathfrak{p}_i$ viser nu, at $1 = \dim A/\mathfrak{p}_{i-1} - \dim A/\mathfrak{p}_i$. Ved addition af disse ligniger for $i = 1, \dots, h$ fås $h = \dim A/\mathfrak{p}_0 - \dim A/\mathfrak{p}_h$. Da kæden var maksimal, er $\mathfrak{p}_h$ et maksimalideal i A, og følgelig er $\dim A/\mathfrak{p}_h = 0$. Altså gælder ligningen,

$$h = \dim A/\mathfrak{p}_0.$$

Da kæden var maksimal er $\mathfrak{p}_0$ et minimalt primideal i A. Vi aflæser derfor, at A er bi-equidimensional, hvis og kun hvis A er equidimensional. Specielt er A altså bi-equidimensional (og dermed katernær), når A er et integritetsområde, fx når $A = k[X_1, \dots, X_n]$.

For et givet primideal $\mathfrak{p}$ i A kan vi vælge $\mathfrak{p}_0 \subseteq \mathfrak{p}$ med $\operatorname{ht}\mathfrak{p} = \operatorname{ht}\mathfrak{p}/\mathfrak{p}_0$, og anvende formlen på primidealet $\mathfrak{p}/\mathfrak{p}_0$ i $A/\mathfrak{p}_0$. Det giver $\operatorname{ht} p + \operatorname{tdeg}_k A = \dim A/\mathfrak{p}_0$. en maksimal kæde være valgt, så den indeholder $\mathfrak{p}$, fx med $\mathfrak{p} = \mathfrak{p}_n$ og $n = \operatorname{ht} p$. Formlen kan så anvendes på integritetsområdet $A/\mathfrak{p}_0$, og den viser, at $\operatorname{ht}\mathfrak{p} + \operatorname{tdeg}_k A/\mathfrak{p} = \dim A/\mathfrak{p}_0$. Primidealet $\mathfrak{p}_0$ er med sikkerhed et minimalt primideal i A. Hvis A er equidimensional, er formlens højreside altså lig med $\dim A$. Med andre ord: Dimensionsformlen (4.15.1) gælder, når A blot antages at være equidimensional.

5. Dimension af endeligt frembragte algebraer over legemer.

(5.1) Setup. I denne paragraf betegner k et legeme. Den noetherske ring R vil typisk være en endeligt frembragt algebra over k, eller, ækvivalent, R vil være en kvotient af polynomiumsringen $k[X_1, \dots, X_n]$ modulo et ideal.

(5.2) Nøglelemma. *Antag, at R er et integritetsområde, endeligt frembragt som algebra over k. Lad $\mathfrak{p}$ være et primideal i R. Antag, at $\mathfrak{p}$ er isoleret primideal for et hovedideal $Rf \neq (0)$. Da gælder ligningen,*

$$\operatorname{tdeg}_k(R/\mathfrak{p}) = \operatorname{tdeg}_k R - 1. \tag{5.2.1}$$

Bevis. Ideen i beviset er følgende: Først vises nøglelemmaet i specialtilfældet, hvor R er polynomiumsringen $k[X_1, \dots, X_n]$. Dernæst reduceres den almindelige påstand til specialtilfældet ved hjælp af Noether's Normaliseringslemma: Algebraen R er hel over en delring R_0, som er en polynomiumsring. Lad $\mathfrak{p}_0 = R_0 \cap \mathfrak{p}$. Da R er hel over R_0 har R og R_0 samme transcendensgrad over k. Af samme grund har $R/\mathfrak{p}$ og $R_0/\mathfrak{p}_0$ samme transcendensgrad. Ligningen (5.2.1) gælder altså for R og $\mathfrak{p}$, hvis og kun hvis den gælder for R_0 og $\mathfrak{p}_0$. Da påstanden er vist for polynomiumsringen R_0, skal det altså vises, at når $\mathfrak{p}$ er isoleret primideal for et hovedideal $Rf \neq (0)$, så er $\mathfrak{p}_0$ isoleret primideal for et hovedideal $R_0 f_0 \neq (0)$. Denne sidste påstand er det ikke så nemt at vise direkte. Vi går en omvej: Først vises, at det er nok at bevise ligning (5.2.1) når $\mathfrak{p}$ har egenskaben, at det er det eneste isolerede primideal for et hovedideal forskelligt fra (0). Dernæst vises, at hvis $\mathfrak{p}$ har denne egenskab, så har $\mathfrak{p}_0$ den også.

Disse enkelte skridt gennemføres i følgende 3 lemmaer. Når de er vist, er Nøglelemmaet altså bevist. □

(5.3) Lemma. *Påstanden i Nøglelemmaet gælder, hvis $R := k[X_1, \dots, X_n]$ er polynomiumsringen.*

Bevis. Antag nemlig, at $\mathfrak{p}$ er isoleret primideal for et hovedideal $Rf \neq (0)$. Polynomiet f kan ikke være konstant. Skriv f som produkt af irreducible polynomier p_i. Da f tilhører $\mathfrak{p}$, vil en af de irreducible faktorer p_i tilhøre $\mathfrak{p}$. Altså er $Rf \subseteq Rp_i \subseteq \mathfrak{p}$. Da $\mathfrak{p}$ forudsættes at være isoleret primideal for Rf, følger det, at $\mathfrak{p} = Rp_i$. Forudsætningen medfører altså, at $\mathfrak{p}$ er et hovedideal frembragt af et irreducibelt polynomium p.

Polynomiet p kan ikke være konstant, så vi kan antage, at fx den variable X_n forekommer i p. Det er nok at vise, at de $n-1$ restklasser x_i af X_i modulo Rp for $i = 1, \dots, n-1$ er algebraisk uafhængige over k. Antag hertil, at der findes en algebraisk relation $F(x_1, \dots, x_{n-1}) = 0$, hvor F er et polynomium i $n-1$ variable. Vi slutter så, at $F(X_1, \dots, X_{n-1})$ tilhører idealet Rp, altså at der findes en ligning,

$$F(X_1, \dots, X_{n-1}) = hp,$$

med et polynomium h i $k[X_1, \dots, X_n]$. Den variable X_n forekommer i polynomiet p, men ikke på ligningens venstreside. Heraf sluttes, at venstresiden må være nul-polynomiet. Følgelig er $x_1, \dots, x_{n-1}$ algebraisk uafhængige. □

(5.4) Lemma. *Det er nok at bevise, at påstanden i Nøglelemmaet gælder, når $\mathfrak{p}$ er det eneste isolerede primideal for et hovedideal $Rf \neq (0)$.*

Bevis. Antag nemlig, at der yderligere findes r isolerede primidealer $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ for hovedidealet Rf. Da er intet af $\mathfrak{p}_i$'erne indeholdt i $\mathfrak{p}$. Følgelig er fællesmængden af $\mathfrak{p}_i$'erne ikke indeholdt i $\mathfrak{p}$. Altså findes et element g i R således at $g \in \mathfrak{p}_i$ og $g \notin \mathfrak{p}$. Betragt brøkringen $R' := R_g$. Den er en endeligt frembragt algebra over k, da $R' = R[1/g]$. Da $g \notin \mathfrak{p}$ er ekstensionen $\mathfrak{p}' := \mathfrak{p}R'$ et primideal i R'. Ringen R' er en lokalisering af R, og de to ringe har derfor samme transcendensgrad. Kvotientringen $R'/\mathfrak{p}'$ er ifølge Lokaliseringsprincippet en lokalisering af kvotientringen $R/\mathfrak{p}$, og de to kvotientringe har derfor samme transcendensgrad over k. Heraf ses, at ligningen i Nøglelemmaet gælder for R og $\mathfrak{p}$, hvis og kun hvis den gælder for R' og $\mathfrak{p}'$. Det er let at se, at valget af g sikrer, at $\mathfrak{p}'$ er det eneste isolerede primideal for hovedidealet $R'f$. Hermed er påstanden bevist. □

(5.5) Lemma. *Antag, at R er et integritetsområde og helt over en delring R_0, som er en polynomiumsring over k. Lad $\mathfrak{p}$ være et primideal i R, som har egenskaben, at $\mathfrak{p}$ er det eneste isolerede primideal for et hovedideal forskelligt fra (0). Da har kontraktionen $\mathfrak{p}_0 := R_0 \cap \mathfrak{p}$ den samme egenskab.*

Bevis. Bemærk først, at $\mathfrak{p}$ er det eneste isolerede primideal for hovedidealet Rf, hvis og kun hvis $\mathfrak{p} = \mathrm{Rad}(Rf)$. Dette følger af, at radikalet som bekendt er lig med fællesmængden af alle primidealer, som omfatter Rf.

Antag nu, at primidealet $\mathfrak{p}$ har egenskaben, altså at

$$\mathfrak{p} = \mathrm{Rad}(Rf) \quad \text{hvor } f \neq 0.$$

Ringen R er antaget hel over delringen R_0, så brøklegemet for R er algebraisk over brøklegemet for R_0. Betragt det minimale polynomium polynomium for f over brøklegemet for R_0:

$$F = X^m + f_{m-1}X^{m-1} + \cdots + f_1X + f_0.$$

A priori er koefficienterne f_j elementer i brøklegemet for R_0. Det påstås, at alle kofficienterne tilhører R_0. Hertil bemærkes, at polynomiet F i et passende stort legeme kan faktoriseres: $F = (X - \alpha_1) \cdots (X - \alpha_m)$. Da R er hel over R_0 er f rod i et normeret polynomium med koefficienter i R_0. Dette polynomium har det minimale polynomium som divisor, og det har derfor hvert α_i som rod. Altså er hvert α_i helt over R_0. Koefficienterne f_j er summer af produkter af α_i'erne. Derfor er koefficienterne f_j hele over R_0. Desuden tilhører de brøklegemet for R_0. Da R_0 er polynomiumsringen over et legeme, og dermed en faktoriel ring, følger det endelig, at koefficienterne f_j tilhører R_0.

Da $f \neq 0$, er $f_0 \neq 0$. Lemmaet er derfor vist, når vi har bevist ligningen,

$$\mathfrak{p}_0 = \mathrm{Rad}(R_0 f_0). \tag{5.5.1}$$

Højresiden i denne ligning er indeholdt i venstresiden. Det er nemlig hertil nok at vise, at $f_0 \in \mathfrak{p}_0$. Ifølge antagelsen er $f \in \mathfrak{p}$ og af ligningen,

$$F(f) = f^m + f_1 f^{m-1} + \cdots + f_1 f + f_0 = 0,$$

følger specielt, at $f_0 \in Rf \subseteq \mathfrak{p}$. Altså er $f_0 \in R_0 \cap \mathfrak{p} = \mathfrak{p}_0$.

Betragt omvendt et element a_0 på venstresiden, altså $a_0 \in \mathfrak{p}_0$. Det skal vises, at a_0 har en potens, der tilhører $R_0 f_0$. Nu var $a_0 \in \mathfrak{p}_0 \subseteq \mathfrak{p}$ og $\mathfrak{p} = \mathrm{Rad}(Rf)$. Elementet a_0 har derfor en potens, der tilhører idealet Rf. Idet vi kan erstatte a_0 med denne potens, kan vi antage, at a_0 tilhører Rf. Der findes altså en ligning,

$$a_0 = gf, \quad \text{hvor } g \in R.$$

Lad nu G være det minimale polynomium for a_0/f over brøklegemet for R_0. Da $a_0 \in R_0$, bestemmes G ud fra det minimale polynomium F for f ved ligningen,

$$G(X) = \frac{1}{f_0} X^m F(a_0/X).$$

På den anden side var $a_0/f = g$ element i R, og a_0/f er derfor hel over R_0. Polynomiet G har derfor koefficienter i R_0. Specielt er konstantleddet a_0^m/f_0 element i R_0. Altså er $a_0^m \in R_0 f_0$, og følgelig tilhører a_0 højresiden i (5.5.1). Hermed er ligning (5.5.1) eftervist og beviset for lemmaet afsluttet. □

(5.6) Dimensionsformlen. *Antag, at R er en endeligt frembragt k-algebra, og equidimensional. Lad $\mathfrak{p}$ være et primideal i R. Da gælder formlen,*

$$\mathrm{ht}\,\mathfrak{p} + \mathrm{tdeg}_k\, R/\mathfrak{p} = \dim R. \tag{5.6.1}$$

Bevis. Som nævnt i slutningen af (4.15) er det nok at betragte tilfældet, hvor R er et integritetsområde. Betragt en kæde af primidealer i R,

$$(0) = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_h = \mathfrak{p}, \tag{*}$$

og sæt $R_i := R/\mathfrak{p}_i$. For $i < h$ er R_{i+1} så kvotienten af R_i modulo primidealet $\mathfrak{p}_{i+1}/\mathfrak{p}_i$. Heraf følger som bekendt, at $\mathrm{tdeg}_k\, R_{i+1} < \mathrm{tdeg}_k\, R_i$. Da transcendensgrader er ikke-negative følger det specielt, at $h \leqslant \mathrm{tdeg}_k\, R$. Altså er dimensionen endelig, $\dim R \leqslant \mathrm{tdeg}_k\, R$.

Antag nu, at kæden (*) er uforfinelig. I ringen R_i, for $i < h$, findes da ingen primidealer mellem $\mathfrak{p}_{i+1}/\mathfrak{p}_i$ og primidealet (0). Primidealet $\mathfrak{p}_{i+1}/\mathfrak{p}_i$ er derfor isoleret for hovedidealet frembragt at et vilkårligt af sine elementer forskellige fra 0. Af Nøglelemma'et sluttes derfor, at $\mathrm{tdeg}_k\, R_{i+1} = \mathrm{tdeg}_k\, R_i - 1$. Heraf ses, at

$$\mathrm{tdeg}_k\, R_h = \mathrm{tdeg}_k\, R - h.$$

Dette resultat anvendes først med $\mathfrak{p}$ lig med et maksimalideal i R. I dette tilfælde følger det af Hilbert's Nulpunktssætning, at legemet $R/\mathfrak{p}$ er af transcendensgrad 0 over k. Altså er i dette tilfælde $h = \mathrm{tdeg}_k\, R$. I R gælder altså, at enhver uforfinelig kæder af primidealer fra (0) til et maksimalideal indeholder $\mathrm{tdeg}_k\, R$ skarpe inklusionstegn. Transcendensgraden $\mathrm{tdeg}_k\, R$ er altså lig med dimensionen af R og også lig med den fælles højde af maksimalidealerne i R.

Betragt nu et vilkårligt primideal $\mathfrak{p}$ i R og en uforfinelig kæde af primidealer (*). Supplér med en uforfinelig kæde af primidealer,

$$\mathfrak{p} = \mathfrak{p}'_0 \subset \cdots \subset \mathfrak{p}'_l,$$

således at $\mathfrak{p}'_l$ er et maksimalideal. Af det lige viste, anvendt på R og på $R/\mathfrak{p}$, følger, at $h + l = \operatorname{tdeg}_k R = \dim R$ og $l = \operatorname{tdeg}_k(R/\mathfrak{p})$. Altså er

$$h + \operatorname{tdeg}_k R/\mathfrak{p} = \dim R.$$

Da kæden (*) var en vilkårlig uforfinelig kæde, følger heraf dimensionsformlen (5.6.1). □

(5.7) Bemærkning. Som nævnt i (4.15) medfører Dimensionsformlen alle de tidligere viste resultater om polynomiumsringen $k[X_1, \ldots, X_n]$. Specielt følger det, at polynomiumsringen er bi-equidimensional (og specielt katernær).

Notater

1. Hilbert-polynomium.

(1.1) Definition. Lad et øjeblik A være en kommutativ (additivt skrevet) gruppe (i anvendelserne er A oftest lig med $\mathbb{Z}$). Betragt funktioner $\varphi\colon \mathbb{Z} \to A$. For sådanne funktioner defineres *differensoperatoren* Δ ved

$$\Delta\varphi(n) := \varphi(n+1) - \varphi(n).$$

Differensligningen $\Delta\varphi = 0$ har som løsninger øjensynlig netop de konstante funktioner. En højreinvers til Δ er summationsoperatoren Σ. For værdier $n \geqslant 0$ er den defineret ved summen,

$$\Sigma\varphi(n) := \sum_{0 \leqslant i < n} \varphi(i).$$

Bemærk, at $\Sigma\varphi(0) = 0$. Det er klart, at for $n \geqslant 0$ gælder ligningen,

$$\Delta\Sigma\varphi(n) = \varphi(n).$$

Det er ikke svært at udvide definitionen af $\Sigma\varphi(n)$ til negative værdier af n således at den sidste ligning gælder for alle værdier af n.

(1.2) Observation. For et givet element a i A defineres for $i \geqslant 0$ funktionerne $\varphi_{i,a}$ ved

$$\varphi_{i,a}(n) := \binom{n}{i} a.$$

Funktionen $\varphi_{0,a}$ er den konstante funktion a og for $i = 1$ fås funktionen $n \mapsto na$ (her og i det følgende betegner $na = an$ den n'te potens af a i gruppen A).

For $i > 0$ gælder ligningen $\Delta\varphi_{i,a} = \varphi_{i-1,a}$, idet binomialkoefficienterne som bekendt opfylder ligningen $\binom{n+1}{i} - \binom{n}{i} = \binom{n}{i-1}$. Heraf følger ligningen,

$$\Sigma\varphi_{i,a} = \varphi_{i+1,a}.$$

Funktionerne på ligningens to sider giver nemlig samme funktion når Δ anvendes, nemlig funktionen $\varphi_{i,a}$. Desuden har de begge værdien 0 for $n = 0$. Følgelig er de to funktioner identiske.

(1.3) Eksempel. Funktionen $\sigma_2(n) := 1^2 + 2^2 + \cdots + (n-1)^2$ fås ved at anvende operatoren Σ på funktionen n^2. Øjensynlig er $n^2 = 2\binom{n}{2} + \binom{n}{1}$. Følgelig udledes ligningen $\sigma_2(n) = 2\binom{n}{3} + \binom{n}{2}$, og altså den velkendte formel,

$$1^2 + 2^2 + \cdots + n^2 = 2\binom{n+1}{3} + \binom{n+1}{2}.$$

(1.4) Definition. I det følgende vil vi kun interessere os for funktionsværdierne $\varphi(n)$ for store værdier af n. Vi vil her sige, at funktionen $\varphi\colon \mathbb{Z} \to A$ er en *polynomial funktion*, hvis der findes et tal $r \geqslant 0$, således at $\Delta^{r+1}\varphi(n) = 0$ for $n \gg 0$.

Ved *graden* af en polynomial funktion φ forstås det største tal r for hvilket funktionen $\Delta^r\varphi(n)$ for $n \gg 0$ ikke er identisk 0. Hvis $\varphi(n) = 0$ for $n \gg 0$ findes ingen sådanne tal r; en sådan funktion tillægges graden $-\infty$.

En funktion φ er øjensynlig polynomial af grad $\leqslant r$, hvis og kun hvis $\Delta^{r+1}\varphi(n) = 0$ for $n \gg 0$. At φ er polynomial af grad 0 betyder, at funktionsværdien $\varphi(n)$ for store værdier af n er en konstant forskellig fra nul-elementet i A.

(1.5) Sætning. *For funktioner $\varphi\colon \mathbb{Z} \to A$ og et givet tal $r \geqslant 0$ er følgende betingelser ækvivalente:*

(i) *Funktionen φ er polynomial af grad $\leqslant r$.*
(ii) *Funktionen $\Delta\varphi$ er polynomial af grad $\leqslant r-1$.*
(iii) *Der findes $r+1$ elementer $a_0, \dots, a_r$ i A således at*

$$\varphi(n) = a_r\binom{n}{r} + \cdots + a_1\binom{n}{1} + a_0 \text{ for } n \gg 0.$$

(iv) (Når A er en undergruppe i $\mathbb{C}$:) *Der findes et polynomium f af grad $\leqslant r$ således at $\varphi(n) = f(n)$ for $n \gg 0$.*

Hvis betingelserne er opfyldt, så gælder yderligere, at koefficienterne a_i i (iii) *er entydigt bestemt ved φ, og at φ har grad r, hvis og kun hvis $a_r \neq 0$.*

Bevis. Det følger umiddelbart af definitionen, at (i) og (ii) er ækvivalente. I (iii) er funktionen på højresiden summen af funktionerne φ_{i,a_i} for $i = 0, \dots, r$. Af udregningen i Observation (1.2) følger, at denne sum er polynomial af grad $\leqslant r$. Altså vil (iii) medføre (i). Binomialkoefficienten $\binom{n}{i}$ er, som funktion af n, et polynomium af grad i. Heraf ses, at (iii) medfører (iv). Når operatoren Δ anvendes på monomiet n^r fås øjensynlig et polynomium af grad $r-1$ med ledende koefficient r. Heraf ses, at når Δ^r anvendes på et polynomium af grad r med ledende koefficient a fås konstanten $r!a$. Herefter er det klart, at (iv) medfører (i).

Vi mangler at vise, at (i) medfører (iii). Denne påstand vises ved induktion efter r. Den er sand for $r = 0$, idet begge betingelser udtrykker, at $\varphi(n)$ er konstant for $n \gg 0$. Antag $r > 0$. Funktionen $\Delta\varphi$ er polynomial af grad $\leqslant r-1$, så induktivt findes altså r elementer $a_1, \dots, a_r$ i A således at de to funktioner $\Delta\varphi$ og $\varphi_{a_r,r-1} + \cdots + \varphi_{a_2,1} + \varphi_{a_1,0}$ har samme værdi i n, når $n \gg 0$. Disse to funktioner fås ved at anvende operatoren Δ på funtionerne φ og $\varphi_{a_r,r} + \cdots + \varphi_{a_1,1}$. Heraf ses, at når Δ anvendes på differensen,

$$\varphi - \big(\varphi_{a_r,r} + \cdots + \varphi_{a_1,1}\big),$$

så fås en funktion, der er 0 for store værdier af n. Differensen selv må derfor være en konstant for store værdier af n. Betegnes denne konstant med a_0, gælder øjensynlig den ønskede relation i (iii).

Hermed er vist, at betingelserne er ækvivalente. Entydigheden af koefficienterne (iii) vises ved et lignende induktivt argument. Endelig følger det af relationen i (iii), at $\Delta^r\varphi(n) = a_r$ for $n \gg 0$. Graden af φ er altså r (og ikke mindre end r), netop når $a_r \neq 0$. □

(1.6) Setup. I det følgende betragtes en noethersk ring R, og polynomiumsringen $G := R[X_1, \dots, X_r]$ i r variable. Som bekendt er også G en noethersk ring. Ringen G er *gradueret*: Idet G_i er undermodulen af homogene polynomier af grad i, kan ethvert polynomium $f \in G$ skrives som summen af sine homogene led:

$$f = f_0 + f_1 + f_2 + \cdots$$

(summen er naturligvis endelig: $f_i \neq 0$ gælder kun for endelig mange i).

Videre betragtes en endeligt frembragt, gradueret G-modul N. At N er gradueret, betyder, at der i N er givet R-undermoduler N_j for $j \in \mathbb{Z}$ således, at N som R-modul er den direkte sum af undermodulerne N_j:

$$N = \cdots \oplus N_{-1} \oplus N_0 \oplus N_1 \oplus N_2 \oplus \cdots ;$$

det betyder, at hvert element $x \in N$ entydigt kan skrives som en sum af sine *homogene* led:

$$x = \cdots + x_{-1} + x_0 + x_1 + x_2 + \cdots, \quad \text{med } x_j \in N_j \text{ for } j \in \mathbb{Z}, \text{ og } x_j = 0, \text{ når } |j| \gg 0,$$

og at multiplikation med en skalar, der er homogen af grad i i G, afbilder $N_j \to N_{i+j}$. Med andre ord, hvis $f \in G_i$ og $x \in N_j$, så er $fx \in N_{i+j}$.

Da N er endeligt frembragt, er N også frembragt af endelig mange homogene elementer v_α; lad n_α være graden af v_α. Hvert polynomium f er en R-linearkombination af endelig mange *monomier* m_β. Hvis d_β er graden af monomiet m_β, så har $m_\beta v_\alpha$ graden $d_\beta + n_\alpha$. Derfor er N_n frembragt af de produkter $m_\beta v_\alpha$ for hvilke $d_\beta + n_\alpha = n$, og det giver kun endelig mange muligheder for β. Specielt er N_n en endeligt frembragt R-modul.

Vi vil interessere os for følgende betingelse:

($*$) Hver af de homogene komponenter N_n har endelig længde som R-modul.

Da hvert N_n er endeligt frembragt som R-modul, er betingelsen ($*$) fx opfyldt, når ringen R har endelig længde.

Observation. Betingelsen ($*$) er opfyldt, når blot hver af de endelig mange cykliske undermoduler Rv_α af N_{n_α} har endelig længde. For hvert monomium m_β i G definerer multiplikation med m_β nemlig en surjektiv homomorfi af Rv_α på $Rm_\beta v_\alpha$. Hvis alle undermodulerne Rv_α har endelig længde, så følger det, at også undermodulerne $Rm_\beta v_\alpha$ har endelig længde, og da N_n var en sum af endelig mange sådanne undermoduler, har også N_n endelig længde.

(1.7) Sætning. *Antag setup'et i* (1.6), *og at betingelsen* $(*)$ *er opfyldt. Da er funktionen,*

$$\lambda_N(n) := \operatorname{long} N_n,$$

en polynomial funktion med værdier i $\mathbb{Z}$ *af grad mindre end* r *(hvor* r *var antallet af variable i polynomiumsringen* G*).*

Bevis. Sætningen vises ved induktion efter r. For $r = 0$, er $G = G_0 = R$ og $G_i = 0$ for $i \neq 0$. Der er kun ét homogent monomium i G, nemlig konstanten 1, og den største grad af et produkt $m_\beta v_\alpha$ er derfor den største grad af frembringerne v_α. Derfor er $N_n = 0$, når n er større end denne grad. For $n \gg 0$ er altså $\lambda_N(n) = 0$, og følgelig er λ_N polynomial af grad $\leqslant -1$.

Antag, at $r \geqslant 1$, og betragt multiplikation med skalaren X_r i modulen N. Denne multiplikation er en lineær afbildning af N ind i N, og den er homogen af grad 1. Lad K være kernen og lad L være kokernen. Da er K og L graduerede moduler, idet K_n blot er kernen for multiplikationen $X_r \colon N_n \to N_{n+1}$ og L_n defineres som kokernen for denne multiplikation. Vi har da for hvert n en eksakt følge,

$$0 \to K_n \to N_n \xrightarrow{X_r} N_{n+1} \to L_n \to 0.$$

Modulen L er en kvotient af N, og derfor endeligt frembragt. Da G som nævnt er noethersk, er også undermodulen K i N endeligt frembragt. Videre er K_n, som undermodul af N_n, og L_n, som kvotientmodul af N_{n+1}, af endelig længde som R-moduler. Modulerne K og L opfylder altså betingelsen $(*)$. Af den eksakte følge sluttes videre, at den alternerende sum af de indgående modulers længde er lig med 0. Da $\operatorname{long} N_{n+1} - \operatorname{long} N_n = \lambda_N(n+1) - \lambda_N(n) = \Delta\lambda_N(n)$, gælder altså ligningen,

$$\Delta\lambda_N = \lambda_L - \lambda_K\,. \tag{1.7.1}$$

De to moduler L og K annulleres af skalaren X_r, og de kan derfor opfattes som moduler over kvotientringen G/X_rG, som vi kan identificere med polynomiumsringen $R[X_1, \dots, X_{r-1}]$ i $r-1$ variable. Modulerne L og K, som moduler over G/GX_r, opfylder altså forudsætningen med $r-1$ i stedet for r. Induktivt sluttes derfor, at de to funktioner på højresiden af (1.7.1) er polynomiale af grad mindre end $r-1$. Altså er $\Delta\lambda_N$ polynomial af grad mindre en $r-1$. Af Sætning (1.5) følger så, at λ_N er polynomial af grad mindre end r, som påstået. □

(1.8) Definition. Antag, at betingelserne i Sætning (1.7) er opfyldt. Funktionen λ_N er da polynomial af en grad d, der er mindre end eller lig med $r-1$. Antag først, at $d = -\infty$. I dette tilfælde er altså $\operatorname{long} N_n = 0$ for $n \gg 0$, altså $N_n = 0$ for $n \gg 0$. Da også $N_n = 0$ for $n \ll 0$ (dette følger af at N er endeligt frembragt), er altså kun endelig mange N_n'er forskellige fra 0. Modulen N er den direkte sum af N_n'erne, så N har derfor endelig længde som R-modul. Omvendt er det klart, at hvis N har endelig længde som R-modul, så er kun endelig mange N_n'er forskellige fra 0. Betingelsen $d = -\infty$ gælder altså hvis og kun hvis N har endelig længde som R-modul.

Antag dernæst, at $d \geqslant 0$. Af Sætning (1.5), anvendt med $A = \mathbb{Z}$, følger så, at der findes $d+1$ hele tal $e_0, \dots, e_d$, så at

$$\operatorname{long} N_n = e_d \binom{n}{d} + \cdots + e_1 \binom{n}{1} + e_0 \text{ for } n \gg 0. \tag{1.8.1}$$

Polynomiet på højresiden af ovenstående ligning kaldes for *Hilbert-polynomiet* hørende til den givne modul N, og det betegnes χ_N. Graden af Hilbert-polynomiet, altså tallet d, kaldes også den *homogene dimension* af N, og koefficienten e_d kaldes *multipliciteten* af N. Bemærk, at multipliciteten e_d er positiv. Multipliciteten er nemlig forskellig fra 0, og var den negativ ville højresiden i (1.8.1) være negativ når $n \gg 0$, i modstrid med at venstresiden i (1.8.1) er en længde, og dermed ikke-negativ.

(1.9) Bemærkning. Betragt, under forudsætningerne i Sætning (1.7), den akkumulerede sum,

$$\sigma_N(n) := \sum\nolimits_{i<n} \operatorname{long} N_i,$$

Den herved definerede funktion σ_N opfylder øjensynlig $\Delta\sigma_N = \lambda_N$. Da λ_N er polynomial af grad $\leqslant r-1$, er σ_N polynomial af grad $\leqslant r$. Hvis $d \geqslant 0$, så har σ_N graden $d+1$. Hvis $d = -\infty$, så er kun endelig mange N_n forskellige fra 0, så når n er stor er $\sigma_N(n) = \operatorname{long} N$, jfr diskussionen i (1.8). I dette tilfælde, dvs når N har endelig længde som R-modul, er altså graden af σ_N lig med 0 når $N \neq 0$ og lig med $-\infty$ når $N = 0$. Bemærk, at vi (når $N \neq 0$) har følgende ligning for den akkumulerede funktion (med en konstant l):

$$\sum\nolimits_{i<n} \operatorname{long} N_i = e_d \binom{n}{d+1} + \cdots + e_0 \binom{n}{1} + l \quad \text{når } n \gg 0$$

(1.10) Sætning. *Antag, at N opfylder betingelserne i Sætning (1.7). Lad N' være en homogen undermodul i N, og lad $N'' = N/N'$ være den tilhørende kvotientmodul. Da vil også N' og N'' opfylde betingelserne, og for Hilbert-polynomierne gælder ligningen,*

$$\chi_N = \chi_{N'} + \chi_{N''}.$$

Bevis. Da G som nævnt er noethersk, er undermodulen N' endeligt frembragt, og trivielt er kvotienten N'' endeligt frembragt. For hvert n findes en eksakt følge,

$$0 \to N'_n \to N_n \to N''_n \to 0.$$

Specielt følger heraf, at N'_n og N''_n har endelig længde. Altså er betingelsen $(*)$ opfyldt for både N' og N''. Af den eksakte følge fås ligningen,

$$\lambda_N(n) = \lambda_{N'}(n) + \lambda_{N''}(n).$$

Differensfunktionen $\lambda_{N'} + \lambda_{N''} - \lambda_N$ er altså 0. Funktionerne λ stemmer for store værdier af n overens med de tilsvarende polynomier χ. Værdien i n af differenspolynomiet $\chi_{N'} + \chi_{N''} - \chi_N$ er altså lig med 0, når $n \gg 0$. Heraf følger, at differenspolynomiet er lig med 0 for alle n, hvormed den søgte ligning er bevist. ∎

(1.11) Bemærkning. Som nævnt (1.6) er betingelsen $(*)$ opfyldt, når ringen R selv har endelig længde. Den mest oplagte anvendelse er på polynomiumsringen $G = k[X_1, \dots, X_r]$, hvor $R = k$ er et legeme. Længden af en k-modul V er vektorrumsdimensionen, som vi betegner $\operatorname{rk} V$. Til enhver endeligt frembragt, gradueret G-modul N vil Hilbertpolynomiet χ_N altså opfylde, at $\operatorname{rk} N_n = \chi_N(n)$ for $n \gg 0$. Graden af χ_N og koefficienterne $e_0, \dots, e_d$ er invarianter for modulen N; de spiller en vigtig rolle i algebraisk geometri.

Betragt fx $N = G$. Her består N_n af de homogene polynomier af grad n. Monomierne af grad n er en k-basis, og der er $\binom{n+r-1}{r-1}$ sådanne polynomier (idet vi antager $r \geqslant 1$). Altså gælder ligningen,

$$\operatorname{rk} G_n = \binom{n+r-1}{r-1} \quad \text{for } n \geqslant 0.$$

Her er højresiden et polynomium af grad $r-1$, og dette polynomium er altså Hilbert polynomiet χ_G. Det er ikke svært at skrive dette polynomium som linearkombination af polynomierne $\binom{n}{i}$ for $i = 1, \dots, r-1$, og det er i hvert fald klart, at multipliciteten er $e_{r-1} = 1$.

Betragt videre et homogent polynomium f forskelligt fra 0, af grad h. Lad N være kvotienten G/Gf. Multiplikation med f giver da for alle n en eksakt følge,

$$0 \to G_{n-h} \xrightarrow{f} G_n \to N_n \to 0.$$

(Idet vi sætter $G_n := 0$ for $n < 0$.) Altså er $\lambda_N(n) = \lambda_G(n) - \lambda_G(n-h)$. For $n \geqslant h$ slutter vi, at $\lambda_N(n) = \chi_G(n) - \chi_G(n-h)$. Her er højresiden $\chi_G(n) - \chi_G(n-h)$ et polynomium for alle n, og dette polynomium er derfor Hilbert-polynomiet χ_N. Altså er

$$\chi_{G/fG}(n) = \binom{n+r-1}{r-1} - \binom{n-h+r-1}{r-1}.$$

Det er klart, at Hilbert-polynomiet $\chi_{G/fG}$ har grad $r-2$ (her antager vi at $r \geqslant 2$), og at multipliciteten er graden h af polynomiet f.

(1.12) Opgaver.

U9 **1.** Eftervis formlen $\binom{n+r}{p} = \sum_{i+j=p} \binom{n}{i}\binom{r}{j}$. [Vink: brug binomialformlen på $(1+x)^{n+r} = (1+x)^n(1+x)^r$.] Udtryk binomialkoefficienten $\binom{n+r}{r}$ som linearkombination af binomialkoefficienterne $\binom{n}{i}$ for $i = 0, 1, \dots, r$.

2. Samuel-Polynomium.

(2.1) Setup. Betragt en noethersk ring R, et ideal $\mathfrak{a}$ i R, og en endeligt frembragt R-modul M. *Rees-ringen* $\tilde{R}$ og *Rees-modulen* $\tilde{M}$ er de direkte summer,

$$\tilde{R} = R \oplus \mathfrak{a} \oplus \mathfrak{a}^2 \oplus \cdots ,$$
$$\tilde{M} = M \oplus \mathfrak{a}M \oplus \mathfrak{a}^2 M \oplus \cdots .$$

Rees-ringen $\tilde{R}$ er en gradueret ring. Det er bekvemt at tænke på den som delringen af polynomiumsringen $R[T]$ bestående af de polynomier, hvor koefficienten til T^i tilhører $\mathfrak{a}^i$ for alle i. Alternativt er $\tilde{R}$ frembragt som R-algebra af alle homogene førstegradspolynomier aT med $a \in \mathfrak{a}$. Hvis idealet $\mathfrak{a}$ er frembragt af r elementer, $\mathfrak{a} = (a_1, \dots, a_r)$, så er $\tilde{R}$ frembragt som R-algebra af elementerne $a_1T, \dots, a_rT$, der er homogene af grad 1. Når et sådant frembringersystem for $\mathfrak{a}$ er givet, kan vi opfatte $\tilde{R}$ som en kvotient af polynomiumsringen $G = R[X_1, \dots, X_r]$ modulo et homogent ideal.

Rees-modulen er en gradueret $\tilde{R}$-modul. Hvis (v_α) er et endeligt frembringersystem for M, så vil v_α'erne, opfattet som homogene elementer af grad 0 i $\tilde{M}_0 = M$, udgøre et frembringersystem for $\tilde{M}$ som $\tilde{R}$-modul.

Betragt nu undermodulen $\mathfrak{a}\tilde{M}$ i $\tilde{M}$. Elementerne i $\mathfrak{a}$ opfattes her som homogene skalarer af grad 0 i $\tilde{R}$, så $\mathfrak{a}\tilde{M}$ er den homogene undermodul,

$$\mathfrak{a}\tilde{M} = \mathfrak{a}M \oplus \mathfrak{a}^2 M \oplus \mathfrak{a}^3 M \oplus \cdots .$$

Kvotientmodulen $\tilde{M}/\mathfrak{a}\tilde{M}$ er derfor den graduerede modul,

$$\tilde{M}/\mathfrak{a}\tilde{M} = M/\mathfrak{a}M \oplus \mathfrak{a}M/\mathfrak{a}^2 M \oplus \mathfrak{a}^2 M/\mathfrak{a}^3 M \oplus \cdots .$$

Den betegnes også udførligt $\mathrm{Gr}_{\mathfrak{a}}(M)$. Da $\tilde{R}$-modulen $\tilde{M}$ er endeligt frembragt af v_α'erne, vil restklasserne af v_α'erne i $\mathrm{Gr}_{\mathfrak{a}}(M)_0 = M/\mathfrak{a}M$ være et $\tilde{R}$-frembringersystem for kvotienten $\mathrm{Gr}_{\mathfrak{a}}(M)$.

(2.2) Definition. Antag, at kvotienten $M/\mathfrak{a}M$ har endelig længde. Som bekendt har en R-modul endelig længde, hvis og kun hvis alle primidealer i støtten er maximalidealer. Støtten for M består af de primidealer, der omfatter annullatoren $\mathrm{Ann}\, M$, og støtten for $M/\mathfrak{a}M$ er delmængden heraf bestående af de primidealer, som desuden omfatter omfatter $\mathfrak{a}$. Antagelsen er altså, at alle sådanne primidealer, dvs alle primidealer der indeholder $\mathfrak{a} + \mathrm{Ann}\, M$, er maksimalidealer. Specielt er antagelsen opfyldt, hvis $R/\mathfrak{a}$ har endelig længde.

Det påstås, hvis vi opfatter $\tilde{R}$ som en kvotient af polynomiumsringen $G = R[X_1, \dots, X_r]$, så er betingelsen $(*)$ i (1.6), med $N := \mathrm{Gr}_{\mathfrak{a}}(M)$ som G-modul, opfyldt. Dette følger af, at N som nævnt er frembragt af de endelig mange restklasser i $N_0 = M/\mathfrak{a}M$ af v_α modulo $\mathfrak{a}M$, og N_0 har derfor ifølge antagelsen endelig længde. Af Sætning (1.7) fås derfor følgende:

Resultat. *For alle n har kvotienten $\mathfrak{a}^n M/\mathfrak{a}^{n+1}M$ endelig længde, og funktionen,*

$$n \mapsto \operatorname{long} \mathfrak{a}^n M/\mathfrak{a}^{n+1}M,$$

er polynomial af grad mindre end r, og dermed af grad mindre end det minimale antal elementer, der frembringer idealet $\mathfrak{a}$.

Betragt nu den akkumulerede sum af længderne $\sum_{i<n} \operatorname{long} \mathfrak{a}^i M/\mathfrak{a}^{i+1}M$, ligesom i Bemærkning (1.9). De enkelte moduler $\mathfrak{a}^i M/\mathfrak{a}^{i+1}M$ er de successive kvotienter i filtrationen af $M/\mathfrak{a}^n M$ defineret ved kæden,

$$\mathfrak{a}^n M \subseteq \cdots \subseteq \mathfrak{a}M \subseteq M.$$

Summen af længderne er derfor lig med længden af $M/\mathfrak{a}^n M$. Som bemærket i (1.9) fås derfor følgende:

Sætning. *For alle n har kvotienten $M/\mathfrak{a}^n M$ endelig længde, og funktionen,*

$$\sigma_{\mathfrak{a},M}(n) = \operatorname{long} M/\mathfrak{a}^n M,$$

er polynomial af grad mindre end eller lig med det minimale antal elementer, der frembringer idealet $\mathfrak{a}$.

Polynomiet hørende til den polynomiale funktion $\sigma = \sigma_{\mathfrak{a},M}$ kaldes *Hilbert-Samuel-polynomiet* eller blot *Samuel-polynomiet*, og vi vil betegne det $\chi_{\mathfrak{a},M}$. Graden af Samuel-polynomiet betegnes $d = d_{\mathfrak{a}}(M)$. Hvis $M = \mathfrak{a}M$, er øjensynlig $\sigma(n) = 0$ for alle n. I dette tilfælde er Samuel-polynomiet altså nul-polynomiet og $d = -\infty$. Antag, at $\mathfrak{a}M \subset M$. Funktionen $\sigma(n)$ er øjensynlig voksende, så det følger, at $\sigma(n) > 0$ for alle $n \geqslant 1$. Samuel-polynomiet er derfor ikke nul-polynomiet, og graden d er derfor større end eller lig med 0. Af Sætning (1.5) følger, at der findes $d+1$ hele tal $e_0, \dots, e_d$ således at

$$\operatorname{long} M/\mathfrak{a}^n M = e_d\binom{n}{d} + \cdots + e_1\binom{n}{1} + e_0 \quad \text{for } n \gg 0.$$

Med $e = e_{\mathfrak{a}}(M)$ betegnes koefficienten e_d. Den er positiv, idet polynomiet for $n \gg 0$ har ikke-negative værdier.

(2.3) Bemærkning. Antag, at $M/\mathfrak{a}M$ har endelig længde. Af resultaterne i (2.2) følger, at graden $d_{\mathfrak{a}}(M)$ er mindre end eller lig med det mindste antal elementer der frembringer idealet $\mathfrak{a}$. Modulen M er en modul over kvotientringen $\bar{R} := R/\operatorname{Ann} M$. Lad $\bar{\mathfrak{a}}$ betegne billedet af $\mathfrak{a}$ i kvotientringen $\bar{R}$. Det er klart, at længden af kvotienten $M/\mathfrak{a}^n M$, der definerer funktionen $\sigma_{\mathfrak{a},M}$, ikke ændres, hvis M opfattes som $\bar{R}$-modul og $\mathfrak{a}$ erstattes med $\bar{\mathfrak{a}}$. Heraf følger, at $d_{\mathfrak{a},M}$ er mindre end eller lig med det mindste antal elementer, der frembringer idealet $\bar{\mathfrak{a}}$ i $\bar{R}$.

(2.4) Eksempel. Betragt $R = \mathbb{Z}$, og lad $\mathfrak{a} = (a)$ være hovedidealet frembragt af et positivt helt tal a. Da er $\mathbb{Z}/(a)$ en endelig ring, og specielt af endelig længde, så resultatet i (2.2) kan anvendes på enhver endeligt frembragt kommutativ gruppe M. Da idealet er frembragt af ét element får Samuel-polynomiet $\chi_{(a),M}$ grad højst 1. Lad $a = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ være primopløsningen af a. Længden af $\mathbb{Z}/(a)$ er da summen $\alpha := \alpha_1 + \cdots + \alpha_t$, og mere generelt, længden af $\mathbb{Z}/(a)^n$ er lig med αn. Samuel-polynomiet $\chi_{(a),\mathbb{Z}}$ er altså førstegradspolynomiet αn, og $e_{(a)}(\mathbb{Z}) = \alpha$. Betragt videre en cyklisk gruppe $M = \mathbb{Z}/(q^\varepsilon)$, hvor q er et primtal. Hvis q er forskelligt fra p_i'erne, vil multiplikation med a være bijektiv på M. Er derimod q lig med et af p_i'erne, vil multiplikation med a^n på M være nul-afbildningen når $n \gg 0$. I det første tilfælde er long $M/a^n M = 0$ for alle n, så Samuel-polynomiet er nulpolynomiet. I det andet tilfælde er long $M/a^n M = \operatorname{long} M = \varepsilon$ når $n \gg 0$, så Samuel-polynomiet er det konstante polynomium ε.

(2.5) Sætning. *Antag, at $M/\mathfrak{a}M$ har endelig længde. Lad M' være en undermodul i M og lad $M'' = M/M'$ være den tilhørende kvotientmodul. Da har begge kvotienter $M'/\mathfrak{a}M'$ og $M''/\mathfrak{a}M''$ endelig længde. Videre gælder ligningen,*

$$d_{\mathfrak{a}}(M) = \max\{d_{\mathfrak{a}}(M'), d_{\mathfrak{a}}(M'')\}. \tag{2.5.1}$$

Endelig gælder, at funktionen,

$$\sigma_{\mathfrak{a},M'} + \sigma_{\mathfrak{a},M''} - \sigma_{\mathfrak{a},M}, \tag{2.5.2}$$

overalt er ikke-negativ, og den er polynomial af en grad, der er $\leqslant d_{\mathfrak{a}}(M') - 1$ og dermed $\leqslant d_{\mathfrak{a}}(M) - 1$.

Bevis. At $M/\mathfrak{a}M$ har endelig længde er som nævnt enbetydende med at alle primidealer, som omfatter $\mathfrak{a} + \operatorname{Ann} M$ er maksimalidealer. For både undermodulen M' og kvotientmodulen M'' gælder, at annullatoren omfatter Ann M. Heraf sluttes, at både $M'/\mathfrak{a}^n M'$ og $M''/\mathfrak{a}^n M''$ har endelig længde.

Funktionerne $\sigma_{M'}(n) = \operatorname{long} M'/\mathfrak{a}^n M'$ og $\sigma_{M''}(n) = \operatorname{long} M''/\mathfrak{a}^n M''$ er altså polynomiale. Lad d' og d'' betegne deres grader, og lad δ betegne funktionen i (2.5.2), altså

$$\delta(n) = \sigma_{M'}(n) + \sigma_{M''}(n) - \sigma_M(n). \tag{2.5.3}$$

Da er δ en polynomial funktion, idet de tre indgående funktioner σ i (2.5.2) er polynomiale. Nu findes som bekendt for hvert n en eksakt følge,

$$M'/\mathfrak{a}^n M' \to M/\mathfrak{a}^n M \to M''/\mathfrak{a}^n M'' \to 0.$$

Da homomorfien $M/\mathfrak{a}^n M \to M''/\mathfrak{a}^n M''$ er surjektiv, sluttes at $0 \leqslant \sigma_{M''}(n) \leqslant \sigma_M(n)$. Heraf ses, at der for graderne gælder uligheden $d'' \leqslant d$. I den eksakte følge er kernen for den første homomorfi undermodulen i $M'/\mathfrak{a}^n M'$ bestemt ved $K_n/\mathfrak{a}^n M'$, hvor

$$K_n := M' \cap \mathfrak{a}^n M.$$

Af den eksakte følge suppleret med denne kerne sluttes, at den alternerende sum af længderne af de indgående moduler er lig med 0. Denne relation kan skrives

$$\delta(n) = \sigma_{M'} + \sigma_{M''}(n) - \sigma_M(n) = \operatorname{long} K_n/\mathfrak{a}^n M'.$$

Heraf følger først, at $\delta(n) \geqslant 0$, som påstået. Øjensynlig er $\mathfrak{a}^n M' \subseteq K_n$. Af Artin–Rees' Lemma følger, at der findes et naturligt tal h, således at der for alle $n \geqslant h$ gælder $K_n \subseteq \mathfrak{a}^{n-h} M'$. For $n \geqslant h$ er altså

$$\mathfrak{a}^n M' \subseteq K_n \subseteq \mathfrak{a}^{n-h} M' \subseteq M',$$

og heraf fås uligheden,

$$\begin{aligned}\delta(n) &= \operatorname{long} K_n/\mathfrak{a}^n M' = \operatorname{long} M'/\mathfrak{a}^n M' - \operatorname{long} M'/K_n \\ &\leqslant \operatorname{long} M'/\mathfrak{a}^n M' - \operatorname{long} M'/\mathfrak{a}^{n-h} M' = \sigma_{M'}(n) - \sigma_{M'}(n-h).\end{aligned}$$

Da funktionen $\sigma_{M'}$ er polynomial af grad d' sluttes, at differensen $\sigma_{M'}(n) - \sigma_{M'}(n-h)$, som funktion af n, er polynomial af grad $d' - 1$. Denne differens majoriserer $\delta(n)$, og da $\delta(n) \geqslant 0$ følger det, at δ er polynomial af grad $\leqslant d' - 1$. Ligningen (2.5.3) er, når $n \gg 0$, en ligning mellem polynomier. Venstresiden har grad $\leqslant d' - 1$. Polynomierne på højresiden har grader d', d'' og d, og vi har vist, at $d'' \leqslant d$. Det ses, at ligningen kun kan være opfyldt, når $d = \max\{d', d''\}$ (og yderligere ses når $d \geqslant 0$, at koefficienterne e', e'' og e til d-tegradsleddene på højresiden må opfylde, at $e' + e'' = e$).

Hermed er sætningens påstande eftervist. ▯

(2.6) Korollar. *Antag, at $M/\mathfrak{a}M$ har endelig længde. Da gælder for enhver homomorfi $f\colon M \to M$, at differensen,*

$$\sigma_{\mathfrak{a},\operatorname{Coker} f} - \sigma_{\mathfrak{a},\operatorname{Ker} f},$$

er polynomial af grad $\leqslant d_{\mathfrak{a}}(M) - 1$. Specielt gælder, hvis homomorfien f er injektiv, at $d_{\mathfrak{a}}(\operatorname{Coker} f) \leqslant d_{\mathfrak{a}}(M) - 1$.

Bevis. Korollaret fås ved at anvende sætningens sidste del først med $M' := \operatorname{Ker} f$ og $M'' := f(M)$ og dernæst med $M' := f(M)$ og $M'' := \operatorname{Coker} f$. Korollarets sidste påstand er blot specialtilfældet, hvor $\operatorname{Ker} f = 0$. ▯

(2.7) Bemærkning. Antag, at $R/\mathfrak{a}$ har endelig længde. Sætningen kan da anvendes på enhver (endeligt frembragt) R-modul M, og specielt på $M = R$. Yderligere er

$$d_{\mathfrak{a}}(M) \leqslant d_{\mathfrak{a}}(R),$$

thi da M er endeligt frembragt, er M homomorft billede af en fri modul R^r, og gentagen anvendelse af Sætning (2.5) giver relationerne $d_{\mathfrak{a}}(M) \leqslant d_{\mathfrak{a}}(R^r) = d_{\mathfrak{a}}(R)$.

(2.8) Opgaver.
1. Bestem for $R = \mathbb{Z}$ og $\mathfrak{a} = (24)$ Hilbert–Samuel-polynomiet $\chi_{\mathfrak{a},M}$ for $M = \mathbb{Z}$. – Og for $M = \mathbb{Z}/9\mathbb{Z}$, og $M = \mathbb{Z}/10\mathbb{Z}$ og $M = \mathbb{Z}/11\mathbb{Z}$.

3. Op og ned.

(3.1) Cohen–Seidenberg's første Sætning. *Lad $R \to R'$ være en hel ringhomomorfi. Da gælder:*

(i) *Lad $\mathfrak{p}'$ være et primideal i R' og lad $\mathfrak{p} = R \cap \mathfrak{p}'$ betegne kontraktionen. Da er $\mathfrak{p}'$ et maksimalideal i R', hvis og kun hvis $\mathfrak{p}$ er et maksimalideal i R.*

(ii) *Lad $\mathfrak{p}'$ og $\mathfrak{q}'$ være primidealer i R' og lad $\mathfrak{p} = R \cap \mathfrak{p}'$ og $\mathfrak{q} = R \cap \mathfrak{q}'$ betegne kontraktionerne. Hvis $\mathfrak{q}' \subset \mathfrak{p}'$, så er $\mathfrak{q} \subset \mathfrak{p}$.*

(iii) ('Lying over') *Antag, at homomorfien $R \to R'$ er injektiv. Da findes for hvert primideal $\mathfrak{p}$ i R et primideal $\mathfrak{p}'$ i R' således at $R \cap \mathfrak{p}' = \mathfrak{p}$.*

(iv) ('Going up') *Lad $\mathfrak{a}'$ være et ideal i R' og lad $\mathfrak{a} = R \cap \mathfrak{a}'$ betegne kontraktionen. Lad der videre være givet et primideal $\mathfrak{p}$ i R med $\mathfrak{p} \supseteq \mathfrak{a}$. Da findes i R' et primideal $\mathfrak{p}'$ med $\mathfrak{p}' \supseteq \mathfrak{a}'$ og $R \cap \mathfrak{p}' = \mathfrak{p}$.*

Bevis. (i): Den sammensatte homomorfi $R \to R' \to R'/\mathfrak{p}'$ har kernen $\mathfrak{p}$, så kvotienten $R'/\mathfrak{p}'$ er altså hel over delringen $R/\mathfrak{p}$. Vi kan altså erstatte R' med integritetsområdet $R'/\mathfrak{p}'$ og R med delringen $R/\mathfrak{p}$ af det nye R'. Påstanden er så, at R' er et legeme, hvis og kun hvis R er et legeme. Denne påstand er velkendt.

(ii): Homomorfien $R \to R'$ inducerer en hel homomorfi $R_{\mathfrak{p}} \to R'_{\mathfrak{p}}$. Antag, at $\mathfrak{q}' \subset \mathfrak{p}'$. Disse to primidealer er da disjunkte med billedet af $R \setminus \mathfrak{p}$ i R', så ved lokaliseringen $R' \to R'_{\mathfrak{p}}$ svarer de til primidealer $\mathfrak{q}'R'_{\mathfrak{p}}$ og $\mathfrak{p}'R'_{\mathfrak{p}}$ i ringen $R'_{\mathfrak{p}}$. Det skal vises, at $\mathfrak{q} \subset \mathfrak{p}$, og ved eventuelt at erstatte R med $R_{\mathfrak{p}}$ ses, at det er nok at vise påstanden når $\mathfrak{p}$ er et maksimalideal. Nu følger påstanden af (i): Da $\mathfrak{q}' \subset \mathfrak{p}'$, er $\mathfrak{q}'$ ikke et maksimalideal i R'; følgelig er kontraktionen $\mathfrak{q}$ ikke et maksimalideal i R. Specielt er altså $\mathfrak{q} \neq \mathfrak{p}$, og dermed er $\mathfrak{q} \subset \mathfrak{p}$.

(iii): Antag, at $R \to R'$ er injektiv og at $\mathfrak{p}$ er et givet primideal. Den lokaliserede homomorfi $R_{\mathfrak{p}} \to R'_{\mathfrak{p}}$ er da ligeledes hel og injektiv. Specielt er $R'_{\mathfrak{p}}$ ikke nul-ringen, da den lokale ring $R_{\mathfrak{p}}$ ikke er nul-ringen. Lad $\mathfrak{m}$ være et maksimalideal i $R'_{\mathfrak{p}}$. Ifølge (i) er kontraktionen af $\mathfrak{m}$ til $R_{\mathfrak{p}}$ et maksimalideal, og da $R_{\mathfrak{p}}$ er lokal, må dette maksimalideal være $\mathfrak{p}R_{\mathfrak{p}}$. Heraf følger, at kontraktionen af $\mathfrak{m}$ til R er det givne primideal $\mathfrak{p}$. Kontraktionen af $\mathfrak{m}$ til R' er derfor et primideal i R', hvis kontraktion til R er lig med $\mathfrak{p}$.

(iv): Påstanden indses ved at anvende (iii) på homomorfien $R/\mathfrak{a} \hookrightarrow R'/\mathfrak{a}'$.

Hermed er de fire påstande eftervist. □

(3.2) Korollar. *Antag, at ringen R' er hel over en delring R. Da gælder ligheden for Krull-dimensionerne,*

$$\dim R' = \dim R.$$

Bevis. Det følger af (ii), at for en kæde af primidealer i R' med h skarpe inklusioner er kontraktionerne til R en kæde af primidealer med h skarpe inklusioner. Altså er $\dim R' \leqslant \dim R$. Lad der omvendt være givet en kæde af primidealer i R med h skarpe inklusioner,

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_h. \tag{1}$$

Det følger af (iii), at der i R' findes et primideal $\mathfrak{p}'_0$, hvis kontraktion til R er $\mathfrak{p}_0$. Ved gentagen anvendelse af (iv) følger nu, at der i R' findes en voksende kæde af primidealer, hvis kontraktioner er kæden (1). Heraf fås den omvendte ulighed $\dim R' \geqslant \dim R$. Altså gælder den påståede lighed. ▯

(3.3) Lemma. *Lad $R \to R'$ være en hel ringhomomorfi. Lad $\mathfrak{a}$ være et ideal i R, og betragt ekstensionen $\mathfrak{a}R'$. Hvert element α i $\mathfrak{a}R'$ er da rod i et normeret polynomium*

$$X^n + a_1X^{n-1} + \cdots + a_n, \qquad \text{hvor } a_i \in \mathfrak{a}^i \text{ for } i = 1, \dots, n.$$

Bevis. Et element α i $\mathfrak{a}R'$ kan skrives på formen $\alpha = a_1\xi_1 + \cdots + a_l\xi_l$, hvor $a_j \in \mathfrak{a}$ og $\xi_j \in R'$. Da R' er hel over R, er delringen $R[\xi_1, \dots, \xi_l]$ endeligt frembragt som R-modul. Lad $e_1, \dots, e_n$ være et frembringersystem for R-modulen $R[\xi_1, \dots, \xi_l]$. Elementet ξ_j tilhører modulen og modulen er en R-algebra. Multiplikation med ξ_j er derfor en R-lineær afbildning af modulen ind i sig selv. Følgelig findes en matrixligning,

$$\xi_j(e_1, \dots, e_n) = (e_1, \dots, e_n)A_j, \qquad (j)$$

hvor A_j er en matrix i $\mathrm{Mat}_n(R)$. Multiplicer ligningen (j) med a_j og læg sammen, for $j = 1, \dots, l$. Herved fås en matrixligning,

$$\alpha(e_1, \dots, e_n) = (e_1, \dots, e_n)A,$$

hvor $A = \sum a_jA_j$. Af denne matrixligning følger, via Cramer's formler, at α er rod i polynomiet $\det(X - A)$. Matricen A har øjensynlig koefficienter, der tilhører idealet $\mathfrak{a}$. Derfor har polynomiet $\det(X - A)$ den søgte form. ▯

(3.4) Normal ring. En ring R kaldes *normal*, hvis R er et integritetsområde og helt afsluttet i sit brøklegeme. Med andre ord: et integritetsområde R er normalt, når der for alle $a, s \in R$ og $s \neq 0$ gælder, at hvis brøken a/s er rod i et normeret polynomium med koefficienter i R, så er a/s element i R (dvs $a \in Rs$).

Det er velkendt, at en faktoriel ring er normal.

(3.5) Sætning. *Lad R' være et integritetsområde, og lad $R \subseteq R'$ være en normal delring. Lad α være et element i R'. Da er α hel over R, hvis og kun hvis α er algebraisk over R og det minimale polynomium for α over brøklegemet for R har koefficienter i R.*

Bevis. Lad K være brøklegemet for R. Elementet α er da algebraisk over R, hvis og kun hvis det er algebraisk over K; det minimale polynomium er i så fald den normerede frembringer for (hoved-)idealet i $K[X]$ bestående af polynomier, der har α som rod.

Det er klart, at et element α i R', som er helt over R også er algebraisk over R. I beviset kan vi altså antage, at α er algebraisk over R. Lad f betegne det minimale polynomium for α over K. Hvis f har alle koefficienter i R, så er α øjensynlig hel over R. Hermed er „hvis“ bevist.

Antag omvendt, at α er hel over R, altså at der findes et normeret polynomium $g \in R[X]$ med α som rod. I et passende legeme, som omfatter R', kan f som bekendt skrives som produkt af førstegradspolynomier,

$$f = (X - \alpha_1) \cdots (X - \alpha_n).$$

Da g har α som rod, er f divisor i g. Følgelig har g hvert α_i som rod. Altså er hvert α_i helt over R. Koefficienterne i f er summer af produkter af α_i'erne. Derfor er koefficienterne hele over R. Desuden tilhører de brøklegemet K for R. Da R var antaget normal, følger det at koefficienterne tilhører R. Hermed er også „kun hvis" bevist. ∎

(3.6) Cohen–Seidenberg's anden Sætning. *Lad der være givet et integritetsområde R', der er helt over en normal delring R. Da gælder:*

('Going down') *Lad $\mathfrak{p}'$ være et primideal i R' og lad $\mathfrak{p} = R \cap \mathfrak{p}'$ betegne kontraktionen. Lad der videre være givet et primideal $\mathfrak{q}$ i R med $\mathfrak{q} \subseteq \mathfrak{p}$. Da findes i R' et primideal $\mathfrak{q}'$ med $\mathfrak{q}' \subseteq \mathfrak{p}'$ og $R \cap \mathfrak{q}' = \mathfrak{q}$.*

Bevis. Betragt mængden $S = (R' \setminus \mathfrak{p}')(R \setminus \mathfrak{q})$, bestående af alle produkter σs, hvor $\sigma \in R' \setminus \mathfrak{p}'$ og $s \in R \setminus \mathfrak{q}$. Øjensynlig er S en multiplikativ delmængde i R', så vi kan betragte brøkringen $S^{-1}R'$ og ekstensionen $\mathfrak{q}S^{-1}R'$.

Det påstås, at det er nok at vise, at $\mathfrak{q}S^{-1}R'$ er et ægte ideal. Antag nemlig, at dette er vist. Da findes i $S^{-1}R'$ et primideal (fx et maksimalideal) som omfatter $\mathfrak{q}S^{-1}R'$. Dette primideal svarer ifølge Brøkprincippet til et primideal $\mathfrak{q}'$ i R', som er disjunkt med S, og øjensynlig er $\mathfrak{q}' \supseteq \mathfrak{q}R'$. Dette primideal $\mathfrak{q}'$ opfylder de stillede krav. Da $\mathfrak{q}'$ er disjunkt med S, er $\mathfrak{q}'$ nemlig specielt disjunkt med $R' \setminus \mathfrak{p}'$ og følgelig er $\mathfrak{q}' \subseteq \mathfrak{p}'$. Yderligere er $\mathfrak{q}'$ disjunkt med $R \setminus \mathfrak{q}$, så kontraktionen $R \cap \mathfrak{q}'$ er indeholdt i $\mathfrak{q}$. Da $\mathfrak{q}' \supseteq \mathfrak{q}R'$, må der altså gælde $R \cap \mathfrak{q}' = \mathfrak{q}$.

Det vises nu, at $\mathfrak{q}S^{-1}R' \subset S^{-1}R'$. Antag indirekte, at $\mathfrak{q}S^{-1}R' = S^{-1}R'$. Dette betyder som bekendt, at idealet $\mathfrak{q}R'$ ikke er disjunkt med S. Lad α være et element i fællesmængden. Vi har altså

$$\alpha = \sigma s, \text{ hvor } \sigma \in R' \setminus \mathfrak{p}' \text{ og } s \in R \setminus \mathfrak{q}, \quad \text{og } \alpha \in \mathfrak{q}R'. \tag{1}$$

Lad K være brøklegemet for R og lad f betegne det minimale polynomium for α over K. På den ene side er $\alpha = \sigma s$. Lad f_σ være det minimale polynomium for σ over K. Det følger af Sætning (3.5) at f_σ har koefficienter i R:

$$f_\sigma = X^m + c_1X^{m-1} + \cdots + c_m, \text{ hvor } c_i \in R \text{ for } i = 1, \ldots m. \tag{2}$$

Da $s \in R$, er det minimale polynomium f for $\alpha = \sigma s$ bestemt ved ligningen $f(X) = s^m f_\sigma(X/s)$, altså

$$f = X^m + sc_1X^{m-1} + \cdots + s^m c_m. \tag{3}$$

På den anden side er $\alpha \in \mathfrak{q}R'$. Det følger derfor af Lemma (3.3), at α er rod i polynomium

$$h = X^n + a_1X^{n-1} + \cdots + a_n, \text{ hvor } a_i \in \mathfrak{q} \text{ for } j = 1, \ldots, n. \tag{4}$$

Da h har α som rod, er det minimale polynomium f divisor i h. Der findes altså en ligning $h = gf$, og da f er normeret, er g's koefficienter i R. Modulo $\mathfrak{q}$ fås nu ligningen $\bar{h} = \bar{g}\bar{f}$ i $(R/\mathfrak{q})[X]$. Af (4) følger at $\bar{h} = X^n$. Det normerede polynomium $\bar{f}$ i $(R/\mathfrak{q})[X]$ er altså divisor i X^n. Heraf følger, da $R/\mathfrak{q}$ er et integritetsområde, at $\bar{f} = X^m$. Idet koefficienterne i f er bestemt ved (3) slutter vi, at $s^i c_i \in \mathfrak{q}$ for $i = 1, \ldots, m$. Da $s \notin \mathfrak{q}$ følger det videre, at

$$c_i \in \mathfrak{q} \text{ for } i = 1, \ldots, m.$$

Da σ er rod i f_σ gælder ligningen

$$\sigma^m = -\sigma^{m-1}c_1 - \cdots - c_m.$$

På højresiden er $c_i \in \mathfrak{q}$. Specielt er c_i derfor element i $\mathfrak{p}'$, og højresiden er derfor element i $\mathfrak{p}'$. Altså viser ligningen, at $\sigma^m \in \mathfrak{p}'$. Følgelig er $\sigma \in \mathfrak{p}'$. Hermed er den ønskede modstrid opnået, idet σ var antaget at tilhøre $R' \setminus \mathfrak{p}'$. $\square$

(3.7) Korollar. *Lad der være givet et integritetsområde R', der er helt over en normal delring R. Lad $\mathfrak{a}'$ være et ideal i R' og lad $\mathfrak{a} = R \cap \mathfrak{a}'$ betegne kontraktionen. Da er*

$$\operatorname{ht} \mathfrak{a}' = \operatorname{ht} \mathfrak{a}.$$

Bevis. Det følger af 'Going up', at hvert primideal, der omfatter $\mathfrak{a}$, er kontraktion af et primideal, der omfatter $\mathfrak{a}'$. Det er derfor nok at vise ligningen, når $\mathfrak{a}' = \mathfrak{p}'$ er et primideal.

Lad $\mathfrak{p} = R \cap \mathfrak{p}'$ betegne kontraktionen. Så følger uligheden $\operatorname{ht} \mathfrak{p}' \leqslant \operatorname{ht} \mathfrak{p}$ af Cohen-Seidenberg's første Sætning (3.1)(ii), og den modsatte ulighed følger af 'Going down'. $\square$

4. Homologi.

(4.1) Definition. Ved et *kompleks* forstås en uendelig nulfølge af moduler,

$$X: \qquad \cdots \longrightarrow X_{n+1} \xrightarrow{\partial_{n+1}} X_n \xrightarrow{\partial_n} X_{n-1} \longrightarrow \cdots .$$

Det er underforstået at følgen er uendelig i begge retninger, altså at n kan antage alle værdier i $\mathbb{Z}$. Homomorfierne ∂_n kaldes kompleksets *differentialer*. Da følgen er en nulfølge, er $\partial_n \partial_{n+1}$ nul-homomorfien fra X_{n+1} til X_{n-1}. Kort skrives: $\partial\partial = 0$.

Elementerne i X_n siges også at være *n-kæder* i komplekset. En n-kæde x kaldes en *n-cykel*, hvis den tilhører kernen for ∂_n, altså hvis $\partial x = 0$, og den kaldes en *n-rand*, hvis den tilhører billedet af ∂_{n+1}, altså hvis der findes en $(n+1)$-kæde y således at $x = \partial y$.

Undermodulen af n-cykler betegnes $Z_n = Z_n(X)$ og undermodulen af n-rande betegnes $B_n = B_n(X)$. Da $\partial\partial = 0$, er $B_n \subseteq Z_n$. Kvotientmodulen,

$$H_n(X) := Z_n/B_n,$$

kaldes kompleksets n'te *homologimodul*, og elementerne i H_n kaldes *homologiklasser*.

(4.2) Observation. Komplexet X er øjensynlig eksakt i X_n hvis og kun hvis $H_n(X) = 0$, og det er således et eksakt kompleks, hvis og kun hvis alle homologimodulerne er lig med nul.

(4.3) Bemærkning. Af definitionen på homologimodulerne for komplekset X fremgår, at vi har en eksakt følge,

$$0 \longrightarrow B_n \longrightarrow Z_n \longrightarrow H_n \longrightarrow 0.$$

Modulen Z_n er kernen for homomorfien ∂_n. Kokernen for homomorfien ∂_{n+1} betegnes Z_n^*, altså $Z_n^* = X_n/B_n$. Kvotientmodulen X_n/Z_n er ifølge Isomorfisætningen isomorf med billedet B_{n-1}. Modulerne $B_n \subseteq Z_n$ er undermoduler i X_n. Af Noether's anden Isomorfisætning fås derfor en eksakt følge,

$$0 \longrightarrow H_n \longrightarrow Z_n^* \longrightarrow B_{n-1} \longrightarrow 0.$$

Den surjektive homomorfi $Z_n^* \to B_{n-1}$ er induceret af ∂_n: et element i Z_n^* (dvs en klasse i X_n/B_n) repræsenteret ved n-kæden x afbildes på $\partial_n x$. Da B_{n-1} er indeholdt i Z_{n-1}, kan homomorfien $Z_n^* \to B_{n-1}$ opfattes som en homomorfi $Z_n^* \to Z_{n-1}$. Denne sidste homomorfi har stadig kernen H_n, og da dens billede er B_{n-1}, er dens kokerne H_{n-1}. Differentialet ∂_n inducerer således en eksakt følge,

$$0 \longrightarrow H_n \longrightarrow Z_n^* \longrightarrow Z_{n-1} \longrightarrow H_{n-1} \longrightarrow 0. \tag{4.3.1}$$

(4.4) Definition. Ved en *kompleks-homomorfi* $f\colon X' \to X$ mellem komplexer X' og X forstås en familie $f = (f_n)$ af homomorfier $f_n\colon X'_n \to X_n$, som kommuterer med differentialerne, dvs opfylder at $\partial f = f\partial$. Mere præcist kræves for alle n, at $f_{n-1}\partial_n = \partial_n f_n$, altså at følgende diagram er kommutativt:

$$\begin{tikzcd} X'_n \arrow[r, "\partial_n"] \arrow[d, "f_n"'] & X'_{n-1} \arrow[d, "f_{n-1}"'] \\ X_n \arrow[r, "\partial_n"] & X_{n-1}. \end{tikzcd}$$

En homomorfi $f\colon X' \to X$ afbilder øjensynlig $Z_n(X')$ ind i $Z_n(X)$ og $B_n(X')$ ind i $B_n(X)$; homomorfien inducerer altså en homomorfi mellem homologimodulerne,

$$H_n(X') \to H_n(X).$$

En følge bestående af to homomorfier mellem komplekser, $X' \to X \to X''$ kaldes *eksakt i* X, hvis der for alle n gælder, at følgen $X'_n \to X_n \to X''_n$ er eksakt i X_n.

(4.5) Sætning. *Lad* $0 \to X' \to X \to X'' \to 0$ *være en kort eksakt følge af komplekser. Da induceres naturligt en lang eksakt følge mellem homologimodulerne,*

$$H_n(X') \longrightarrow H_n(X) \longrightarrow H_n(X'') \xrightarrow{\delta} H_{n-1}(X') \longrightarrow H_{n-1}(X) \longrightarrow H_{n-1}(X'')\,.$$

Bevis. Vi har et kommutativt diagram med eksakte rækker:

$$\begin{tikzcd} 0 \arrow[r] & X'_{n+1} \arrow[r] \arrow[d, "\partial"'] & X_{n+1} \arrow[r] \arrow[d, "\partial"'] & X''_{n+1} \arrow[r] \arrow[d, "\partial"'] & 0 \\ 0 \arrow[r] & X'_n \arrow[r] & X_n \arrow[r] & X''_n \arrow[r] & 0. \end{tikzcd}$$

Af Slangelemma'et fås nu en eksakt følge mellem kokernerne: $Z'^{*}_n \to Z^{*}_n \to Z''^{*}_n \to 0$ og (af det tilsvarende diagram for $n-2$) en eksakt følge mellem kernerne: $0 \to Z'_{n-1} \to Z_{n-1} \to Z''_{n-1}$. Disse to eksakte følger indgår som rækker i diagrammet,

$$\begin{tikzcd} & Z'^{*}_n \arrow[r] \arrow[d] & Z^{*}_n \arrow[r] \arrow[d] & Z''^{*}_n \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & Z'_{n-1} \arrow[r] & Z_{n-1} \arrow[r] & Z''_{n-1}. \end{tikzcd}$$

I dette diagram er de lodrette pile homomorfierne beskrevet i (4.3). Det er let at se, at diagrammet er kommutativt. Den søgte eksakte følge er nu blot den eksakte følge mellem kerner og kokerner, der induceres af dette diagram ifølge Slangelemma'et. ∎

(4.6) Definition. Lad der være givet komplekser X' og X. Lad $s = (s_n)$ være en familie af homomorfier $s_n\colon X'_n \to X_{n+1}$. Betragt familien af homomorfier $f = (f_n)$, hvor $f_n = \partial_{n+1}s_n + s_{n-1}\partial_n$ (eller kort: $f = \partial s + s\partial$):

$$\begin{tikzcd} & X'_{n+1} \arrow[r] \arrow[dl] \arrow[d, dashed] & X'_n \arrow[r, "\partial_n"] \arrow[dl, "s_n"'] \arrow[d, dashed, "f_n"'] & X'_{n-1} \arrow[r] \arrow[dl, "s_{n-1}"'] \arrow[d, dashed] & X'_{n-2} \arrow[dl] \\ X_{n+2} \arrow[r] & X_{n+1} \arrow[r, "\partial_{n+1}"] & X_n \arrow[r] & X_{n-1} & \end{tikzcd}$$

(Bemærk, at ovenstående diagram ikke er kommutativt.) Familien f ses let at være en homomorfi af komplekser. En homomorfi af komplexer, der er af denne form med en passende familie $s = (s_n)$, siges også at være *nulhomotop*. To homomorfier $X' \to X$ siges at være *homotope*, hvis deres differens er nulhomotop.

(4.7) Lemma. *En homomorfi mellem komplekser $f\colon X' \to X$, som er nulhomotop, inducerer nul-homomorfien $H_n(X') \to H_n(X)$. To homomorfier $X' \to X$, som er homotope, inducerer den samme homomorfi $H_n(X') \to H_n(X)$.*

Bevis. Den sidste påstand er øjensynlig en konsekvens af den første. For at vise den første antages, at $f = \partial s + s\partial$ med en familie af homomorfier $s = (s_n)$. Den inducerede homomorfi $H_n(X') \to H_n(X)$ afbilder klassen repræsenteret ved n-cyklen x' på klassen repræsenteret ved billedet fx'. Da x' er en n-cykel er $\partial x' = 0$. Følgelig er $fx' = \partial s x' + s\partial x' = \partial s x'$. Altså er fx' en rand, og fx' repræsenterer derfor nulklassen i $H_n(X)$. $\square$

5. Cykler.

(5.1) Setup. I denne paragraf antages, at R er en noethersk ring. Videre betegner $\mathcal{P}$ en fast mængde af primidealer i R. Det antages, at der ikke findes inklusioner mellem primidealerne i $\mathcal{P}$.

(5.2) Definition. Den frie kommutative gruppe frembragt af primidealerne i $\mathcal{P}$ betegnes $\mathrm{Cyc}_{\mathcal{P}}(R) = \mathbb{Z}^{\oplus\mathcal{P}}$, og elementerne i denne gruppe kaldes $\mathcal{P}$-*cykler*. En $\mathcal{P}$-cykel $\mathfrak{z}$ er med andre ord en formel heltalslinearkombination,

$$\mathfrak{z} = \sum_{\mathfrak{p}\in\mathcal{P}} n_{\mathfrak{p}}.\mathfrak{p},$$

hvor koefficienterne $n_{\mathfrak{p}}$ tilhører $\mathbb{Z}$ og kun endelig mange er forskellige fra 0. Koefficienten $n_{\mathfrak{p}}$ i cyklen $\mathfrak{z}$ betegnes også $v_{\mathfrak{p}}(\mathfrak{z})$. For en cykel $\mathfrak{z}$ skrives $\mathfrak{z} \geqslant 0$, hvis $v_{\mathfrak{p}}(\mathfrak{z}) \geqslant 0$ for alle $\mathfrak{p}$ i $\mathcal{P}$. Summen af koefficienterne er cyklens *grad*, $\deg \mathfrak{z} = \sum n_{\mathfrak{p}}$.

(5.3) Definition. En R-modul M vil vi kalde en $\mathcal{P}$-*torsionsmodul*, hvis M er endeligt frembragt og hvis der for hvert primideal $\mathfrak{p}$ i $\mathcal{P}$ gælder, at modulen $M_{\mathfrak{p}}$ er af endelig længde over den lokale ring $R_{\mathfrak{p}}$. For en endeligt frembragt R-modul M, er $M_{\mathfrak{p}}$ kun forskellig fra 0 når $\mathfrak{p}$ ligger i støtten for M, og når $M_{\mathfrak{p}} \neq 0$, så er $M_{\mathfrak{p}}$ som bekendt af endelig længde, netop når $\mathfrak{p}$ er et minimalt primideal for M. For en endeligt frembragt modul betyder betingelsen altså at ethvert primideal i fællesmængden $\mathcal{P} \cap \mathrm{Supp}\, M$ er et minimalt primideal for M.

Lad M være en $\mathcal{P}$-torsionsmodul. Den til M hørende *fundamentale cykel*, $[M] = [M]_{\mathcal{P}}$, er da $\mathcal{P}$-cyklen,

$$[M] := \sum_{\mathfrak{p}\in\mathcal{P}} \operatorname{long} M_{\mathfrak{p}}.\mathfrak{p},$$

hvor altså $v_{\mathfrak{p}}[M] = \operatorname{long} M_{\mathfrak{p}}$. Koefficienten $\operatorname{long} M_{\mathfrak{p}}$ i summen er endelig for alle indices $\mathfrak{p}$, og den er kun forskellig fra 0 for endelig mange indices $\mathfrak{p}$, idet sådanne $\mathfrak{p}$'er findes blandt de endelig mange minimale primidealer for M. Altså er $[M]$ en veldefineret cykel.

(5.4) Observation. Hvert primideal $\mathfrak{p}$ i $\mathcal{P}$ definerer et element i $\mathrm{Cyc}_{\mathcal{P}}(R)$, nemlig cyklen $1.\mathfrak{p}$, hvor koefficienten til $\mathfrak{p}$ er lig med 1, og alle andre koefficienter er lig med nul. Bemærk, at $R/\mathfrak{p}$ er en $\mathcal{P}$-torsionsmodul og at

$$[R/\mathfrak{p}] = 1.\mathfrak{p}.$$

(5.5) Eksempel. (1) Lad $\mathcal{P}$ være mængden af samtlige maksimalidealer i R. I dette tilfælde består $\mathcal{P}$-torsionsmodulerne netop af modulerne af endelig længde. [Hvorfor?]. Bemærk, at for en modul M af endelig længde kan længden af M fås udfra cyklen $[M]$ som summen af koefficienterne, altså $\operatorname{long} M = \deg[M]$.

(2) Antag, at R er et integritetsområde. Lad $\mathcal{P}$ bestå af det ene primideal (0). Gruppen $\mathrm{Cyc}_{\mathcal{P}}(R)$ har da én frembringer, og den kan identificeres med $\mathbb{Z}$. Enhver endeligt frembragt R-modul er da en torsionsmodul, og cyklen $[M]$ kan, som et helt tal, identificeres med *rangen*

af M, dvs med rangen af $M_{(0)}$ (lokalisering i primidealet (0)) som vektorrum over brøklegemet for R.

(3) Antag, at R er et integritetsområde. Lad $\mathcal{P}$ bestå af samtlig primidealer af højde 1. En endeligt frembragt modul M er her en torsionsmodul, netop når $M_{(0)}$ er nul-modulen, altså netop når der til hvert element x i M findes et element $f \neq 0$ i R således at $fx = 0$. Det er denne egenskab, der normalt forbindes med torsionsmoduler. Da M forudsættes endeligt frembragt, er egenskaben ækvivalent med at der findes et element $f \neq 0$ i R, som annulllerer alle elementer i M. Bemærk, at hvis integritetsområdet antages at have dimension 1, så er torsionsmodulerne netop modulerne af endelig længde betragtet i (1).

(4) Lad d være givet, og lad $\mathcal{P}$ bestå af de primidelaler for hvilke $\dim R/\mathfrak{p} = d$. Ethvert primideal $\mathfrak{q}$ således at $\dim R/\mathfrak{q} \geqslant d$ vil øjensynlig være indeholdt i et primideal $\mathfrak{p}$ fra $\mathcal{P}$. Heraf ses, at en endeligt frembragt R-modul er en $\mathcal{P}$-torsionsmodul, hvis og kun hvis $\dim M \leqslant d$.

(5.6) Lemma. *Lad der være givet en eksakt følge af R-moduler,*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0.$$

Da er M en $\mathcal{P}$-torsionsmodul, hvis og kun hvis både M' og M'' er $\mathcal{P}$-torsionsmoduler. Er dette opfyldt, så gælder i $\operatorname{Cyc}_{\mathcal{P}}(R)$ ligningen,

$$[M] = [M'] + [M''].$$

Bevis. Da R er noethersk, er M endeligt frembragt, hvis og kun hvis M' og M'' begge er endeligt frembragte. Vi kan derfor i det følgende antage, at alle tre moduler er endeligt frembragte.

For hvert primideal $\mathfrak{p}$ i $\mathcal{P}$ fremkommer ved lokalisering i $\mathfrak{p}$ en eksakt følge af $R_{\mathfrak{p}}$-moduler,

$$0 \longrightarrow M'_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \longrightarrow M''_{\mathfrak{p}} \longrightarrow 0.$$

I denne følge har den midterste modul endelig længde, hvis og kun hvis de to yderste moduler har endelig længde. Heraf fremgår Lemma'ets første påstand. Antag, at de tre moduler er $\mathcal{P}$-torsionsmoduler. Den anførte ligningen mellem cykler er blot for hvert $\mathfrak{p} \in \mathcal{P}$ ligningen mellem koefficienterne, $\operatorname{long} M_{\mathfrak{p}} = \operatorname{long} M'_{\mathfrak{p}} + \operatorname{long} M''_{\mathfrak{p}}$, og denne ligning er velkendt. □

(5.7) Observation. Af Lemma'et følger på sædvanlig vis, at for en eksakt følge af $\mathcal{P}$-torsionsmoduler,

$$0 \longrightarrow M_n \longrightarrow M_{n-1} \longrightarrow \cdots \longrightarrow M_0 \longrightarrow 0,$$

gælder i $\operatorname{Cyc}_{\mathcal{P}}(R)$ ligningen $\sum_i (-1)^i [M_i] = 0$. Videre følger det for en endelig filtration i en $\mathcal{P}$-torsionsmodul M,

$$(0) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = M,$$

at $[M] = \sum_i [F_i/F_{i-1}]$.

(5.8) Definition. En homomorfi $u\colon M \to N$ mellem R-moduler siges at *have et $\mathcal{P}$-index*, hvis homomorfiens kerne og kokerne er $\mathcal{P}$-torsionsmoduler. I bekræftende fald defineres homomorfiens *index* $\chi(u)$ som $\mathcal{P}$-cyklen,

$$\chi(u) := [\operatorname{Coker} u] - [\operatorname{Ker} u].$$

(5.9) Observation. Hvis M og N er $\mathcal{P}$-torsionsmoduler, så har enhver homomorfi $u\colon M \to N$ et index, og $\chi(u) = [N] - [M]$. Dette fremgår af den eksakte følge $0 \longrightarrow \operatorname{Ker} u \longrightarrow M \longrightarrow N \longrightarrow \operatorname{Coker} u \longrightarrow 0$, jfr Lemma (5.6). Det følger specielt, at enhver endomorfi i en $\mathcal{P}$-torsionsmodul har index 0.

(5.10) Additivitet af Index. *Index af homomorfier er additivt i følgende forstand:* (1) *Lad der være givet homomorfier $M \xrightarrow{u} N$ og $N \xrightarrow{v} P$, og betragt den sammensatte homomorfi $M \xrightarrow{vu} P$. Hvis to af de tre homormofier u, v og vu har et index, så har også den tredie et index, og i bekræftende fald er $\chi(vu) = \chi(v) + \chi(u)$.*

(2) *Betragt et kommutativt diagram med eksakte rækker:*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle u'} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle u''} & & \\
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0.
\end{array}$$

Hvis to af de tre homormofier u', u og u'' har et index, så har også den tredie et index, og i bekræftende fald er $\chi(u) = \chi(u') + \chi(u'')$.

Bevis. Begge påstande følger af Lemma (5.6) ved at betragte de tilsvarende eksakte kerne-kokerne følger. □

(5.12) Bemærkning. Vi er normalt mest interesserede i endeligt frembragte moduler. Men det skal understreges, at en del af de foregående definitioner og resultater kan anvendes på vilkårlige moduler. I matematisk analyse optræder fx mellem vektorrum af uendelig dimension operatorer, hvor kernen og kokernen er endeligdimensionale (såkaldte Fredholm operatorer). Disse operatorer har altså et index svarende til Eksempel (5.5)(2) (eller (5.5)(1)).

Vi har valgt at lade betingelsen „endeligt frembragt“ indgå i definitionen af en $\mathcal{P}$-torsions-modul, men det kan generaliseres. Specielt fremhæves Eksempel 5(3) for et integritetsområde R: En R-modul M er en torsionsmodul, når lokaliseringen $M_{(0)} = 0$. I modsætning hertil er M *torsionsfri*, når homomorfien $M \to M_{(0)}$ er injektiv, dvs når ligningen $fx = 0$ for $x \in M$ og $f \neq 0$ i R medfører $x = 0$.

(5.13) Setup. I resten af denne paragraf antages, at R er et noethersk integritetsområde. Med K betegnes brøklegemet for R. Vi betragter gruppen af cykler $\operatorname{Cyc}(R)$ svarende til mængden af primidealer af højde 1 i R. De tilsvarende torsionsmoduler er da de endeligt frembragte R-moduler, som annulleres af et element forskelligt fra 0 i R. Cyklerne kaldes i øvrigt også *divisorer*.

Lad $f \neq 0$ være et element i R. For enhver endeligt frembragt modul M har endomorfien f_M (multiplikation med f på M) et index, idet kernen og kokernen for f_M annulleres af f. Af Additivitet af Index følger, når $f, g \neq 0$, at

$$\chi((fg)_M) = \chi(f_M) + \chi(g_M). \tag{5.13.1}$$

Hvis f er regulær på M, specielt hvis M er torsionsfri, er kernen for f_M lig med 0, så index $\chi(f_M)$ er lig med den fundamentale cykel $[M/fM]$.

(5.14) Sætning. *Antag, at R er et noethersk integritetsområde, og lad M være en endeligt frembragt R-modul. For hvert element $f \neq 0$ i R gælder da i* $\mathrm{Cyc}(R)$ *ligningen,*

$$\chi(f_M) = (\mathrm{rk}\, M)\,[R/fR]. \tag{5.14.1}$$

Specielt, hvis M desuden er torsionsfri, er $[M/fM] = (\mathrm{rk}\, M)[R/fR]$.

Bevis. Lad K være brøklegemet for R. Rangen $r = \mathrm{rk}\, M$ af M er som bekendt rangen af $M_{(0)}$ som vektorrum over K. Vælg så r elementer $e_1, \dots, e_r$ i M således at billederne i $M_{(0)}$ udgør en K-basis. Disse billeder er specielt lineært uafhængige over K, så elementerne $e_1, \dots, e_r$ er lineært uafhængige over R. De r elementer e_i bestemmer derfor en injektiv R-homomorfi $R^r \to M$. Lad Q betegne kokernen for denne homomorfi. Ifølge valget af elementerne bliver homomorfien en isomorfi efter lokalisering i primidealet (0). Heraf følger, at Q er en torsionsmodul. Af Additivitet af Index fås nu ligningen,

$$\chi(f_M) = \chi(f_{R^r}) + \chi(f_Q).$$

Da Q er en torsionsmodul, er $\chi(f_Q) = 0$. Yderligere følger det af additiviteten, at $\chi(f_{R^r}) = r\chi(f_R) = r[R/fR]$. Ligningen ovenfor medfører derfor, at $\chi(f_M) = r[R/fR]$. ∎

(5.15) Bemærkning. Vi viser en vigtig anvendelse af Formel (5.14.1) under antagelse af, at R er et noethersk integritetsområde af dimension 1. Cyklerne i Eksemplerne (5.5) (1) og (3) er da de samme, og de endeligt frembragte torsionsmoduler er netop modulerne af endelig længde.

(5.16) Lemma. *Under antagelsen i* (5.15) *gælder for enhver torsionsfri modul M af endelig rang, og hvert element $f \neq 0$ i R, at M/fM har endelig længde, med*

$$\mathrm{long}\, M/fM \leqslant (\mathrm{rk}\, M)\,\mathrm{long}\, R/fR. \tag{5.16.1}$$

Bevis. Hvis M er endeligt frembragt følger påstanden umiddelbart af formlen, endda med lighed i (5.16.1).

Betragt det almindelige tilfælde. For at vise, at en modul Q har endelig længde højst d, er det øjensynlig nok at vise, at der for enhver endeligt frembragt undermodul U af Q gælder $\mathrm{long}\, U \leqslant d$.

Enhver endeligt frembragt undermodul U af M/fM er billede ved homomorfien $M \to M/fM$ af en endeligt frembragt undermodul $M' \subset M$, og dermed også billede af M'/fM', og så er $\mathrm{long}\, U \leqslant \mathrm{long}\, M'/fM'$. Det er derfor nok at vise, med $d := (\mathrm{rk}\, M)\,\mathrm{long}\, M/fM$, at for hver endelig frembragt undermodul $M' \subset M$ er $\mathrm{long}\, M'/fM' \leqslant d$. Denne ulighed følger af den viste lighed $\mathrm{long}\, M' = (\mathrm{rk}\, M')\,\mathrm{long}\, R/fR$, idet $\mathrm{rk}\, M' \leqslant \mathrm{rk}\, M$. ∎

(5.17) Krull–Akizuki's sætning. *Antag, at R er et noethersk integritetsområde af dimension 1. Lad K betegne brøklegemet for R og lad K' være en endelig legemsudvidelse af K. Lad endelig R' være en delring af K' med $R \subseteq R'$. Da er R' noethersk af dimension $\leqslant 1$.*

Bevis. Det er nok at vise for hvert ideal $\mathfrak{a}' \neq 0$ i R', at $R'/\mathfrak{a}'$ har endelig længde.

Hertil vælges først et element $\alpha \neq 0$ i $\mathfrak{a}'$. Da K' specielt er algebraisk over K, er α rod i et polynomium i $F \in R[X]$ af positiv grad. Vi kan antage, at konstantleddet i F er forskelligt fra 0, og ligningen $F(\alpha) = 0$ kan så skrives:

$$f_n\alpha^n + \cdots + f_1\alpha = f \quad \text{hvor } f_i, f \in R, \quad f \neq 0.$$

Af ligningen følger, at $f \in R'\alpha$, hvoraf videre $f \in \mathfrak{a}'$. Idealet $\mathfrak{a}'$ indeholder altså et element $f \neq 0$ fra R. Så er $R'f \subseteq \mathfrak{a}'$, og dermed er $R'/\mathfrak{a}'$ en kvotient af $R'/R'f$. Det er alså nok at vise, at $R'/R'f$ har endelig længde som R'-modul. At denne længde er endelig, følger af Lemma (5.16): R'/fR' har endda endelig længde som R-modul. ▯

6. Klassegruppen.

(6.1) Setup. I denne paragraf antages, at R er et noethersk integritetsområde. Med K betegnes brøklegemet for R. Vi betragter gruppen af cykler $\mathrm{Cyc}(R)$ svarende til mængden af primidealer af højde 1 i R. De tilsvarende torsionsmoduler er da de endeligt frembragte R-moduler, som annulleres af et element forskelligt fra 0 i R.

Som i Notater 5 betegnes med $\chi(f_M)$, for $f \neq 0$ og en endelig frembragt R-modul M, index af multiplikationen $x \to fx$ i M. Af Additivitet af Index følger, når $f, g \neq 0$, at

$$\chi((fg)_M) = \chi(f_M) + \chi(g_M). \tag{6.1.1}$$

Hvis f er regulær på M, er kernen for f_M lig med 0, så index $\chi(f_M)$ er lig med den fundamentale cykel $[M/fM]$. Som bekendt gælder i $\mathrm{Cyc}(R)$ ligningen,

$$\chi(f_M) = (\mathrm{rk}\, M)\,[R/fR]. \tag{6.1.2}$$

(6.2) Definition. For hvert $f \neq 0$ i R sættes $\mathrm{div}(f) := \chi(f_R)$. Da R er et integritetsområde, er multiplikation med f injektiv, og følgelig er

$$\mathrm{div}(f) = [R/fR].$$

Koefficienten til $\mathfrak{p}$ i cyklen $\mathrm{div}(f)$, altså tallet $\mathrm{long}(R_\mathfrak{p}/fR_\mathfrak{p})$ for et primideal $\mathfrak{p}$ af højde 1, betegnes også $v_\mathfrak{p}(f)$.

Af ligning (6.1.1) følger specielt, at $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$. Derfor kan afbildningen $\mathrm{div}\colon R\backslash\{0\} \to \mathrm{Cyc}(R)$ udvides til en homomorfi af grupper,

$$\mathrm{div}\colon K^* \to \mathrm{Cyc}(R),$$

hvor K er brøklegemet for R. En brøk $\alpha = f/g$, hvor $f, g \neq 0$, afbildes herved på den *principale divisor* $\mathrm{div}(\alpha) = \mathrm{div}(f) - \mathrm{div}(g)$. Kokernen ved homomorfien, altså kvotienten af $\mathrm{Cyc}(R)$ modulo de principale divisorer, kaldes *klassegruppen* for R og betegnes $\mathrm{Cl}(R)$.

(6.3) Observation. Lad $f \neq 0$ være et element i R. Øjensynlig er $v_\mathfrak{p}(f) > 0$, hvis og kun hvis $f \in \mathfrak{p}$. Endvidere er $\mathrm{div}(f) = 0$, hvis og kun hvis $f \in R^*$. Hvis nemlig $f \neq 0$ ikke er en enhed, kan vi betragte et minimalt primideal $\mathfrak{p}$ for f. Ifølge Krull's Hovedidealsætning er $\mathfrak{p}$ af højde 1, og $v_\mathfrak{p}(f) > 0$.

Antag, at $R_\mathfrak{p}$ er en diskret valuationsring. Maksimalidealet $\mathfrak{p}R_\mathfrak{p}$ er da et hovedideal, frembragt af et element $p \in \mathfrak{p}$. Elementet p er et primelement i $R_\mathfrak{p}$, og hvert element forskelligt fra 0 i $R_\mathfrak{p}$ har en primopløsning εp^n, hvor ε er en enhed i $R_\mathfrak{p}$. Vektorrummet $R_\mathfrak{p} p^n/R_\mathfrak{p} p^{n+1}$ er af dimension 1 over restklasselegemet for $R_\mathfrak{p}$, så længden af $R_\mathfrak{p}/(p^n)$ er lig med n. Heraf ses, at tallet $v_\mathfrak{p}(f)$ angiver antallet af gange p forekommer i primopløsningen (inden for $R_\mathfrak{p}$) af f. Mere generelt kan hver brøk α i K^* skrives εp^n, hvor ε er en enhed i $R_\mathfrak{p}$ og $n \in \mathbb{Z}$, og vi finder $n = v_\mathfrak{p}(\alpha)$.

Hvis R er faktoriel, eller ækvivalent, hvis alle primidealer af højde 1 er hovedidealer, så får vi for hvert primelement p, at $v_p(f)$ er lig med antallet af gange p forekommer i primopløsningen af f. Divisoren $\mathrm{div}(f)$ er således blot en additiv skrivemåde for primopløsningen (modulo enheder) af f. Det følger specielt, at enhver divisor i $\mathrm{Cyc}(R)$ er principal. Klassegruppen for en faktoriel ring er altså lig med 0.

(6.4) Eksempel. Hvis en brøk $\alpha = f/g$ er hel over R, så er $\operatorname{div}(\alpha) \geqslant 0$. Da α er hel over R, er nemlig $M := R[\alpha]$ en endeligt frembragt R-modul. Da α tilhører brøklegemet, har denne modul rang 1. I M er multiplikation med α en R-lineær afbildning, og øjensynlig er $f_M = \alpha_M g_M$. Af Additivitet af Index følger derfor, at $\chi(f_M) = \chi(g_M) + \chi(\alpha_M)$. Under brug af Sætning (6.2) får vi derfor, at

$$\operatorname{div}(\alpha) = \chi(f_M) - \chi(g_M) = \chi(\alpha_M) = [M/\alpha M] \geqslant 0.$$

(6.5) Sætning. *Antag, at R er normal. For en brøk α i K^* er da $\operatorname{div}(\alpha) \geqslant 0$, hvis og kun hvis $\alpha \in R$. Videre gælder, at følgen,*

$$0 \longrightarrow R^* \longrightarrow K^* \xrightarrow{\operatorname{div}} \operatorname{Cyc}(R) \longrightarrow \operatorname{Cl}(R) \longrightarrow 0, \tag{6.5.1}$$

er eksakt. Endelig gælder for hvert primideal $\mathfrak{p}$ af højde 1, at $\mathfrak{p}$ er et hovedideal, hvis og kun hvis cyklen $1.\mathfrak{p}$ er principal.

Bevis. Hvis $\alpha \in R$, så er $\operatorname{div}(\alpha) = [R/R\alpha] \geqslant 0$.

Antag omvendt, at $\operatorname{div}(\alpha) \geqslant 0$. For et givet primideal $\mathfrak{p}$ af højde 1 er altså $v_\mathfrak{p}(\alpha) \geqslant 0$. Da R er normal, er også lokaliseringen $R_\mathfrak{p}$ normal. Yderligere er $R_\mathfrak{p}$ af dimension 1. Heraf følger som bekendt, at $R_\mathfrak{p}$ er en diskret valuationsring. Idet p er et element i $\mathfrak{p}$, som frembringer maksimalidealet $\mathfrak{p}R_\mathfrak{p}$, kan α skrives $\alpha = \varepsilon p^n$, hvor ε er en enhed i $R_\mathfrak{p}$ og $n = v_\mathfrak{p}(\alpha)$, jfr Observation (6.3). Af antagelsen følger derfor, at $n \geqslant 0$. Følgelig er $\alpha \in R_\mathfrak{p}$. Brøken α tilhører således $R_\mathfrak{p}$ for alle primidealer $\mathfrak{p}$ af højde 1. Heraf følger som bekendt, at α tilhører R.

Betragt følgen (6.5.1). Det er nok at vise, at hvis der for en brøk α i K^* gælder $\operatorname{div}(\alpha) = 0$, så er α element i R^*. Antag altså, at $\operatorname{div}(\alpha) = 0$. Da er specielt $\operatorname{div}(\alpha) \geqslant 0$, så af det lige viste følger at $\alpha \in R$. Når α er element i R, er det klart, at ligningen $\operatorname{div}(\alpha) = 0$ medfører, at $\alpha \in R^*$. Hermede er eksaktheden bevist.

Betragt endelig Sætningens sidste påstand. Hvis $\mathfrak{p}$ er et hovedideal, $\mathfrak{p} = Rp$, så er $1.\mathfrak{p} = [R/Rp] = \operatorname{div}(p)$ principal. Antag omvendt, at $1.\mathfrak{p}$ er principal, altså at $1.\mathfrak{p} = \operatorname{div}(p)$, hvor $p \in K^*$. Nu er specielt $\operatorname{div}(p) = 1.\mathfrak{p} \geqslant 0$, så af Sætningens første påstand følger, at $p \in R$.

Vi viser, at $\mathfrak{p} = Rp$. På den ene side er $v_\mathfrak{p}(p) = 1$, hvoraf det følger, at $p \in \mathfrak{p}$. Altså er $Rp \subseteq \mathfrak{p}$. Antag omvendt, at $f \in \mathfrak{p}$, $f \neq 0$. Vi har $\operatorname{div}(f) \geqslant 0$ og koefficienten $v_\mathfrak{p}(f)$ er positiv, da $f \in \mathfrak{p}$. Altså er $0 \leqslant \operatorname{div}(f) - 1.\mathfrak{p} = \operatorname{div}(f/p)$. Af Sætningens første påstand følger derfor, at $f/p \in R$, altså at $f \in Rp$. Hermed er den ønskede lighed $\mathfrak{p} = Rp$ bevist. □

(6.6) Sætning. *Lad $u\colon R^r \to R^r$ være en endomorfi. Da er følgende betingelser ækvivalente:*

(i) *Homorfien u har et index.*
(ii) *Homomorfien u er injektiv.*
(iii) *Determinanten $\det u$ er forskellig fra 0.*

Hvis disse betingelser er opfyldt, så gælder i $\operatorname{Cyc}(R)$ ligningen,

$$\chi(u) = [R^r/u(R^r)] = [R/(\det u)] = \operatorname{div}(\det u). \tag{6.6.1}$$

Bevis. Endomorfien u opfattes som en $r \times r$ matrix. Beviset for påstanden er i en række skridt, der hver for sig er lette:

(1) Af additivitet følger for et produkt af $r \times r$ matricer $w = vu$, at hvis påstanden gælder for to af matricerne u, v og w, så gælder påstanden også for den tredie.

(2) Det er klart, at betingelserne er opfyldt og (6.6.1) gælder, hvis u er en isomorfi. Videre gælder påstanden, hvis u er en diagonalmatrix; hvis diagonalelementerne er forskellige fra 0, så er betingelserne opfyldt, og (6.6.1) gælder.

(3) Ved hjælp af følgende operationer:

(a) addition til en række af en skalar gange en anden række; tilsvarende med søjler,
(b) multiplikation af en række med en skalar $f \neq 0$; tilsvarende med søjler,

kan den givne matrix overføres til en diagonalmatrix.

(4) Operationerne i (a) svarer til multiplikation (fra venstre eller fra højre) med en matrix, der afviger fra enhedsmatricen med et element g uden for diagonalen. Operationerne i (b) svarer til multiplikation (fra venstre eller fra højre) med en matrix, der afviger fra enhedsmatricen med et element f i diagonalen.

Ifølge (2) gælder påstanden for de matricer, der anvendes ved operationerne. Videre gælder påstanden for den matrix, der resulterer af u ved at anvende operationerne som i (3). Af (1) følger derfor, at påstanden gælder for u.

Hermed er Sætningen bevist. □

(6.7) Sætning. *Lad M være en endeligt frembragt R-modul. Lad r betegne rangen af M, og vælg en injektiv homomorfi $e\colon R^r \to M$. Klassen $c(M)$ i $\mathrm{Cl}(R)$, repræsenteret ved cyklen,*

$$\chi(e) = [M/e(R^r)],$$

er da uafhængig af valget af homorfien e. Yderligere gælder for en kort eksakt følge $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ af endeligt frembragte R-moduler, at $c(M) = c(M') + c(M'')$.

Bevis. Homorfien $e\colon R^r \to M$ er givet ved et sæt af r elementer $e_1, \dots, e_r$ i M, således at billederne i $M_{(0)}$ er en basis for $M_{(0)}$ som vektorrum over brøklegemet. De r elementer er altså specielt uafhængige over R, og der findes et element $f \neq 0$ i R, således fM er indeholdt i $Re_1 + \cdots + Re_r$. Kokernen for e er altså en torsionsmodul, så index $\chi(e)$ er defineret.

Lad $\hat{e}$ være et alternativt valg, svarende til r elementer $(\hat{e}_1, \dots, \hat{e}_r)$ i M. At $f\hat{e}_i \in Re_1 + \cdots + Re_r$ for $i = 1, \dots, r$ betyder, at der findes en matrixligning,

$$f(\hat{e}_1, \dots, \hat{e}_r) = (e_1, \dots, e_r)u,$$

hvor u er en $r \times r$ matrix. Denne ligning betyder, at følgende diagram af homomorfier er kommutativt:

$$\begin{tikzcd} R^r \arrow[r, "f"] \arrow[d, "u"'] & R^r \arrow[d, "\hat{e}"] \\ R^r \arrow[r, "e"] & M. \end{tikzcd}$$

Af Additivitet af Index følger nu, at $\chi(\hat{e}) + \chi(f_{R^r}) = \chi(e) + \chi(u)$. Af Sætning (6.6) følger nu videre, at

$$\chi(\hat{e}) - \chi(e) = \chi(u) - \chi(f_{R^r}) = \operatorname{div}(\det u) - \operatorname{div}(f^r)).$$

Differensen $\chi(\hat{e}) - \chi(e)$ er derfor en principal divisor, nemlig lig med divisoren for brøken $(\det u)/f^r$. Følgelig repræsenterer $\chi(\hat{e})$ og $\chi(e)$ den samme klasse i $\mathrm{Cl}(R)$.

Betragt nu den eksakte følge $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$. Lad r', r og r'' betegne rangene af de tre moduler. Vælg en injektiv homomorfi $e'\colon R^{r'} \to M'$ og en injektiv homomorfi $e''\colon R^{r''} \to M''$. Nu er $R^r = R^{r'} \oplus R^{r''}$, og vi kan betragte den homomorfi $e\colon R^r \to M$, som på $R^{r'}$ er lig med e' og som på $R^{r''}$ er en løftning af e''. Vi har da et kommutativt diagram med eksakte rækker:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & R^{r'} & \longrightarrow & R^r & \longrightarrow & R^{r''} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle e'} & & \downarrow{\scriptstyle e} & & \downarrow{\scriptstyle e''} & & \\
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0
\end{array}$$

Af Additivitet af Index følger, at $\chi(e) = \chi(e') + \chi(e'')$. Altså gælder i $\mathrm{Cl}(R)$, at $c(M) = c(M') + c(M'')$.

Hermed er Sætningens to påstande bevist. ▯

(6.8) Observation. For en endeligt frembragt torsionmodul M er klassen $c(M)$ lig med klassen repræsenteret af den fundamentale cykel $[M]$. Dette følger af at rangen r i Sætning (6.7) er lig med 0.

For en fri modul $M = R^r$ bliver klassen $c(M)$ lig med 0, idet vi i Sætning (6.7) kan vælge e som en isomorfi.

For en eksakt følge $0 \longrightarrow M_n \longrightarrow \cdots \longrightarrow M_0 \longrightarrow 0$ af endeligt frembragte R-moduler følger det af additiviteten i Sætning (6.7), at $\sum_i (-1)^i c(M_i) = 0$. Specielt følger heraf, at hvis en modul M har en endelig fri resolution, dvs hvis der findes en eksakt følge,

$$0 \longrightarrow F_n \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M \longrightarrow 0,$$

hvor hvert F_i er en (endeligt frembragt) fri modul, så er $c(M) = 0$.

(6.9) Korollar. *Antag, at R er normal. Lad $\mathfrak{p}$ være et primideal af højde 1. Da er $\mathfrak{p}$ et hovedideal, hvis og kun hvis kvotienten $R/\mathfrak{p}$ har en endelig fri resolution.*

Bevis. Hvis $\mathfrak{p}$ er et hovedideal, $\mathfrak{p} = Rp$, så er følgen $0 \to R \xrightarrow{p} R \to R/\mathfrak{p} \longrightarrow 0$ en endelig fri resolution af $R/\mathfrak{p}$.

Antag omvendt, at $R/\mathfrak{p}$ har en endelig fri resolution. Cyklen $1.\mathfrak{p}$ er fundamentalcyklen $[R/\mathfrak{p}]$, så den repræsenterer klassen $c(R/\mathfrak{p})$. Som nævnt i Observation (6.8) følger det af antagelsen, at klassen $c(R/\mathfrak{p})$ er lig med 0. Altså er cyklen $1.\mathfrak{p}$ principal. Af Sætning (6.5) følger nu, at $\mathfrak{p}$ er et hovedideal. ▯

(6.10) Bemærkning. Lad R være en regulær lokal (noethersk) ring. Som bekendt er R da et normalt integritetsområde. Man kan vise, at regularitet er ensbetydende med at enhver endeligt frembragt R-modul har en endelig fri resolution. Af Korollar (6.9) følger derfor, at ethvert primideal af højde 1 er et hovedideal. Altså er R en faktoriel ring. En regulær lokal ring er derfor faktoriel (Auslander–Buchsbaum's sætning).

7. Kompletion.

(7.1) Setup. Betragt en kommutativ gruppe M med en uendelig filtration med undergrupper,

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots .$$

Lad $G(M) := \bigoplus M_n/M_{n+1}$ være den tilhørende graduerede gruppe. For et element x af *orden* n i M, dvs således at $x \in M_n \setminus M_{n+1}$, defineres *formen* x^* som restklassen af x modulo M_{n+1}. Formen er homogen af grad n i $G(M)$.

(7.2). Vis, at der findes en pseudo-metrik i M, således at to elementer x, y i M har lille afstand netop når differensen $x - y$ tilhører M_n for en stor værdi af n. Vis, at M er et Hausdorff rum, hvis og kun hvis $\bigcap_n M_n = (0)$.

(7.3). Gruppen M kaldes *fuldstændig*, når M er Hausdorff og enhver fundamentalfølge er konvergent. Vis, at den sidste betingelse er ækvivalent med at enhver uendelig række $\sum x_n$, hvor $x_n \to 0$ for $n \to \infty$, er konvergent.

(7.4). Lad $\widehat{M}$ betegne mængden af alle følger $\xi = (\xi^{(1)}, \xi^{(2)}, \dots)$, hvor $\xi^{(n)} \in M/M_n$ og $\xi^{(n+1)} \mapsto \xi^{(n)}$ ved den kanoniske homomorfi $M/M_{n+1} \to M/M_n$. Øjensynlig er $\widehat{M}$ en kommutativ gruppe. Den filtreres ved at $\widehat{M}_n$ defineres som kernen for homomorfien $\xi \mapsto \xi^{(n)}$. Vis, denne homomorfi er surjektiv, og slut, at $\widehat{M}/\widehat{M}_n = M/M_n$ og at $G(\widehat{M}) = G(M)$. Definér en kanonisk homomorfi $x \mapsto \widehat{x}$ af M ind i $\widehat{M}$ og vis, at $\widehat{M}$ er *kompletionen* af M.

(7.5). Ifølge konstruktionen er $\widehat{M}$ en delmængde af produktet $\prod M/M_n$. Denne delmængde af produktet kaldes i øvrigt den projektive limes, og den betegnes også $\varprojlim M/M_n$. Vis, idet de enkelte faktorer forsynes med den diskrete topologi og produktet med produkttoplogien, at $\widehat{M}$ er en afsluttet delmængde og at toplogien på $\widehat{M}$ defineret ved filtrationen er lig med den inducerede topologi.

(7.6) Setup. Antag i det følgende, at M er en modul over en given ring A, og at der i A er givet en filtration,

$$A = \mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots .$$

Det antages, for alle i og j, at

$$\mathfrak{a}_i \mathfrak{a}_j \subseteq \mathfrak{a}_{i+j} \quad \text{og} \quad \mathfrak{a}_i M_j \subseteq M_{i+j}.$$

Specielt er altså $\mathfrak{a}_n$ et ideal i A og M_n en undermodul af M. Øjensynlig er så $G(A)$ en gradueret ring og $G(M)$ er en gradueret $G(A)$-modul.

(7.7) Sætning. *Antag, at A er fuldstændig og at M er Hausdorff. Lad $N \subseteq M$ være en undermodul, og lad N^* være $G(A)$-undermodulen af $G(M)$ frembragt af alle former x^*, hvor $x \in N$. Antag, at der er givet endelig mange elementer e_j i N, således at formerne e_j^* frembringer N^*. Da vil e_j'erne frembringe N.*

Bevis. Beviset overlades til læseren. ∎

(7.8). Vis, at med koordinatvise kompositioner er $\widehat{A}$ en ring og $\widehat{M}$ en $\widehat{A}$-modul. Vis, at hvis $A/\mathfrak{a}_1$ er en lokal ring, så er $\widehat{A}$ en lokal ring. [Vink: af antagelserne følger specielt, at $\mathfrak{a}_1^n \subseteq \mathfrak{a}_n$. Når $A/\mathfrak{a}_1$ er lokal, så er derfor også $A/\mathfrak{a}_n$ lokal, og et element i $A/\mathfrak{a}_n$ er invertibelt, når blot dets billede i $A/\mathfrak{a}_1$ er invertibelt.]

(7.9) Setup. I det følgende antages, at A er en noethersk ring og at filtrationerne er de $\mathfrak{a}$-*adiske* svarende til et givet ideal $\mathfrak{a}$ i A, dvs $\mathfrak{a}_i = \mathfrak{a}^i$ og $M_i = \mathfrak{a}^i M$.

(7.10). Vis, at $\widehat{A}$ er noethersk ring. Antag, at M er frembragt af endelig mange elementer e_j. Vis (mere generelt), at $\widehat{M}$ er frembragt af de endelig mange elementer $\widehat{e_j}$ og at enhver $\widehat{A}$-undermodul af $\widehat{M}$ er endeligt frembragt. [Vink: udnyt, at $G(A)$ er noethersk og at $G(M)$ er en endeligt frembragt $G(A)$-modul, og brug Sætning (7.7).] Vis, at filtrationen i $\widehat{M}$ er den $\mathfrak{a}$-adiske, dvs $\widehat{M}_n = \mathfrak{a}^n \widehat{M}$. Specielt er filtrationen også lig med den $\widehat{\mathfrak{a}}$-adiske, hvor $\widehat{\mathfrak{a}} := \widehat{A}_1$.

(7.11). Betragt en eksakt følge $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ af A-moduler. Vis, at der induceres en eksakt følge $\widehat{M'} \longrightarrow \widehat{M} \longrightarrow \widehat{M''} \longrightarrow 0$.

Antag, at M er endeligt frembragt. Vis, at den $\mathfrak{a}$-adiske topologi på M' er lig med delrumstopologien induceret af den $\mathfrak{a}$-adiske topologi på M. Vis, at $\widehat{M'} \longrightarrow \widehat{M}$ er injektiv.

(7.12). Antag, at $\mathfrak{a}$ er $\mathfrak{m}$-primært, hvor $\mathfrak{m}$ er et maksimalideal i A. Vis, at den $\mathfrak{a}$-adiske topologi er lig med den $\mathfrak{m}$-adiske. Vis, at kompletionen $\widehat{A}$ er en lokal ring og at idealet $\widehat{\mathfrak{a}}$ er primært. Vis, at $\widehat{A}$ også fås ved at komplettere den lokale ring $A_{\mathfrak{m}}$ mht maksimalidealet $\mathfrak{m}A_{\mathfrak{m}}$.

(7.13). Antag, at A er lokal og at $\mathfrak{a}$ er maksimalidealet. Vis, at ringene A og $\widehat{A}$ har samme Samuelpolynomium (og specielt samme dimension). Vis, at A er regulær, hvis og kun hvis $\widehat{A}$ er regulær. [Vink: $G(A) = G(\widehat{A})$.]

(7.14). Vis, at når $A = k[X_1, \dots, X_n]$ er polynomiumsringen over et legeme k og $\mathfrak{a} = (X_1, \dots, X_n)$, så er $\widehat{A}$ lig med potensrækkeringen $k[[X_1, \dots, X_n]]$. Potensrækkeringen er altså en lokal noethersk ring, regulær af dimension n.

(7.15). Antag, at R er en lokal noethersk ring med maksimalidealet $\mathfrak{m}$ og at R indeholder et legeme k således at restklasselegemet $R/\mathfrak{m}$ er af endelig dimension over k. Antag, at $\mathfrak{q}$ er er $\mathfrak{m}$-primært ideal i R, frembragt at elementer $(x_1, \dots, x_n)$. Vis, at $R/\mathfrak{q}$ er af endelig dimension over k. Vælg et endeligt k-frembringersystem e_j for $R/\mathfrak{q}$. Lad nu A være polynomiumsringen $A := k[X_1, \dots, X_n]$ og $\mathfrak{a} = (X_1, \dots, X_n)$. Betragt R som modul over A via homomorfien $A \to R$ bestemt ved x_i'erne. Vis, at den $\mathfrak{a}$-adiske topologi på R er lig med den $\mathfrak{m}$-adiske. Vis, at elementerne $\widehat{e_j}$ frembringer $\widehat{R}$ som $\widehat{A}$-modul.

Kompletionen $\widehat{A}$ er potensrækkeringen $k[[X_1, \dots, X_n]]$. Vis, at hvis $(x_1, \dots, x_n)$ er et parametersystem, så er homomorfien $\widehat{A} \to \widehat{R}$ injektiv. [Vink: $\widehat{R}$ er hel over billedet, $\widehat{R}$ og $\widehat{A}$ har samme dimension, og $\widehat{A}$ er et integritetsområde.]

Antag yderligere, at $k = R/\mathfrak{m}$. Vis, at hvis $(x_1, \dots, x_n)$ frembringer $\mathfrak{m}$, så er $\widehat{A} \to \widehat{R}$ surjektiv. Vis, at hvis $(x_1, \dots, x_n)$ er et regulært parametersystem i R, så er

$$k[[X_1, \dots, X_n]] = \widehat{R}.$$

(7.16). Ringen, der fås ved at komplettere $\mathbb{Z}$ mht maksimalidealet (p) frembragt af et primtal p, kaldes ringen af hele p-adiske tal og betegnes $\widehat{\mathbb{Z}}_p$. Vis, at $\widehat{\mathbb{Z}}_p$ er en diskret valuationsring (og specielt et integritetsområde). Brøklegemet for $\widehat{\mathbb{Z}}_p$ kaldes legemet af p-adiske tal og betegnes $\mathbb{Q}_p$. Vis, at $\widehat{\mathbb{Z}}_p$ er kompakt. [Vink: brug Tychonoff's sætning.]

8. Valuationsringe.

(8.1) Definition. I dette afsnit betragtes (kommutative) ringe, der ikke nødvendigvis er noetherske. Hvis V er en lokal ring, betegnes med $\mathfrak{m}(V)$ maksimalidealet i V. Hvis V og V' er delringe af en ring K, siges V' at *dominere* V, og vi skriver $V' \succeq V$, hvis $V' \supseteq V$ og $\mathfrak{m}(V') \supseteq \mathfrak{m}(V)$.

(8.2) Observation. De ringe vi betragter vil typisk være delringe af et legeme K. For enhver delring R af K og enhver multiplikativ delmængde S af R, hvor $0 \notin S$, vil da også brøkringen $S^{-1}R$ være delring af K. Lad $R \subseteq R'$ være delringe af K, lad $\mathfrak{p}'$ være et primideal i R' og lad $\mathfrak{p} := R \cap \mathfrak{p}'$ være kontraktionen. Da er øjensynlig $R_\mathfrak{p} \preceq R'_{\mathfrak{p}'}$.

(8.3) Sætning. *Lad K være et legeme, lad $R \subseteq K$ være en delring, og lad α være element i K.*

(1) *Antag, at α er hel over R. For hvert primideal $\mathfrak{p}$ i R findes da en lokal delring V af K, således at $V \succeq R_\mathfrak{p}$ og $\alpha \in V$.*
(2) *Antag, at α ikke er hel over R. Da findes et maksimalideal $\mathfrak{p}$ i R og en lokal delring V af K, således at $V \succeq R_\mathfrak{p}$ og $\alpha^{-1} \in \mathfrak{m}(V)$.*

Bevis. (1) Da α er hel over R, er delalgebraen $R' := R[\alpha]$ hel over R. Af 'Lying over sætningen' følger derfor, at der findes et primideal $\mathfrak{p}'$ i R' således at $\mathfrak{p} = R \cap \mathfrak{p}'$. Den lokale ring $V := R'_{\mathfrak{p}'}$ vil så opfylde det stillede krav.

(2) Antag, at α ikke er hel over R. Betragt delmængden $\mathfrak{a}$ af R bestående af de elementer $r \in R$ for hvilke der findes en relation,

$$r\alpha^n + r_1\alpha^{n-1} + \cdots + r_n = 0 \quad \text{med } r_i \in R. \tag{*}$$

Øjensynlig er $\mathfrak{a}$ et ideal i R, og da α ikke er hel over R er $\mathfrak{a}$ et ægte ideal i R. Der findes derfor et maksimalideal $\mathfrak{p}$ i R, således at $\mathfrak{a} \subseteq \mathfrak{p}$. Betragt nu delalgebraen $R' := R[\alpha^{-1}]$, og heri idealet $R'\mathfrak{p} + R'\alpha^{-1}$. Dette ideal er et ægte ideal i R'. Antag nemlig, indirekte, at der findes en fremstilling $1 = \beta + \gamma\alpha^{-1}$, hvor $\beta \in R'\mathfrak{p}$ og $\gamma \in R'$. Elementerne i R' har formen $f(\alpha)/\alpha^n$, hvor $f \in R[X]$ er et polynomium af grad højst n. Af en fremstilling $1 = \beta + \gamma\alpha^{-1}$ ville vi derfor kunne udlede en relation (*) med r af formen $r = 1 - p$, hvor $p \in \mathfrak{p}$, og dette er i modstrid med at $r \in \mathfrak{a} \subseteq \mathfrak{p}$ og $\mathfrak{p} \subset R$.

Da idealet $R'\mathfrak{p} + R'\alpha^{-1}$ er et ægte ideal i R', er det indeholdt i et maksimalideal $\mathfrak{p}'$. Den lokale ring $V := R'_{\mathfrak{p}'}$ vil så opfylde det stillede krav. □

(8.4) Definition. En ring V kaldes en *valuationsring*, hvis V er et integritetsområde og idealerne i V er totalt ordnede ved inklusion. I en valuationsring er øjensynlig foreningsmængden af alle ægte idealer igen et (ægte) ideal. Følgelig er en valuationsring en lokal ring.

(8.5) Korollar. *Antag, at V er delring af et legeme K. Da er følgende fire betingelser ækvivalente:*

(i) *V er en valuationsring med K som brøklegeme.*

(ii) *Hovedidealerne i V er totalt ordnede ved inklusion og K er brøklegemet for V.*
(iii) *For alle $\alpha \in K^*$ er $\alpha \in V$ eller $\alpha^{-1} \in V$.*
(iv) *V er maksimal (mht dominans) blandt de lokale delringe af K.*

Hvis betingelserne er opfyldt, så er $\mathfrak{m}(V) = \{\alpha \in K \mid \alpha^{-1} \notin V\}$, og yderligere gælder, at V er normal.

Bevis. Antag, at hovedidealerne i V er totalt ordnede, og lad $\mathfrak{a}$ og $\mathfrak{b}$ være idealer i V, således at $\mathfrak{b} \not\subseteq \mathfrak{a}$. Vælg $b \in \mathfrak{b} \setminus \mathfrak{a}$. Lad $a \in \mathfrak{a}$. Da $b \notin \mathfrak{a}$, er det udelukket, at $Vb \subseteq Va$. Af antagelsen følger derfor, at $Va \subseteq Vb \subseteq \mathfrak{b}$. Altså er $\mathfrak{a} \subseteq \mathfrak{b}$. Følgelig er V en valuationsring.

Heraf ses, at betingelserne (i) og (ii) ækvivalente. De er klart ækvivalente med (iii), idet vi for en brøk $\alpha = a/b$ i brøklegemet for V har $\alpha \in V$, hvis og kun hvis $Va \subseteq Vb$.

Når betingelsen (iii) er opfyldt, så gælder den anførte beskrivelse af maksimalidealet $\mathfrak{m}(V)$, idet komplementærmængden $V \setminus \mathfrak{m}(V)$ består af enhederne i V. Af denne beskrivelse følger også, at V er maksimal. Antag nemlig, at $V \preceq V'$, og betragt et element $\alpha \neq 0$ i V'. Da $\mathfrak{m}(V')$ er et ægte ideal i V', sluttes at $\alpha^{-1} \notin \mathfrak{m}(V')$. Da $\mathfrak{m}(V) \subseteq \mathfrak{m}(V')$, følger det, at $\alpha^{-1} \notin \mathfrak{m}(V)$. Af beskrivelsen af $\mathfrak{m}(V)$ fås nu, at $\alpha \in V$.

Vi mangler at vise, at betingelsen (iv) medfører (iii) og at V er normal. Antag altså, at V er maksimal mht dominans, og lad α være et element i K^*. Hvis α er hel over V, anvendes Sætning (8.3)(1) med $\mathfrak{p} := \mathfrak{m}(V)$. Af maksimaliteten af V følger så, at $\alpha \in V$. Specielt følger det, at V er normal. Hvis α ikke er hel over V anvendes Sætning (8.3)(2). Da V er lokal, er maksimalidealet $\mathfrak{p}$ nødvendigvis lig med $\mathfrak{m}(V)$, og maksimaliteten af V sikrer, at $\alpha^{-1} \in \mathfrak{m}(V)$. Altså er betingelsen (iii) opfyldt.

Hermed er Korollaret bevist. □

(8.6) Korollar. *Lad K være et legeme. Enhver lokal delring af K domineres da af en valuationsring med K som brøklegeme. Yderligere gælder for enhver delring R af K, at den hele afslutning af R i K er lig med fællesmængden af de valuationsringe, der omfatter R og har K som brøklegeme.*

Bevis. Det er let at se, at de lokale delringe af K, ordnet ved dominans, udgør en induktivt ordnet mængde. Af Zorn's Lemma og Korollar (8.5) følger derfor den første påstand.

Lad R være en delring af K, og lad R' være den hele afslutning af R i K. Det følger af den sidste påstand i Korollar (8.5), at enhver valuationsring V, der har K som brøklegeme og omfatter R, vil omfatte R'. Altså er R' indeholdt i den anførte fællesmængde.

For at vise den omvendte inklusion betragtes et element α i K^* som ikke tilhører R'. Af Sætning (8.3)(2) følger så, at der findes en lokal delring W af K, således at $W \supseteq R$ og $\alpha^{-1} \in \mathfrak{m}(W)$. Ifølge den første påstand domineres W af en valuationsring V med K som brøklegeme. Da $V \succeq W$, er $\alpha^{-1} \in \mathfrak{m}(V)$. Følgelig er $\alpha \notin V$. Elementet α tilhører derfor ikke den anførte fællesmængde.

Hermed er vist, at R' er lig med den anførte fællesmængde, hvormed beviset er fuldført. □

(8.7) Bemærkning. Et legeme er naturligvis en valuationsring. Som bekendt gælder, at en noethersk valuationsring er et hovedidealområde. En noethersk valuationsring, der ikke er et legeme, kan som bekendt karakteriseres som en (noethersk) regulær lokal ring af dimension 1 (en *diskret valuationsring*).

(8.8) Bemærkning. Lad K være et legeme og lad G være en totalt ordnet kommutativ (additivt skrevet) gruppe. Ved en G-*valuation* i K forstås da en afbildning $v\colon K^* \to G$, som opfylder betingelserne,

$$v(\alpha\beta) = v(\alpha) + v(\beta), \quad v(\alpha + \beta) \geqslant \min\{v(\alpha), v(\beta)\}$$

(hvor vi bekvemt sætter $v(0) := +\infty$). Lad der være givet en G-valuation i K. Øjensynlig er da delmængden,

$$V := \{\alpha \in K \mid v(\alpha) \geqslant 0\},$$

en delring af K. Det følger af Korollar (8.5), (iii) $\Longrightarrow$ (i), at V er en valuationsring med K som brøklegeme og maksimalideal $\mathfrak{m}(V)$ bestående af de elementer α for hvilke $v(\alpha) > 0$. Hvis valuationen v er triviel, dvs hvis $v(\alpha) = 0$ for alle $\alpha \in K^*$, så er $V = K$. Værdigruppen, dvs undergruppen $v(K^*)$ af G, er øjensynlig isomorf med $\mathbb{Z}$, hvis og kun hvis V er en diskret valuationsring.

Enhver valuationsring V med K som brøklegeme fremkommer på denne måde. Hertil bemærkes, at kvotientgruppen $G := K^*/V^*$ kan ordnes ved at fastlægge, at de positive elementer er klasserne repræsenteret af elementer i $\mathfrak{m}(V)$. Det er let at se, at kvotienten G herved er en totalt ordnet gruppe og at V er valuationsringen hørende til den kanoniske homomorfi $v\colon K^* \to K^*/V^*$.

Index.