Pakke Mat 3AG 1994

Noter til Matematik 3AG

Algebra og geometri

Anders Thorup

Noter til Matematik 3AG, 1994

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 element* i R. Et sådant element kaldes også en *enhed* i R. At r er et invertibelt element 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). Et element r i R kaldes en *nul-divisor*, hvis der findes et element $a \neq 0$ i R, således at $ra = 0$. Bemærk, at der ikke findes nogen nul-divisorer i nul-ringen. I alle andre ringe er nul-elementet en nul-divisor. Ringen kaldes et *integritetsområde*, hvis ringen ikke er nul-ringen og den eneste nul-divisor 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 $\mathbf{Z}$ af hele tal er et integritetsområde. Ringene $\mathbf{Q}$, $\mathbf{R}$ og $\mathbf{C}$ af henholdsvis rationale, reelle og komplexe tal er legemer.

(1.3). 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). 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). 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*, hvis den desuden er et integritetsområde.

De trivielle idealer er øjensynlig hovedidealer: hovedidealet (0) består kun af nulelementet, 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). 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*, 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*, eller at være en Gauss'isk ring. Den kaldes også et UFD (engelsk: Unique Factorization Domain). Det er velkendt, at et hovedidealområde er en fakto-

riel ring. To elementer i en faktoriel ring kaldes *primiske*, hvis deres fælles divisorer kun er enhederne.

(1.7). 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* $\mathfrak{ab}$ forstås idealet bestående af alle endelige summer af produkter ab, hvor $a \in \mathfrak{a}$ og $b \in \mathfrak{b}$. Ved *radikalet* $\operatorname{Rad}\mathfrak{a}$ 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 $\operatorname{Rad}(0)$ af det trivielle ideal (0) består af de nilpotente elementer i R.

(1.8). Til hvert ideal $\mathfrak{a}$ i R hører 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*. 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). Med $R[X]$ betegnes ringen af *polynomier* med koefficienter i R. Elementerne i $R[X]$ er endelige summer,

$$f = r_0 + r_1 X + \cdots + r_n X^n.$$

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). 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,

$$r_0 + r_1 X + \cdots + r_{n-1} X^{n-1}.$$

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). 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. ∎

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

De irreducible (normerede) polynomier i $\mathbf{R}[X]$ er netop polynomierne $X - a$ for $a \in \mathbf{R}$ 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 $\mathbf{R}[X]$. 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 komplex rod α, og med α er også det komplext konjugerede tal $\overline{\alpha}$ rod i f. Disse tal er forskellige, så inden for $\mathbf{C}[X]$ er f delelig med produktet $p = (X - \alpha)(X - \overline{\alpha})$. Polynomiet p har reelle koefficienter, og er af den ønskede form. I ringen $\mathbf{C}[X]$ går p op i f; det følger så, fx af Sætningen om division med rest, at p også i ringen $\mathbf{R}[X]$ 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 $\mathbf{R}$, og antag at K har endelig dimension som vektorrum over $\mathbf{R}$. Da er enten $K = \mathbf{R}$ eller K er isomorf med $\mathbf{C}$*

Bevis. Antag, at $\mathbf{R} \subset K$, og betragt et element α i overskudsmængden. Som i (1.12) indses, at α er rod i et irreducibelt polynomium p i $\mathbf{R}[X]$. Da $\alpha \notin \mathbf{R}$, 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 $x, y \in \mathbf{R}$, udgør et med $\mathbf{C}$ isomorft dellegeme af K. Af resultatet i (1.12), anvendt for $k = \mathbf{C}$, følger nu, at K er lig med dette dellegeme. Hermed er resultatet bevist. ∎

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

$$F = \sum_{i_1, \ldots, i_n} r_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n}.$$

De specielle polynomier af formen $rX_1^{i_1}\cdots X_n^{i_n}$, hvor $r \in R$, kaldes *monomier*. Hvis $r \neq 0$ tillægges monomiet graden $i_1 + \cdots + i_n$. Et polynomium er således en endelig sum af monomier. Monomiet $X_1^{i_1}\cdots X_n^{i_n}$ siges at *forekomme* i polynomiet F, hvis den tilhørende koefficient $r_{i_1,\ldots,i_n}$ 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 monomier $r_{i_1,\ldots,i_n}X_1^{i_1}\cdots X_n^{i_n}$, der har graden h.

Monomierne i F kan ordnes efter en af de variable, fx efter X_n. Herved fremkommer et polynomium i den ene variable X_n, hvis koefficienter er polynomier i de resterende variable $X_1, \ldots, X_{n-1}$. Specielt fås følgende induktive definition af polynomier:

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

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 $R[X_1, \ldots, X_n]$ i n variable en faktoriel ring. Specielt følger det ved induktion, at polynomiumsringen $k[X_1, \ldots, X_n]$ med koefficienter i et legeme k er en faktoriel ring. [Induktionsstarten er her, at polynomiumsringen $k[X]$ er faktoriel, jfr (1.12).]

(1.15). Ved en *modul* M over ringen R forstås som bekendt en kommutativ gruppe M forsynet med en multiplikation med elementer fra ringen, $R \times M \to M$, som opfylder de linearitetskrav, der kendes fra vektorrum. Multiplikationen betegnes $(r, x) \mapsto rx$, hvis misforståelser er udelukkede. I denne forbindelse kaldes ringens elementer ofte *skalarer*. Bemærk, at betingelsen $1x = x$, hvor 1 er et-elementet i R, er med blandt kravene: moduler forudsættes at være unitære. Modulen, der har netop ét element, kaldes *nul-modulen* og betegnes 0.

(1.16). Det mest oplagte eksempel på en R-modul er mængden R^n af n-sæt med koefficienter i R. Addition og multiplikation med skalarer fra R er koordinatvise. For $n = 1$ fås specielt ringen R opfattet som modul over sig selv. Hvis $M_1, \ldots, M_n$ er givne R-moduler defineres mere generelt den *direkte sum*,

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

som mængden af n-sæt $(x_1, \ldots, x_n)$, hvor $x_i \in M_i$. Addition og multiplikation med skalarer fra R defineres koordinatvis.

(1.17). 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.

En modul M siges at være *endeligt frembragt*, hvis der i M findes endelig mange elementer $e_1, \ldots, e_n$ 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, siges modulen M at være en *fri modul*, og sættet $e_1, \ldots, e_n$ kaldes en *basis* for modulen. Det er let at se, at M er endeligt frembragt, hvis og kun hvis der findes en surjektiv homomorfi $R^n \to M$, og at M er fri, hvis og kun hvis der findes en isomorfi $R^n \to M$.

(1.18). 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). Bemærk, at i modulen R er undermodulerne netop idealerne i ringen R.

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

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

Relationen kaldes også *kongruens modulo* N. Ækvivalensklasserne kaldes også *sideklasser*. 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 $\hat{x}$, 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,

$$\hat{x} + \hat{y} = \widehat{x+y}, \quad r\hat{x} = \widehat{rx}.$$

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

Lad $\varphi\colon M \to N$ være en modulhomomorfi. Da udsiger *Isomorfisætning for moduler* som bekendt følgende: *Kernen for φ, dvs originalmængden $\varphi^{-1}(0)$, er en undermodul i M, og billedet φM er en undermodul i N, og φ inducerer en naturlig isomorfi fra kvotientmodulen $M/\varphi^{-1}(0)$ på billedmodulen φM.*

(1.20). 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 opfylder $rx = 0$, og det kaldes også *annullatoren* for elementet x, og det betegnes $\operatorname{Ann}(x)$. Billedet 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 en *cyklisk modul*, 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). Antag, at R er et hovedidealområde. Som bekendt gælder da følgende *Struktursætning*: *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.

(1.22). 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,

$$\det \alpha = \sum_\sigma \operatorname{sign}(\sigma) \alpha_{1\sigma_1} \cdots \alpha_{n\sigma_n}$$

hvor der summeres over alle permutationer i den symmetriske gruppe S_n.

Lad nu $\tilde{\alpha}$ betegne matricen defineret ved at $\tilde{\alpha}_{ij}$ er fortegnet $(-1)^{i+j}$ multipliceret med determinanten af den delmatrix af α, der fremkommer ved at slette j'te række og i'te søjle. (Denne matrix kaldtes klassisk den adjugerede til matricen α.) Med denne notation gælder da for en vilkårlig søjle $x \in R^n$ og $k = 1, \ldots, n$ formlen,

$$\det(\alpha_1, \ldots, x, \ldots, \alpha_n) = ({}_k\tilde{\alpha})x,$$

hvor x er placeret som k'te søjle i matricen på venstresiden.

For at bevise denne formel udvikles determinanten på venstresiden efter den k'te søjle. For determinanten fremkommer herved et udtryk, der øjensynlig har formen,

$$\det(\alpha_1, \ldots, x, \ldots, \alpha_n) = A_1 x_1 + \cdots + A_n x_n,$$

hvor A_i'erne kun afhænger af matricen α og ikke af søjlen x. Følgelig kan A_i bestemmes ved i udtrykket at indsætte den søjle x, der har 1 på den i'te plads og 0 på de øvrige pladser. Den søgte formel følger umiddelbart af denne bestemmelse.

Formlerne ovenfor vedrører rækkerne i den adjugerede matrix $\tilde{\alpha}$. Tilsvarende formler for søjlerne i den adjugerede matrix udledes analogt (eller ved transponering). De to sæt formler medfører følgende identiteter, kaldet *Cramer's formler*,

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

hvor 1_n betegner $n \times n$ enhedsmatricen.

2. Kerne og kokerne. Exakte følger.

(2.1) Definition. 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,

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

[Her, som i det følgende, siges et diagram bestående af moduler og homomorfier at være *kommutativt*, hvis det for 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) Definition. 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 *exakt i modulen* M_i, hvis billedet af φ_{i+1} er lig med kernen for φ_i, og den kaldes en *exakt følge*, hvis den er exakt 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:

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

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

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

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

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

Betragt nu videre følgerne:

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

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

Følgen (2.4.4) er exakt i M, netop når φ er injektiv, dvs når φ afbilder M isomorft på billedet φM. Den er exakt i N, hvis φM er lig med kernen for ψ. At følgen er exakt 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 exakt 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 exakt i N betyder, at K er lig med billedet af φ, altså at N/K er lig med kokernen for φ. At følgen er exakt 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,*

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

er exakt, 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 exakte rækker,*

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

Da induceres naturligt en exakt følge mellem kerner og kokerner,

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

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) Definition. 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 exakt 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 exakt 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 exaktheden. Vi efterviser kun to af påstandene, og overlader resten til læseren.

Følgen er exakt 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 exakt, 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 exakt 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 exakte rækker:

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

Konklusionen er så en udvidet exakt kerne-kokerne følge,

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

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 exakt følge mellem kvotienterne,*

$$0 \to F_2'/F_1' \to F_2/F_1 \to F_2''/F_1'' \to 0.$$

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 exakte 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 exakte følge af kvotienter er altså den sidste del af den exakte 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 exakte følge fra (2.10) er altså $F_2''/F_1'' = 0$. Exaktheden 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 exakt følge,*

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

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 exakte følge i (2.10) er altså den ønskede. ∎

(2.13) Bemærkning. Ifølge Isomorfisætning (2.5) kan exaktheden 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 exakt følge,*

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

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 $x \in M$ er repræsentant for en klasse i $\operatorname{Coker}\varphi$, så er ψx 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 exakt overlades til læseren. ∎

(2.15) Opgave. Elementerne i en direkte sum $M_1 \oplus \cdots \oplus M_n$, der som bekendt er n-sæt x, hvor den i'te koordinat x_i tilhører M_i, skrives bekvemt som søjler. 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,

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

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,

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

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,

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

Gør rede for hvorledes afbildningerne, specielt den midterste lodrette, er definerede. Vis, at rækkerne er exakte 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 exakt.

3. Brøkring og brøkmodul.

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

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

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

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

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

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

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

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

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

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

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

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

(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 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) Definition. Ringen $S^{-1}R$ kaldes *brøkringen for R mht S*, og den siges at fremkomme ved at *lokalisere mht S*. 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 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 $\mathbf{Z}_f$, hvor f er et helt tal forskelligt fra 0, ikke må forveksles med restklasseringen modulo f. Den sidste betegnes $\mathbf{Z}/f$. Bemærk videre, at for et primtal p er brøkringene $\mathbf{Z}_p$ og $\mathbf{Z}_{(p)}$ forskellige. Begge kan opfattes som delringe af $\mathbf{Q}$. 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) Definition. 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 $\mathbf{Z}$ af hele tal er legemet $\mathbf{Q}$ af rationale tal.

Ringen $k[X_1, \ldots, X_m]$ af polynomier i m variable over et legeme k er et integritetsområde. Det tilhørende brøklegeme betegnes $k(X_1, \ldots, X_m)$, 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 $x = (x_1, \ldots, x_n)$ er et n-sæt med $x_i \in M_i$. Ved isomorfien svarer denne brøk til n-sættet $(x_1/s, \ldots, x_n/s)$ 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 $(x_1, \ldots, x_n)$ til $t(x_1, \ldots, x_n) = (tx_1, \ldots, tx_n)$, 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 $x = (x_1, \ldots, x_n)$, 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 exakt følge af R-lineære afbildninger. Da induceres en exakt 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 exakt, 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 exaktheden 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 exakt. Ved gentagen anvendelse af Lemma (3.9) fås derfor, at den lokaliserede følge er exakt,

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

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: Lad $(0) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = M$ være en filtration i 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 som bekendt 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) Bemærkning. 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.

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,

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

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,

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

I en noethersk ring kan der ikke findes en sådan uendelig kæde. 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. ∎

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

(4.4) Definition. 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 $v_1, \ldots, v_m$ 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,

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

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,

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

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

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

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 $(v_1, \ldots, v_m)d = 0$. 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 $(v_1, \ldots, v_n)$ 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,

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

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 exakte følge $F \to M \to Q \to 0$, og heraf fås umiddelbart den exakte følge,

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

Forudsætningerne medfører, at afbildningen $F/\mathfrak{m}F \to M/\mathfrak{m}M$ er surjektiv. Af exaktheden 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 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. Betragt først følgende relationer mellem idealer:

$$\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n, \tag{1}$$

$$\mathfrak{a} \cap \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{n-1} \not\subseteq \mathfrak{p}_n, \tag{2}$$

$$\mathfrak{a} \not\subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_{n-1}. \tag{3}$$

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

$$a \in \mathfrak{p}_i \text{ for } i = 1, \ldots, n-1 \text{ og } a \notin \mathfrak{p}_n, \tag{4}$$

$$b \notin \mathfrak{p}_i \text{ for } i = 1, \ldots, n-1 \text{ og } b \in \mathfrak{p}_n, \tag{5}$$

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

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

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

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

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

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

Hermed er den ønskede inklusion nået i alle tilfælde. ∎

(4.10) Definition. 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. Det er let at se, at produktet $\mathfrak{a}R'$ så er et ideal i ringen R'. Det kaldes *extensionen* af idealet $\mathfrak{a}$.

(4.11) Observation. Kontraktionen $\theta^{-1}(\mathfrak{b})$ af et ideal $\mathfrak{b}$ i R' er øjensynlig kernen for den sammensatte ringhomomorfi $R \to R' \to R'/\mathfrak{b}$. 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 extension 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 extension 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 extension 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 extension og kontraktion,*

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

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

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

Bevis. Det er klart, at idealet $S^{-1}\mathfrak{p}$ netop er extensionen 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 extension af et primideal $\mathfrak{p}$, der er disjunkt med S, er et primideal $S^{-1}\mathfrak{p}$. Videre skal det vises, at kontraktion og extension 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 extension 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

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

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 extensionen $S^{-1}\mathfrak{p}$, 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 $i \geq 1$ en naturlig isomorfi,*

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

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) Definition. 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 $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ 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 $i = 1, \ldots, r$ 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 $i = 1, \ldots, r$, 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 $\mathbf{Z}$ af hele tal. Her er alle idealer hovedidealer, dvs af formen (n), hvor $n \geq 0$. 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 $\mathbf{Z}$, 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 $n_1, \ldots, n_r$ og $n := n_1 \cdots n_r$ er*

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

Endelighedsbetingelser

1. Endeligt frembragte moduler.

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

$$Rv_1 + \cdots + Rv_m$$

delmængden af M bestående af de elementer, der har formen

$$r_1v_1 + \cdots + r_mv_m \qquad \text{med } r_i \in R.$$

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 $v_1, \ldots, v_m$, 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 $v_1, \ldots, v_m$ i en modul M defineres en R-lineær afbildning $R^m \to M$ ved

$$(r_1, \ldots, r_m) \mapsto r_1v_1 + \cdots + r_mv_m.$$

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 exakt følge af R-moduler,*

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

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 $v_1, \ldots, v_m$ 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 $v_1, \ldots, v_n$ som frembringer N og elementer $u_1, \ldots, u_p$, som frembringer P. Da ψ er surjektiv, findes elementer $w_1, \ldots, w_p$ i M, som ved ψ afbildes på u_i'erne. Det påstås, at M er frembragt af de endelig mange elementer $\varphi v_1, \ldots, \varphi v_n, w_1, \ldots, w_p$. 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 exakt, 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 exakte følge hørende til en undermodul N af M,

$$0 \to N \to M \to M/N \to 0.$$

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 $i = 1, \ldots, n$ 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) Observation. Antag, at M er frembragt af elementer $v_1, \ldots, v_m$. Sæt

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

for $i = 0, \ldots, m$ (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.

Omvendt følger det af Sætning (1.3) ved induktion, at hvis en modul M har en filtration med endeligt frembragte kvotienter, så er M selv endeligt frembragt.

(1.9) 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 $i = 0, \ldots, n$ (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 kan identificeres med de n-sæt, der har 0'er 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 $(F \oplus N)/F = N$.

(1.10) Lemma. *Lad der være givet en filtration $0 = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = M$ i modulen M. Lad videre N være en undermodul i M. Sæt $F_i' := F_i \cap N$, og lad F_i'' betegne billedet af F_i i kvotienten M/N. Da udgør F_i''erne en filtration i undermodulen N, og F_i'''erne udgør en filtration i kvotientmodulen M/N. For kvotienterne findes en exakt følge,*

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

Bevis. Den første påstand er klar, den anden påstand er en velkendt konsekvens af Slangelemma'et. ∎

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 $\operatorname{long} M$. 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.

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)⇒(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 exakt følge af moduler,*

$$0 \to M' \to M \to M'' \to 0.$$

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.

„$\geq$“: 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 $k' + k'' \leq \operatorname{long} M$. Da filtrationerne i M' og M'' var vilkårlige, følger det endelig, at

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

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

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

Lad k være filtrationens længde. Sæt nu $F'_i := M' \cap F_i$, og lad F''_i betegne billedet af F_i i M''. Herved fremkommer filtrationer i M' og i M'', hvis længder betegnes henholdsvis k' og k''. Af Lemma (1.10) fås den exakte følge,

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

Her er den midterste modul forskellig fra 0 for k værdier af $i = 1, \ldots n$. Af exaktheden 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,

$$k \leq k' + k''.$$

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

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

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 $0 \to N \to M \to M/N \to 0$ er exakt, følger (1) umiddelbart af sætningen. Påstand (2) følger ved induktion efter n af sætningen ved hjælp af den exakte følge,

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

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,*

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

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. ∎

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 $i \leq j$. 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 $v_1, \ldots, v_m$ 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) $\Longleftrightarrow$ (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) Definition. 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 exakt følge,

$$0 \to K' \to K \to K'' \to 0.$$

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 exakt følge* $0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$ *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 exakte følge,

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

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 $\mathbf{Z}$ 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 $n \geq m$. 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 $1, X, \ldots, X^{n_0-1}$. 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 $n \geq n_0$ 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 $n \geq n_0 \geq n_i$, 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 $k[X_1, \ldots, X_r]$ i r variable, hvor k er et legeme eller $k = \mathbf{Z}$, er en noethersk ring.*

Bevis. Påstanden følger ved induktion efter r, idet der for en vilkårlig ring R gælder, at

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

Induktionsstarten er at et legeme k og ringen $\mathbf{Z}$ er noetherske ringe. ∎

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

4. Endeligt frembragte algebraer. Hele udvidelser.

(4.1) Definition. 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, som omfatter $\theta(R)$, selv opfattes som R-algebra. En sådan delring kaldes også en *delalgebra* af A.

En R-algebra A, der er endeligt frembragt som R-modul, kaldes ofte også en *endelig algebra* over R.

(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 $e_1, \ldots, e_n$ i M frembringer M som A-modul, og at p elementer $v_1, \ldots, v_p$ 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,

$$x = a_1 e_1 + \cdots + a_n e_n, \qquad (*)$$

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) Definition. Lad A være en R-algebra. For givne elementer $a_1, \ldots, a_m$ i A betegnes da med

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

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 som R-algebra*, hvis der i A findes endelig mange elementer $a_1, \ldots, a_m$, som *frembringer algebraen* A, dvs opfylder at

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

(4.4) Definition. Polynomiumsringen $R[X_1, \ldots, X_m]$ 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 $X_1, \ldots, X_m$.

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

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

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

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

og det siges at fremkomme ved at *indsætte* $a_1, \ldots, a_m$ 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 $a_1, \ldots, a_m$ 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 $R[X_1, \ldots, X_m]$ for passende m, altså hvis og kun hvis A er isomorf med en kvotient $R[X_1, \ldots, X_m]/\mathfrak{A}$, 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 $a^n + r_1 a^{n-1} + \cdots + r_n = 0$, 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,

$$a^n + r_1 a^{n-1} + \cdots + r_n = 0, \qquad (*)$$

hvor r_i'erne tilhører R. Det påstås, at elementerne $1, a, \ldots, a^{n-1}$ frembringer $R[a]$ som R-modul. Det er øjensynlig nok at vise, at hver potens a^p er en R-linear kombination af $1, \ldots, a^{n-1}$. 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,

$$a^p = s_n + s_{n-1} a + \cdots + s_1 a^{n-1},$$

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

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

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 $1, \ldots, a^{n-1}$. Erstattes a^n på højresiden af $(**)$ med denne linearkombination fås en fremstilling af a^{p+1} som R-linearkombination af $1, \ldots, a^{n-1}$, 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 $b_1, \ldots, b_m$, 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,

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

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

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

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

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

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 $(b_1, \ldots, b_m)d = 0$. 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 $r_1, \ldots, r_m$ 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 $a_1, \ldots, a_m$ i A er da hele over R, hvis og kun hvis delalgebraen $R[a_1, \ldots, a_m]$ er endeligt frembragt som R-modul.*

Bevis. Delalgebraen $R[a_1, \ldots, a_m]$ indeholder a_i'erne. Af betingelsen (4.6)(iii) følger derfor, at hvis delalgebraen er endelig over R, 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 $a_1, \ldots, a_{m+1}$ i A er hele over R, og at påstanden gælder for m elementer. Sæt $B := R[a_1, \ldots, a_m]$. Øjensynlig er $R[a_1, \ldots, a_m, a_{m+1}] = B[a_{m+1}]$, 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 $R[a, b]$ endelig over R. 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 $B := R[a_1, \ldots, a_n]$ 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,

$$s(-r_1 r^{n-1} - r_2 r^{n-2} s - \cdots - r_n s^{n-1}) = r^n.$$

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. Sætningen ovenfor generaliserer 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 $a_1, \ldots, a_m$. Da findes i A et sæt af $t \leq m$ elementer $x_1, \ldots, x_t$, der er algebraisk uafhængige over k og således at A er endeligt frembragt som modul over delalgebraen $k[x_1, \ldots, x_t]$.*

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 $a_1, \ldots, a_m$ er algebraisk uafhængige, er påstanden triviel: vi kan bruge $t = m$ og $x_i = a_i$ for $i = 1, \ldots, m$. Antag derfor, at a_i'erne er algebraisk afhængige, dvs at der findes en relation,

$$\sum r_{i_1,\ldots,i_m} a_1^{i_1} \cdots a_m^{i_m} = 0, \qquad (*)$$

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

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

Det er nok at vise, at hvis g_j'erne vælges passende, så er a_m hel over delalgebraen $B := k[b_1, \ldots, b_{m-1}]$. Antag nemlig, at a_m er hel over B. Da er $B[a_m]$ endeligt frembragt som B-modul. For $i = 1, \ldots, m-1$ 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 $t \leq m-1$ elementer i B, der er algebraisk uafhængige over k, og således at B er endeligt frembragt som modul over $k[x_1, \ldots, x_t]$. Af Lemma (4.2) følger, at A er endeligt frembragt som modul over $k[x_1, \ldots, x_t]$, 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 $i = 1, \ldots, m-1$. Indsættes disse ligninger i ligningen $(*)$ fremkommer på venstresiden en sum af udtryk af formen,

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

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 exponent 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 $r_{i_1,\ldots,i_m}$. Udtrykket har altså formen

$$r_{i_1,\ldots,i_m} a_m^{g_1 i_1 + \cdots + g_{m-1} i_{m-1} + i_m} + \cdots , \qquad (**)$$

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

I den givne relation $(*)$ er $r_{i_1,\ldots,i_m}$'erne kun forskellige fra 0 for endelig mange sæt $i_1, \ldots, i_m$. Svarende til disse endelig mange sæt $i_1, \ldots, i_m$ vælger vi nu g_j'erne, så at de tilhørende exponenter $i_1 g_1 + \cdots + i_{m-1} g_{m-1} + i_m$ er indbyrdes forskellige. At et sådant valg er muligt kan indses således: Vi betragter kun endelig mange sæt $i_1, \ldots, i_m$, 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 exponenter er da

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

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

Med dette valg af g_j'erne opnås det ønskede. For de endelig mange sæt $i_1, \ldots, i_m$, for hvilke $r_{i_1,\ldots,i_m} \neq 0$, er de tilsvarende exponenter $i_1 g^m + \cdots + i_{m-1} g + i_m g^0$ nu forskellige, så blandt dem findes èn, der er størst. Lad N være den største exponent, 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 exponent 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 A. Multiplikation med a definerer en R-lineær afbildning $x \mapsto ax$ af $R[a]$ ind i sig selv. Da A er et integritetsområde er multiplikationsafbildningen injektiv. Videre er a hel over R, og $R[a]$ er derfor endeligt frembragt som R-modul. Med andre ord er $R[a]$ et endeligdimensionalt vektorrum over legemet R. Følgelig er den injektive multiplikationsafbildning bijektiv. Et-elementet 1 i $R[a]$ vil derfor tilhøre billedet. Der findes altså et element x i $R[a]$, så at $ax = 1$. Altså er elementet a invertibelt i 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 $x_1, \ldots, x_t$, der er algebraisk uafhængige over k og således at A er endeligt frembragt som modul over delringen $k[x_1, \ldots, x_t]$. Da A er et legeme, følger det af Lemma (4.14), at også denne delring er et legeme. Da elementerne $x_1, \ldots, x_t$ 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. ∎

5. Transcendensgrad.

I dette afsnit 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. ∎

(5.4) Lemma. *Lad der være givet et sæt af endelig mange elementer $a_1, \ldots, a_m$ 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 $R[a_1, \ldots, a_{m-1}]$ netop hvis der findes en relation,

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

hvor koefficienterne fås ved indsættelse af $a_1, \ldots, a_{m-1}$ i polynomier P_j i $m-1$ variable, og hvor en af koefficienterne $P_j(a_1, \ldots, a_{m-1})$ er forskellig fra 0. Venstresiden i $(*)$ fås øjensynlig ved at indsætte $a_1, \ldots, a_m$ i polynomiet

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

Nu følger „hvis" umiddelbart: Er fx $(*)$ opfyldt, og $P_j(a_1, \ldots, a_{m-1}) \neq 0$, så er $P \neq 0$; af $P(a_1, \ldots, a_m) = 0$ 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 $a_1, \ldots, a_m$, som er algebraisk afhængige. Hvis de $m-1$ elementer $a_1, \ldots, a_{m-1}$ 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 $P(a_1, \ldots, a_m) = 0$. Skriv nu polynomiet P på formen $(**)$. Så er ligningen $(*)$ opfyldt. Yderligere er en af koefficienterne $P_j(a_1, \ldots, a_{m-1})$ forskellig fra nul, idet P ellers ville være nul-polynomiet. Altså er a_m algebraisk over delalgebraen frembragt af de første $m-1$ af a_i'erne. ∎

(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 $a_1, \ldots, a_n$ i A, så at hvert element i V er algebraisk over delringen $R[a_1, \ldots, a_n]$, dvs så at

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

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 $\dim_R^{\text{alg}} V$. Hvis V ikke har endelig algebraisk dimension sættes $\dim_R^{\text{alg}} V := \infty$.

Ved *transcendensgraden* for V over R forstås det største antal af algebraisk uafhængige (over R) elementer, der kan udtages fra V. Transcendensgraden betegnes $\mathrm{tdeg}_R V$. 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 $\mathrm{tdeg}_R V$.

Ved en (endelig) *transcendensbasis* for V over R forstås et endeligt sæt af elementer $v_1, \ldots, v_t$ 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 $v_1, \ldots, v_t$ i V. Følgende betingelser (over R) er da ækvivalente:*

(i) *Sættet $v_1, \ldots, v_t$ er et minimalt algebraisk frembringersystem for V, dvs et frembringersystem hvori intet v_i kan undværes.*

(ii) *Sættet $v_1, \ldots, v_t$ 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 $v_1, \ldots, v_t$ 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

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

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,

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

Men dette strider mod at $v_1, \ldots, v_t$ 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 $V \subseteq \overline{R[v_1, \ldots, v_{t-1}]}$. 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) ⟺ (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,*

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

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 $l \geq t$, 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 $t \geq 1$, 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 $l \geq t - 1$, 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 $l \geq t - 1$; 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 $t \leq l$. 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,*

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

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 $\dim_R^{\mathrm{alg}} V \leq \mathrm{tdeg}_R V$ 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 $\mathrm{tdeg}_R V \leq \dim_R^{\mathrm{alg}} V$. Hvis højresiden er uendelig gælder uligheden nemlig trivielt. Hvis højresiden er endelig, findes et algebraisk frembringersystem $a_1, \ldots, a_l$ 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 $t \leq l$. Altså er $\mathrm{tdeg}_R V \leq l$, 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 $a_1, \ldots, a_m$ i A betegnes med

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

brøklegemet for delalgebraen $R[a_1, \ldots, a_m]$. 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 $a_1, \ldots, a_m$, som *frembringer legemet* A, dvs opfylder at

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

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 $a_1, \ldots, a_m$. Da er $A = k[a_1, \ldots, a_m]$, og for brøklegemet af A kan anvendes betegnelsen $k(a_1, \ldots, a_m)$. Algebraen A er homomorft billede af en polynomiumsring, altså af formen $A = k[X_1, \ldots, X_m]/\mathfrak{P}$, 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 $k[x_1, \ldots, x_t]$, 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 $t = \mathrm{tdeg}_k A$.

(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,*

$$\mathrm{tdeg}_k(A/\mathfrak{p}) \leq \mathrm{tdeg}_k A.$$

Hvis $\mathrm{tdeg}_k A < \infty$ 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 $P(a_1, \ldots, a_t)$, der fås ved at indsættelse af a_i'er 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 $\mathrm{tdeg}_k A < \infty$ og at lighed gælder i uligheden. Vi kan da vælge a_i'erne, med $t := \mathrm{tdeg}_k(A/\mathfrak{p})$, så at $\hat{a}_i$'erne udgør en transcendensbasis for $A/\mathfrak{p}$. Da er a_i'erne algebraisk uafhængige over k. Specielt afbildes delringen $B := k[a_1, \ldots, a_t]$ derfor isomorft på sit billede $k[\hat{a}_1, \ldots, \hat{a}_m]$ i $A/\mathfrak{p}$. Da $t = \mathrm{tdeg}_k A$, 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,

$$b_m a^m + \cdots + b_1 a + b_0 = 0, \qquad (*)$$

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

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

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 $\mathrm{Ann}(x)$. Ifølge definitionen er altså

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

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 $\mathrm{Ann}\, M$, altså

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

Ved *støtten* for modulen M forstås mængden af de primidealer $\mathfrak{p}$ i R, for hvilke $M_\mathfrak{p} \neq 0$. Støtten betegnes $\mathrm{Supp}\, M$. Bemærk, at støtten er en mængde af primidealer, og ikke en delmængde af R.

Primidealerne blandt annullatorerne $\mathrm{Ann}(x)$ 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

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

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

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

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

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 $\mathrm{Ann}(x)$ for et element x i M.

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

$$\mathrm{Ass}\, M \subseteq \mathrm{Supp}\, M.$$

(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 $\mathrm{Ann}(x)$ er nemlig kernen for den ved $r \mapsto rx$ bestemte lineære afbildning $R \to M$. Hvis $\mathfrak{a} = \mathrm{Ann}(x)$, 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 $\mathrm{Ann}(x) = \mathrm{Ann}(\hat{1}) = \mathfrak{a}$.

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* $\mathrm{Supp}\, M$ *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 $\mathrm{Ann}(x)$. Følgelig er $\mathrm{Ann}(x) \subset R$. Af Eksistenssætningen for maksimalidealer følger derfor, at der i R findes et maksimalideal $\mathfrak{m}$, således at $\mathrm{Ann}(x) \subseteq \mathfrak{m}$. Af den sidste relation følger, at $M_{\mathfrak{m}} \neq 0$. Da maksimalidealet $\mathfrak{m}$ således tilhører støtten $\mathrm{Supp}\, M$, 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 $\mathfrak{p} \supseteq \mathrm{Ann}\, M$.*

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

For at vise det omvendte udnyttes, at M er frembragt af endelig mange elementer $x_1, \ldots, x_n$. 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,

$$\mathrm{Ann}(x_1) \cap \cdots \cap \mathrm{Ann}(x_n) \subseteq \mathrm{Ann}\, M$$

(der forøvrigt klart må være en lighed). Antag nu, at $\mathrm{Ann}\, M \subseteq \mathfrak{p}$. Af inklusionen ovenfor følger så, at fællesmængden af idealerne $\mathrm{Ann}(x_i)$ er indeholdt i primidealet $\mathfrak{p}$. Som bekendt følger heraf, at et af idealerne $\mathrm{Ann}(x_i)$ 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 $\mathrm{Ann}(\hat{1}) = \mathfrak{a}$. Omvendt er det klart, at hvert element i $\mathfrak{a}$ annullerer hvert element i $R/\mathfrak{a}$. Altså er $\mathfrak{a} = \mathrm{Ann}(R/\mathfrak{a})$. 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 $\mathrm{Ann}(x) = \mathfrak{q}$. 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,

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

(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. *Lad S være en multiplikativ delmængde i R og lad $\mathfrak{p}$ være et primideal disjunkt med S. For enhver modul M gælder da,*

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

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

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

Bevis. Primidealet $\mathfrak{p}$ 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 $p_1, \ldots, p_n$. 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

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

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. ∎

(1.9) Lemma. *Lad M være en R-modul. Enhver annullator, der er maksimal blandt annullatorerne* $\mathrm{Ann}(x)$ *for $x \neq 0$, er et primideal (og dermed et associeret primideal for M).*

Bevis. Antag, at $\mathfrak{p} = \mathrm{Ann}(y)$ er maksimalt blandt annullatorerne $\mathrm{Ann}(x)$, hvor $x \neq 0$. Det skal vises, at $\mathfrak{p}$ er et primideal. Da $y \neq 0$, er $\mathfrak{p} \subset R$. Antag videre, at et produkt rs tilhører $\mathfrak{p}$ og at faktoren s ikke tilhører $\mathfrak{p}$. Det skal vises, at faktoren r tilhører $\mathfrak{p}$. Af antagelserne fås relationerne,

$$rsy = 0 \text{ og } sy \neq 0. \qquad (*)$$

Ethvert element i R, som annullerer y, vil også annullere sy. Følgelig er $\mathfrak{p} \subseteq \mathrm{Ann}(sy)$. Den sidste ulighed i $(*)$ viser, at annullatoren $\mathrm{Ann}(sy)$ er blandt de betragtede annullatorer. Maksimaliteten af $\mathfrak{p}$ medfører derfor, at $\mathfrak{p} = \mathrm{Ann}(sy)$. Den første ligning i $(*)$ udsiger, at $r \in \mathrm{Ann}(sy)$. Altså er $r \in \mathfrak{p}$, som ønsket. ∎

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

2. Filtration.

(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. Den sidste påstand er også en konsekvens af den anden påstand, idet det følger af Eksistenssætning (1.4), at hvis M ikke er nul-modulen, så er støtten for M ikke tom. Beviset for sætningen bruger imidlertid ikke Eksistenssætningen, og den sidste påstand vil blive brugt i beviset for den anden påstand.

For at bevise den første påstand betragtes mængden af de annullatorer $\mathrm{Ann}(x)$, hvor $x \neq 0$ og hvor $\mathrm{Ann}(x) \supseteq \mathrm{Ann}(y)$. 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 $\mathrm{Ann}(x)$, hvor $x \neq 0$. Af Sætning (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. Som nævnt følger heraf den sidste påstand.

For at bevise sætningens anden påstand betragtes et primideal $\mathfrak{p}$ i støtten for M. Da er $R_\mathfrak{p}$-modulen $M_\mathfrak{p}$ forskellig fra nul-modulen. Af det allerede viste følger, at der i $R_\mathfrak{p}$ findes et primideal associeret til $M_\mathfrak{p}$. Ifølge Lokaliseringsprincippet har dette primideal formen $\mathfrak{q}R_\mathfrak{p}$, hvor $\mathfrak{q}$ er et primideal indeholdt i $\mathfrak{p}$. Extensionen $\mathfrak{q}R_\mathfrak{p}$ var associeret til $M_\mathfrak{p}$. Af den sidste påstand i Lemma (1.8) (her bruges endnu engang, at R er noethersk) følger derfor, at $\mathfrak{q}$ er associeret til M. Da $\mathfrak{q} \subseteq \mathfrak{p}$ er sætningens anden påstand således godtgjort.

Hermed er sætningen bevist. ∎

(2.2) Definition. Et primideal $\mathfrak{p}$ siges at være *minimalt primideal* for modulen M, hvis $\mathfrak{p}$ er minimalt blandt primidealerne i $\mathrm{Supp}\, M$. Betingelsen er altså, at $\mathfrak{p}$ tilhører støtten, dvs at $M_\mathfrak{p} \neq 0$, og at der for alle primidealer $\mathfrak{q} \subset \mathfrak{p}$ gælder at $M_\mathfrak{q} = 0$.

Det følger af Sætning (2.1), at hvert minimalt primideal for M må være et associeret primideal. Men det er ikke en umiddelbar konsekvens af definitionen, at der overhovedet eksisterer minimale primidealer for en given modul M.

(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 $i = 1, \ldots, n$, 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,*

$$\operatorname{Ass} M \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subseteq \operatorname{Supp} M.$$

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,*

$$\operatorname{long}_{R_\mathfrak{p}} M_\mathfrak{p},$$

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 $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_{n-1}\}$, 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* $\operatorname{Supp} M$ *er maksimalidealer.*
(iii) *Alle primidealer, der omfatter* $\operatorname{Ann} M$*, er maksimalidealer.*

Er disse betingelser opfyldt, så består støtten for M af endelig mange maksimalidealer $\mathfrak{m}_1, \ldots, \mathfrak{m}_q$, 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,

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

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 $\mathrm{Ann}(y)$ er indeholdt i et associeret primideal til M. De associerede primidealer er netop $\mathfrak{m}_j$'erne, så $\mathrm{Ann}(y)$ 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 $\mathrm{long}\, M_{\mathfrak{m}_j}$. Altså har homomorfiens venstre- og højreside samme længde. Da homomorfien er injektiv, følger det at den er en isomorfi. ∎

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 $\mathrm{Ass}(M/N) = \{\mathfrak{p}\}$, udtrykkes ved at sige, at N er en $\mathfrak{p}$-*primær* undermodul i M.

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

$$M \to M/N_1 \oplus M/N_2, \qquad (*)$$

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 $\mathrm{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$.

(2) Lad $\mathfrak{m}$ være et maksimalideal. Enhver potens $\mathfrak{m}^m$, hvor $m \geq 1$, 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) Antag endelig, at R er et integritetsområde, og betragt et primideal, der er et hovedideal (p) frembragt af et element $p \neq 0$ i R. Det påstås, at enhver potens (p^m), hvor $m \geq 1$, er et (p)-primært ideal. Hertil betragtes annullatorer af restklasser $\hat{x}$ i $R/(p^m)$ af elementer $x \notin (p^m)$. Skriv nu x på formen $x = sp^t$, hvor $s \notin (p)$ og $0 \leq t < m$; dette er muligt, da $x \notin (p^m)$. Nu gælder følgende biimplikationer,

$$r \in \mathrm{Ann}(\hat{x}) \iff rx \in (p^m) \iff r \in (p^{m-t}). \qquad (*)$$

Den første er nemlig oplagt, og den anden ses således: Hvis $r \in (p^{m-t})$, altså $r = ap^{m-t}$, så er $rx = ap^{m-t}sp^t = asp^m \in (p^m)$. Omvendt, hvis $rx \in (p^m)$, altså $rsp^t = ap^m$, så følger at $rs = ap^{m-t}$. Da (p) er et primideal og $s \notin (p)$ følger heraf videre, at $r \in (p^{m-t})$.

Af $(*)$ ses, at $\mathrm{Ann}(\hat{x}) = (p^{m-t})$. Øjensynlig er denne annullator et primideal, hvis og kun hvis $m - t = 1$. Heraf ses at den eneste annullator for $R/(p^m)$, der er et primideal, er primidealet (p). Og det er netop påstanden.

(3.4) Definition. 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,*

$$N = N_1 \cap \cdots \cap N_q. \qquad (3.5.1)$$

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 N, 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,

$$M/N \to M/N_1 \oplus \cdots \oplus M/N_q, \qquad (*)$$

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 $\operatorname{Ass} Q$ 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 $M_{\mathfrak{q}}$, er $\operatorname{Ann}(y)$ ikke indeholdt i $\mathfrak{q}$. Men det er i modstrid med at $\operatorname{Ann}(y)$ er indeholdt i et associeret primideal ifølge Sætning (2.1) og $\mathfrak{q}$ 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,

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

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,

$$\begin{array}{ccc} M & \longrightarrow & M/N_j \\ \downarrow & & \downarrow \\ (M/N)_{\mathfrak{p}_j} & \longrightarrow & (M/N_j)_{\mathfrak{p}_j}. \end{array}$$

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,

$$\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_q. \qquad (3.6.1)$$

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 $\mathfrak{m}_1, \ldots, \mathfrak{m}_q$ 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)(3) 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 extensionen $\mathfrak{a}R_{\mathfrak{p}_j}$.

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,

$$R/\mathfrak{m}^i \xrightarrow{\sim} R_{\mathfrak{m}}/\mathfrak{m}^i R_{\mathfrak{m}}.$$

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,*

$$a = q_1 \cdots q_n. \qquad (*)$$

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 $b_2 = ab = ab_1b_2$; 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,

$$a = up^n, \qquad (4.2.1)$$

hvor u er en enhed og $n \geq 1$. 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 $m \geq n$, 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 $(a_1, \ldots, a_n) = (a_1, \ldots, a_{n-1})+(a_n)$, 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 extensionen

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 $\mathbf{Z}_{(p)}$, der består af rationale tal af formen a/s, hvor s ikke er delelig med p, er en valuationsring.

Det er ikke svært at vise, at potensrækkeringen $k[[X]]$ med koefficienter i et legeme k er en valuationsring.

(4.7) Definition. Ringen R kaldes en *Dedekindring*, hvis R er et integritetsområde og hvis der for hvert maksimalideal $\mathfrak{m}$ i R gælder, at den lokale ring $R_\mathfrak{m}$ er en valuationsring.

(4.8) Observation. 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 extensionen $\mathfrak{q}R_\mathfrak{m}$. 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 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.

Lidt om algebraisk geometri

I dette kapitel betegner k et fast grundlegeme. Svarende til et fast tal $n \geq 1$ betragtes mængden af punkter i k^n, dvs n-sæt $p = (p_1, \ldots, p_n)$ med $p_i \in k$, og ringen $k[X_1, \ldots, X_n]$ af polynomier i n variable.

1. Affine mangfoldigheder.

(1.1) Definition. Ved indsættelse af et punkt $p = (p_1, \ldots, p_n)$ i et polynomium F fremkommer værdien $F(p) = F(p_1, \ldots, p_n)$. Hvis $F(p) = 0$, så kaldes p et *nulpunkt* for F, og F siges at *forsvinde* i punktet p. For hver mængde $\mathfrak{F}$ af polynomier betegnes med $\mathcal{V}(\mathfrak{F})$ mængden af fælles nulpunkter for polynomierne i $\mathfrak{F}$. Med andre ord er $\mathcal{V}(\mathfrak{F})$ delmængden af k^n bestående af de punkter p for hvilke $F(p) = 0$ for alle polynomier $F \in \mathfrak{F}$.

En delmængde V af k^n, der har formen $\mathcal{V}(\mathfrak{F})$ for en passende delmængde $\mathfrak{F}$ af $k[X_1, \ldots, X_n]$, kaldes en (affin) *(algebraisk) mangfoldighed*. Den siges også at være bestemt ved mængden $\mathfrak{F}$, eller ved ligningerne $F = 0$ for $F \in \mathfrak{F}$.

(1.2) Observation. Enhver mangfoldighed i k^n kan beskrives som mængden af fælles nulpunkter for polynomierne i et ideal i $R = k[X_1, \ldots, X_n]$. Lad nemlig $\mathfrak{F}$ være en mængde af polynomier. Da udgør de polynomier, der kan skrives på formen $G_1F_1 + \cdots + G_lF_l$, hvor $G_i \in R$ og $F_i \in \mathfrak{F}$, et ideal $\mathfrak{I}$, og det er klart, at $\mathcal{V}(\mathfrak{I}) = \mathcal{V}(\mathfrak{F})$.

Enhver mangfoldighed i k^n kan beskrives som mængden af fælles nulpunkter for endelig mange polynomier. Ifølge Hilbert's Basissætning er nemlig hvert ideal $\mathfrak{I}$ i R frembragt af endelig mange polynomier $F_1, \ldots, F_r$, og så følger det, at $\mathcal{V}(\mathfrak{I}) = \mathcal{V}(F_1, \ldots, F_r)$.

(1.3) Definition. For hver delmængde U af k^n betegnes med $\mathcal{I}(U)$ idealet af polynomier, der forsvinder i alle punkter af U. Med andre ord er $\mathcal{I}(U)$ delmængden af $k[X_1, \ldots, X_n]$ bestående af de polynomier F for hvilke $F(p) = 0$ for alle punkter $p \in U$. Det er klart, at den beskrevne mængde af polynomier udgør et ideal i polynomiumsringen.

Et ideal i $k[X_1, \ldots, X_n]$, der er af formen $\mathcal{I}(U)$ for en passende delmængde U af k^n, vil vi kalde et *geometrisk ideal*.

(1.4) Observation. For en delmængde U bestående af et enkelt punkt p består idealet $\mathcal{I}(p)$ af de polynomier der forsvinder i p. Idealet $\mathcal{I}(p)$ er med andre ord kernen for ringhomomorfien $k[X_1, \ldots, X_n] \to k$ defineret ved $F \mapsto F(p)$. Denne ringhomomorfi er surjektiv, så den tilsvarende kvotientring (af polynomier modulo kernen), er

isomorf med k. Da k er et legeme, følger det, at idealet $\mathcal{I}(p)$ er et maximalideal i $k[X_1, \ldots, X_n]$. Det er velkendt, og let at vise, at idealet netop er maksimalidealet,

$$\mathfrak{M}_p = (X_1 - p_1, \ldots, X_n - p_n),$$

frembragt af polynomierne $X_i - p_i$ for $i = 1, \ldots, n$.

Heraf fås en beskrivelse af $\mathcal{I}(U)$ for enhver delmængde U af k^n: Da $F(p) = 0$, hvis og kun hvis $F \in \mathfrak{M}_p$, gælder ligningen,

$$\mathcal{I}(U) = \bigcap_{p \in U} \mathfrak{M}_p.$$

Specielt ses, at de geometriske idealer i $k[X_1, \ldots, X_n]$ netop er de idealer, der er en fællesmængde af maksimalidealer af formen $\mathfrak{M}_p$.

(1.5) Sætning. *Afbildningerne $\mathcal{V}$ og $\mathcal{I}$, defineret på henholdsvis delmængder $\mathfrak{F}$ af $R = k[X_1, \ldots, X_n]$ og delmængder U af k^n, har følgende egenskaber:*

$$\mathcal{V}(\cup \mathfrak{F}_\alpha) = \cap \mathcal{V}(\mathfrak{F}_\alpha), \quad \mathcal{I}(\cup U_\alpha) = \cap \mathcal{I}(U_\alpha), \tag{1.5.1}$$

$$\mathfrak{F} \supseteq \mathfrak{F}' \Rightarrow \mathcal{V}(\mathfrak{F}) \subseteq \mathcal{V}(\mathfrak{F}'), \quad U \supseteq U' \Rightarrow \mathcal{I}(U) \subseteq \mathcal{I}(U'), \tag{1.5.2}$$

$$U \subseteq \mathcal{V}(\mathcal{I}(U)), \quad \mathfrak{F} \subseteq \mathcal{I}(\mathcal{V}(\mathfrak{F})), \tag{1.5.3}$$

$$U \subseteq \mathcal{V}(\mathfrak{F}) \Leftrightarrow \mathcal{I}(U) \supseteq \mathfrak{F}, \tag{1.5.4}$$

$$\mathcal{V}(\mathcal{I}(\mathcal{V}(\mathfrak{F}))) = \mathcal{V}(\mathfrak{F}), \quad \mathcal{I}(\mathcal{V}(\mathcal{I}(U))) = \mathcal{I}(U), \tag{1.5.5}$$

$$\mathcal{V}(\mathfrak{F} \cdot \mathfrak{F}') = \mathcal{V}(\mathfrak{F}) \cup \mathcal{V}(\mathfrak{F}'), \tag{1.5.6}$$

$$\mathcal{V}(R) = \emptyset, \quad \mathcal{I}(\emptyset) = R, \tag{1.5.7}$$

$$\mathcal{V}(0) = k^n, \quad \mathcal{I}(k^n) = (0), \tag{1.5.8}$$

hvor den sidste ligning dog forudsætter, at legemet k er uendeligt.

Bevis. Egenskaberne i (1.5.1), (1.5.2), (1.5.3) og (1.5.4) følger umiddelbart af definitionerne.

Ligningerne (1.5.5) indses således: Lad $\mathfrak{F}$ være en delmængde af $k[X_1, \ldots, X_n]$. Anvend den første egenskab i (1.5.2) på den anden inklusion i (1.5.3). Det følger, at $\mathcal{V}(\mathcal{I}(\mathcal{V}(\mathfrak{F}))) \subseteq \mathcal{V}(\mathfrak{F})$. Her gælder også den omvendte inklusion, hvilket indses ved at anvende den første inklusion i (1.5.3) på $U := \mathcal{V}(\mathfrak{F})$. Altså gælder den første ligning i (1.5.5). Den anden ligning indses analogt.

I (1.5.6) betegner produktet $\mathfrak{F} \cdot \mathfrak{F}'$ delmængden bestående af alle produkter FF', hvor $F \in \mathfrak{F}$ og $F' \in \mathfrak{F}'$. Det er klart, at $(FF')(p) = 0$, hvis og kun hvis $F(p) = 0$ eller $F'(p) = 0$. Heraf følger ligningen i (1.5.6). Ligningerne i (1.5.7) og den første ligning i (1.5.8) gælder trivielt.

Betragt nu den anden ligning i (1.5.8), og antag, at k har uendelig mange elementer. Det påstås, at hvis F er et polynomium, således at $F(p) = 0$ for alle punkter

$p \in k^n$, så er $F = 0$. Denne påstand vises ved induktion efter n. For $n = 1$ er F et polynomium i én variabel, som har hvert element $p \in k$ som rod. Da k har uendelig mange elementer, har F altså uendeligt mange rødder. Heraf følger, at $F = 0$.

Antag, at $n > 1$ og at påstanden gælder for polynomier i $n - 1$ variable. Idet leddene i F ordnes efter potenser af X_n fås en fremstilling,

$$F = F_N(X_1, \ldots, X_{n-1})X_n^N + F_{N-1}(X_1, \ldots, X_{n-1})X_n^{N-1} + \cdots + F_0(X_1, \ldots, X_{n-1}),$$

hvor F_i'erne er polynomier i de variable $X_1, \ldots, X_{n-1}$. Ved indsættelse af et vilkårligt $(n-1)$-sæt $p' = (p_1, \ldots, p_{n-1})$ for disse variable, fås følgende polynomium i den ene variabel X_n:

$$F(p', X_n) = F_N(p')X_n^N + F_{N-1}(p')X_n^{N-1} + \cdots + F_0(p').$$

Ifølge antagelsen vil dette polynomium forsvinde ved indsættelse af enhver værdi p_n for X_n. Af det lige viste for $n = 1$ følger derfor, at dette sidste polynomium er nulpolynomiet. Hver af koefficienterne $F_i(p')$ er altså lig med 0. Her var $p' = (p_1, \ldots, p_{n-1})$ et vilkårligt $(n-1)$-sæt. Polynomiet F_i forsvinder således i ethvert punkt p' af k^{n-1}. Af induktionsforudsætningen følger derfor, at F_i er nulpolynomiet. Følgelig er $F = 0$. ∎

(1.6) Korollar. (1) *Endelig foreningsmængde og vilkårlig fællesmængde af mangfoldigheder er igen mangfoldigheder. Den tomme mængde $\emptyset$ og hele k^n er mangfoldigheder. Hvis $\mathfrak{I}$ og $\mathfrak{J}$ er idealer af polynomier, da er*

$$\mathcal{V}(\mathfrak{I} \cap \mathfrak{J}) = \mathcal{V}(\mathfrak{I}\mathfrak{J}) = \mathcal{V}(\mathfrak{I}) \cup \mathcal{V}(\mathfrak{J}),$$
$$\mathcal{V}(\mathfrak{I} + \mathfrak{J}) = \mathcal{V}(\mathfrak{I}) \cap \mathcal{V}(\mathfrak{J}).$$

(2) *En vilkårlig fællesmængde af geometriske idealer er igen et geometrisk ideal. Polynomiumsringen $k[X_1, \ldots, X_n]$ er et geometrisk ideal. Idealet* (0) *er geometrisk, hvis legemet k er uendeligt.*

Bevis. (1) De første påstande følger umiddelbart af ligningerne i Sætning (1.5). De første ligninger ses således: Som bekendt er $\mathfrak{I} \cap \mathfrak{J} \supseteq \mathfrak{I}\mathfrak{J}$, og produktet $\mathfrak{I}\mathfrak{J}$ af idealer omfatter produktet $\mathfrak{I}\cdot\mathfrak{J}$ af mængder. Af relationerne i Sætning (1.5) fås derfor følgende kæde af inklusioner,

$$\mathcal{V}(\mathfrak{I} \cap \mathfrak{J}) \subseteq \mathcal{V}(\mathfrak{I}\mathfrak{J}) \subseteq \mathcal{V}(\mathfrak{I}\cdot\mathfrak{J}) = \mathcal{V}(\mathfrak{I}) \cup \mathcal{V}(\mathfrak{J}).$$

På den anden side er $\mathfrak{I} \cap \mathfrak{J} \subseteq \mathfrak{I}$, og heraf følger, at $\mathcal{V}(\mathfrak{I}) \subseteq \mathcal{V}(\mathfrak{I} \cap \mathfrak{J})$. En tilsvarende relation fås for $\mathfrak{J}$, og så følger det, at $\mathcal{V}(\mathfrak{I}) \cup \mathcal{V}(\mathfrak{J}) \subseteq \mathcal{V}(\mathfrak{I} \cap \mathfrak{J})$. Heraf sluttes, at alle inklusionerne i kæden ovenfor må være ligheder. Altså gælder de første ligninger i (1). Den sidste ligning i (1) gælder trivielt.

(2) Påstandene følger umiddelbart af sætningen. ∎

(1.7) Sætning. *Afbildningerne $\mathcal{V}$ og $\mathcal{I}$ definerer en bijektiv forbindelse mellem på den ene side mangfoldighederne i k^n og på den anden side de geometriske idealer i $k[X_1, \ldots, X_n]$. Den bijektive forbindelse vender inklusioner, og endelig forening af mangfoldigheder svarer til endelig fællesmængde af geometriske idealer. For hver mangfoldighed V er $\mathcal{V}(\mathcal{I}(V)) = V$ og for hvert geometrisk ideal $\mathfrak{I}$ er $\mathcal{I}(\mathcal{V}(\mathfrak{I})) = \mathfrak{I}$.*

Bevis. Mangfoldighederne V er delmængderne af formen $V = \mathcal{V}(\mathfrak{F})$. Ligningen $\mathcal{V}(\mathcal{I}(V)) = V$ for mangfoldigheder følger derfor umiddelbart af den første ligning i (1.5.5). Tilsvarende følger ligningen $\mathcal{I}(\mathcal{V}(\mathfrak{I})) = \mathfrak{I}$ for geometriske idealer af den anden ligning i (1.5.5). Af de to ligninger følger, at $\mathcal{V}$ og $\mathcal{I}$ er „hinandens inverse“ på de to anførte mængder. De resterende påstande følger nu umiddelbart. ∎

(1.8) Korollar. *Lad U være en vilkårlig delmængde af k^n. Da er mangfoldigheden $W := \mathcal{V}(\mathcal{I}(U))$ den mindste mangfoldighed, der indeholder U, og $\mathcal{I}(W) = \mathcal{I}(U)$.*

Bevis. Lad V være en mangfoldighed, og sæt $\mathfrak{I} := \mathcal{I}(V)$. Det følger af Sætningen, at $V = \mathcal{V}(\mathfrak{I})$. Af (1.5.4) følger derfor, at $V \supseteq U$, hvis og kun hvis $\mathfrak{I} \subseteq \mathcal{I}(U)$. Den sidste betingelse er, ifølge Sætningen, ensbetydende med at $V \supseteq W$. Den søgte ligning følger umiddelbart af den anden ligning i (1.5.5). ∎

(1.9) Korollar. *Den nedstigende kædes egenskab gælder for mangfoldighederne i k^n. Med andre ord: I enhver uendelig kæde af mangfoldigheder,*

$$V_1 \supseteq V_2 \supseteq V_3 \supseteq \cdots,$$

gælder lighedstegnet fra et vist trin. Og ækvivalent: I enhver ikke-tom mængde $\mathcal{S}$ af mangfoldigheder findes en mangfoldighed, der er minimal blandt mangfoldighederne i $\mathcal{S}$.

Bevis. Ifølge Sætning (1.7) svarer påstandene om mangfoldigheder til tilsvarende påstande om (visse) idealer i $k[X_1, \ldots, X_n]$. Da ringen $k[X_1, \ldots, X_n]$ er noethersk ifølge Hilbert's Basissætning, gælder påstandene. ∎

(1.10) Definition. Lad V være en mangfoldighed. Hvert polynomium F definerer da en *polynomiumsfunktion* $F_V : V \to k$, nemlig afbildningen bestemt ved

$$F_V(p) = F(p) \quad \text{for } p \in V.$$

Polynomiumsfunktionerne på V udgør øjensynlig en ring, endda en k-algebra. Den betegnes $\Gamma(V)$. Specielle polynomiumsfunktioner på V er de n *koordinatfunktioner på* V, dvs funktionerne,

$$v_i : p \mapsto p_i \quad \text{for } p \in V.$$

Afbildningen $F \mapsto F_V$, der til et polynomium F lader svare den tilhørende polynomiumsfunktion F_V, er en surjektiv k-lineær ringhomorfi $k[X_1, \ldots, X_n] \to \Gamma(V)$. Ved denne homomorfi afbildes polynomiet X_i på koordinatfunktionen v_i. Som k-algebra er $\Gamma(V)$ derfor frembragt af de n koordinatfunktioner v_i,

$$\Gamma(V) = k[v_1, \ldots, v_n].$$

Ringen $\Gamma(V)$ af polynomiumsfunktioner på V kaldes også *koordinatringen for* V.

(1.11) Observation. Lad V være en mangfoldighed. Øjensynlig forsvinder et polynomium F i alle punkter $p \in V$, hvis og kun hvis funktionen F_V er nul-funktionen. Idealet $\mathcal{I}(V)$ er altså kernen for homomorfien $F \mapsto F_V$, og homomorfiens billede er netop ringen af polynomiumsfunktioner på V. Isomorfisætningen for ringe bestemmer derfor en naturlig isomorfi,

$$k[X_1, \ldots, X_n]/\mathcal{I}(V) \xrightarrow{\sim} \Gamma(V)\,. \tag{1.11.1}$$

Ved denne isomorfi svarer restklassen $\hat{X}_i$ til koordinatfunktionen v_i.

(1.12) Korollar. *Lad V og W være mangfoldigheder i k^n således at $W \subset V$. Da findes en polynomiumsfunktion på V, som ikke er nul-funktionen og som forsvinder på W.*

Bevis. Det følger af den bijektive forbindelse i Sætning (1.7), at $\mathcal{I}(V) \subset \mathcal{I}(W)$. Vælg et polynomium F, der tilhører $\mathcal{I}(W)$, men ikke $\mathcal{I}(V)$. Da $F \notin \mathcal{I}(V)$ er F_V ikke nul-funktionen. Da $F \in \mathcal{I}(W)$, er restriktionen F_W nul-funktionen på W. ∎

(1.13) Definition. En mangfoldighed V kaldes *reducibel*, hvis V er den tomme mangfoldighed eller V kan skrives som en foreningsmængde, $V = V_1 \cup V_2$, af to mangfoldigheder, der begge er ægte indeholdt i V. En *irreducibel* mangfoldighed, dvs en mangfoldighed der ikke er reducibel, kaldes også en *varietet*.

(1.14) Sætning. *For en mangfoldighed V er følgende betingelser ækvivalente:*

(i) *Mangfoldigheden V er irreducibel.*
(ii) *Idealet $\mathcal{I}(V)$ er et primideal i $k[X_1, \ldots, X_n]$.*
(iii) *Koordinatringen $\Gamma(V)$ er et integritetsområde.*

Bevis. Da $k[X_1, \ldots, X_n]/\mathcal{I}(V) \xrightarrow{\sim} \Gamma(V)$, jfr (1.11.1), følger det umiddelbart, at (ii) og (iii) er ensbetydende.

(i) $\Rightarrow$ (iii): Ringen $\Gamma(V)$ er ikke nul-ringen, thi ringen $\Gamma(V)$ er nul-ringen, hvis og kun hvis $1 \in \mathcal{I}(V)$, og dette gælder kun når $V = \emptyset$.

Det skal videre vises, at nulreglen gælder i $\Gamma(V)$. Antag altså, at f_1 og f_2 er polynomiumsfunktioner på V og at produktet $f_1 f_2$ er nul-funktionen. Lad V_i betegne delmængden bestående af de punkter p i V, hvor $f_i(p) = 0$. Da er V_i en mangfoldighed. Funktionen f_i er nemlig af formen $f_i = (F_i)_V$, hvor F_i er et polynomium, og V er mængden af fælles nulpunkter for en mængde $\mathfrak{F}$ af polynomier, og så er V_i øjensynlig mængden af fælles nulpunkter for mængden $\mathfrak{F} \cup \{F_i\}$. Videre er $V = V_1 \cup V_2$, da produktet $f_1 f_2$ er nul-funktionen. Da V er antaget irreducibel, følger det, at V er lig med et af V_i'erne. At $V = V_i$ betyder netop, at $f_i(p) = 0$ for alle $p \in V$, altså at f_i er nul-funktionen. Altså er et af f_i'erne lig med 0. Hermed er nul-reglen for $\Gamma(V)$ eftervist.

(iii) $\Rightarrow$ (i): Mangfoldigheden V er ikke tom, thi da et integritetsområde ikke er nul-ringen, er funktionerne 1 og 0 forskellige funktioner på V.

Antag videre, at $V = V_1 \cup V_2$ er en foreningsmængde af mangfoldigheder. Det skal vises, at et af V_i'erne er lig med V. Antag, indirekte, at $V_i \subset V$ for $i = 1, 2$. Det følger da af Korollar (1.12), at der findes polynomiumsfunktioner $f_i \neq 0$, så at f_i er nul-funktionen på V_i. Da $V = V_1 \cup V_2$ følger det, at produktfunktionen $f_1 f_2$ er lig med 0. Men dette er den ønskede modstrid, idet nul-reglen gælder i integritetsområdet $\Gamma(V)$. ∎

(1.15) Sætning. *Enhver mangfoldighed V i k^n har en fremstilling som en endelig forening af irreducible mangfoldigheder,*

$$V = V_1 \cup \cdots \cup V_r. \tag{1.15.1}$$

For en sådan fremstilling gælder, at hvis W er en irreducibel mangfoldighed indeholdt i V, da er W indeholdt i et af V_i'erne.

Bevis. Eksistensen af fremstillingen vises ved en såkaldt noethersk induktion. Beviset er indirekte: Antag, at der findes mangfoldigheder, der ikke er en endelig foreningsmængde af irreducible mangfoldigheder. Mængden $\mathcal{S}$ af sådanne mangfoldigheder er da ikke-tom. Ifølge Korollar (1.9) findes da en mangfoldighed V i $\mathcal{S}$, der er minimal blandt mangfoldighederne i $\mathcal{S}$. Da $V \in \mathcal{S}$, kan V specielt ikke selv være irreducibel. Desuden er $V \neq \emptyset$, da den tomme mangfoldighed har en fremstilling af den ønskede form (nemlig som en forening af ingen irreducible mangfoldigheder). Da V er reducibel og ikke-tom, er V en foreningsmængde, $V = V' \cup V''$, af mangfoldigheder, der begge er strengt indeholdt i V. Da $V' \subset V$ og V er minimal i mængden $\mathcal{S}$, kan V' ikke tilhøre $\mathcal{S}$. Altså er V' en endelig forening af irreducible mangfoldigheder. Tilsvarede er V'' en endelig forening af irreducible mangfoldigheder. Men så er også $V = V' \cup V''$ en endelig forening af irreducible mangfoldigheder, i modstrid med at V var element i $\mathcal{S}$. Hermed er eksistensen af fremstillingen bevist.

Betragt nu en fremstilling (1.15.1), og lad $W \subseteq V$ være en irreducibel mangfoldighed. Da $W \subseteq V$ fås følgende ligning,

$$W = (W \cap V_1) \cup \cdots \cup (W \cap V_r).$$

Da W er irreducibel, følger det af ligningen, at W er lig med en af mangfoldighederne $W \cap V_i$ på ligningens højreside. Af $W = W \cap V_i$ følger $W \subseteq V_i$, som ønsket. ∎

(1.16) Definition. Lad V være en mangfoldighed, og betragt en fremstilling (1.15.1). I denne fremstilling kan man bortkaste hvert V_i, der er indeholdt i et af de øvrige. Det følger af Sætning (1.15), at de tiloversblevne V_i'er netop er de maksimale blandt de mangfoldigheder, der er irreducible og indeholdt i V. De kaldes også for V's *komponenter*. Den fremstilling af V, der fremkommer når overflødige V_i'er bortkastes, er entydig, idet de tiloversblevne V_i'erne netop er V's komponenter.

2. Morfier.

(2.1) Definition. Lad V være en mangfoldighed i k^n og lad W være en mangfoldighed i k^m. En afbildning $g\colon W \to V$, der er af formen,

$$g(q) = (G_1(q), \ldots, G_n(q)) \quad \text{for } q \in W,$$

hvor G_i'erne er polynomier i m variable, siges at være en *algebraisk afbildning*, eller at være en *morfi* fra W til V. Betingelsen er, at afbildningens n *koordinatfunktioner*, dvs funktionerne $g_i(q) = G_i(q)$ for $i = 1, \ldots, n$, er polynomiumsfunktioner på W og at afbildningen ind i k^n bestemt ved disse koordinatfunktioner afbilder ind i delmængden $V \subseteq k^n$.

For en morfi g er billedmængden gW sædvanligvis ikke en mangfoldighed i k^n. Den mindste mangfoldighed i k^n, som indeholder billedmængden, jfr Korollar (1.8), kaldes *billedmangfoldigheden*, og betegnes $\overline{gW}$.

(2.2) Observation. De n koordinatfunktioner v_i på V er polynomiumsfunktioner $V \to k$, og de er netop koordinaterne for inklusionsafbildningen $V \to k^n$. Inklusionsafbildningen er altså en morfi. Mere generelt følger det, at hvis V er indeholdt i en mangfoldighed V', så er inklusionsafbildningen $V \to V'$ en morfi.

(2.3) Sætning. *Lad W være en mangfoldighed i k^m, og lad $g\colon W \to k^n$ være morfien svarende til et sæt af n polynomiumsfunktioner $g_1, \ldots, g_n$ på W. Da gælder:*

(1) *For hver mangfoldighed V i k^n er originalmængden $g^{-1}(V)$ en mangfoldighed.*

(2) *Idealet $\mathcal{I}(\overline{gW})$ af polynomier, der forsvinder på billedmangfoldigheden $\overline{gW}$, består af de polynomier F i $k[X_1, \ldots, X_n]$, som opfylder ligningen,*

$$F(g_1, \ldots, g_n) = 0. \qquad (*)$$

(3) *Lad V være en mangfoldighed i k^n bestemt ved delmængden $\mathfrak{F}$ af $k[X_1, \ldots, X_n]$. Da er g en morfi $W \to V$, hvis og kun hvis ligningen $(*)$ gælder for alle F i $\mathfrak{F}$.*

Bevis. (1) Afbildningens koordinatfunktioner er polynomiumsfunktioner på W, dvs af formen $g_i = (G_i)_W$, hvor G_i'erne er polynomier i m variable. Antag nu, at V er bestemt ved mængden $\mathfrak{F}$ af polynomier i $k[X_1, \ldots, X_n]$. Et punkt q i W vil da tilhøre originalmængden $g^{-1}(V)$, hvis og kun hvis der for billedpunktet $g(q)$ gælder, at $F(g(q)) = 0$ for alle $F \in \mathfrak{F}$. Funktionsværdien $F(g(q))$ fås øjensynlig ved at indsætte q i polynomiet $F(G_1, \ldots, G_n)$. De fælles nulpunkter for polynomierne af denne form, for $F \in \mathfrak{F}$, udgør en mangfoldighed i k^m. Da originalmængden $g^{-1}(V)$ er fællesmængden af denne mangfoldighed og W, er originalmængden en mangfoldighed.

(2) Idealet $\mathcal{I}(\overline{gW})$ for billedmangfoldigheden er ifølge Korollar (1.8) netop lig med idealet af polynomier, der forsvinder på billedmængden gW. Det påstås altså, at ligningen $(*)$ er opfyldt, hvis og kun hvis F forsvinder på billedmængden gW. Venstresiden i ligningen $(*)$ er element i $\Gamma(W)$, altså en polynomiumsfunktion på W.

Det er klart, at denne funktions værdi i punktet q netop fås ved indsættelse af $g(q)$ i polynomiet F. Heraf følger påstanden umiddelbart.

(3) Antag, at $V = \mathcal{V}(\mathfrak{F})$. At g definerer en morfi $W \to V$ betyder at billedmængden gW er indeholdt i V. Af egenskaben (1.5.3) følger, at $g(W) \subseteq V$, hvis og kun hvis $\mathfrak{F} \subseteq \mathcal{I}(g(W))$. Påstanden følger derfor umiddelbart af (2). ∎

(2.4) Definition. Lad $g\colon W \to V$ være en morfi. Det følger umiddelbart af definitionen, at hvis $f\colon V \to k$ er en polynomiumsfunktion på V, så er den sammensatte afbildning fg en polynomiumsfunktion på W. Morfien g inducerer altså en homomorfi af k-algebraer $\theta\colon \Gamma(V) \to \Gamma(W)$, kaldet den *associerede homomorfi*.

Hvis v_i er den i'te koordinatfunktion på V, jfr Definition (1.10), så er $v_i g$ øjensynlig den i'te koordinatfunktion for morfien g. Homomorfien θ afbilder altså v_i på funktionen g_i.

(2.5) Korollar. *Afbildningen, der til hver morfi $g\colon W \to V$ knytter den associerede homomorfi af k-algebraer $\theta\colon \Gamma(V) \to \Gamma(W)$, er bijektiv.*

Bevis. Ringen $\Gamma(V)$ af polynomiumsfunktioner på V er frembragt som k-algebra af koordinatfunktionerne v_i,

$$\Gamma(V) = k[v_1, \ldots, v_n].$$

Heraf ses, at en homomorfi θ af k-algebraer fra $\Gamma(V)$ til $\Gamma(W)$ er helt bestemt ved sættet af billeder, $g_i = \theta(v_i)$ for $i = 1, \ldots, n$. Dette sæt af billeder kan ikke foreskrives vilkårligt; af isomorfien (1.11.1) ses, at et foreskrevet sæt $g_1, \ldots, g_n$ af billeder definerer en homomorfi af k-algebraer, hvis og kun hvis følgende betingelse er opfyldt:

$$F(g_1, \ldots, g_n) = 0 \quad \text{for alle } F \in \mathcal{I}(V). \tag{$*$}$$

På den anden side svarer sæt af n polynomiumsfunktioner $g_1, \ldots, g_n$ på W til morfier $W \to k^n$. Et sådant sæt definerer en morfi $W \to V$, hvis og kun hvis afbildningen $W \to k^n$ afbilder ind i V. Da $V = \mathcal{V}(\mathcal{I}(V))$ følger det af Sætning (2.3)(3), at afbildningen afbilder ind i V, hvis og kun hvis betingelsen $(*)$ er opfyldt.

Hermed er den bijektive forbindelse etableret. ∎

(2.6) Bemærkning. Det er klart, at den bijektive forbindelse mellem morfier af mangfoldigheder og homomorfier af k-algebraer respekterer sammensætning: Er $g'\colon V \to V'$ endnu en morfi, svarende til algebrahomomorfien $\theta'\colon \Gamma(V') \to \Gamma(V)$, så svarer den sammensatte morfi $g'g\colon W \to V'$ til den sammensatte homomorfi $\theta\theta'\colon \Gamma(V') \to \Gamma(W)$.

En morfi $g\colon W \to V$ kaldes en *isomorfi*, hvis der findes en morfi $\psi\colon V \to W$, som opfylder at $g\psi = 1_V$ og $\psi g = 1_W$. Det er klart, at g er en isomorfi, hvis og kun hvis g er bijektiv og den inverse afbildning g^{-1} igen er en morfi. Det følger af Sætningen, at morfien g er en isomorfi, hvis og kun hvis den tilhørende homomorfi af k-algebraer er en isomorfi (dvs bijektiv).

(2.7) Bemærkning. Lad $g\colon W \to V$ være en morfi af mangfoldigheder. Betragt billedet for den tilhørende homomorfi af k-algebraer $\theta\colon \Gamma(V) \to \Gamma(W)$. Billedet ændres ikke når θ sammensættes med den surjektive homomorfi $k[X_1, \ldots, X_n] \to \Gamma(V)$. Af Sætning (2.3)(2) følger, at homomorfien $k[X_1, \ldots, X_n] \to \Gamma(W)$ har kernen $\mathcal{I}(\overline{gW})$. Af Isomorfisætningen og isomorfien (1.11.1) følger derfor, at billedet er kanonisk isomorft med koordinatringen $\Gamma(\overline{gW})$. Homomorfien θ er derfor en sammensætning,

$$\Gamma(V) \to \Gamma(\overline{gW}) \to \Gamma(W),$$

hvor den første homomorfi svarer til den surjektive homomorfi på billedet og den anden svarer til inklusionen af billedet i $\Gamma(W)$.

På den anden side er morfien g øjensynlig en sammensætning af morfier,

$$W \to \overline{gW} \to V,$$

hvor den sidste morfi er inklusionen af $\overline{gW}$ i V. Det er let at se, at de to „faktoriseringer" svarer til hinanden: Til morfien $W \to \overline{gW}$ svarer den injektive inklusion af billedalgebraen, $\Gamma(\overline{gW}) \to \Gamma(W)$; til inklusionsmorfien $\overline{gW} \to V$ svarer den surjektive homomorfi på billedalgebraen, $\Gamma(V) \to \Gamma(\overline{gW})$.

Specielt aflæses: *Den associerede homomorfi θ er surjektiv, hvis og kun hvis morfien g er en isomorfi af W på en mangfoldighed indeholdt i V.* Er dette tilfældet, kaldes g en *indlejring* af W i V.

Og videre: *Den associerede homomorfi θ er injektiv, hvis og kun hvis mangfoldigheden V er den mindste mangfoldighed i k^n, som indeholder billedmængden $g(W)$.* I dette tilfælde siges g at være en *dominerende morfi*.

(2.8) Notation. Som nævnt i beviset for Lemma (2.3) er en homomorfi af k-algebraer $\theta\colon \Gamma(V) \to \Gamma(W)$ helt bestemt ved værdierne $\theta(v_i) = g_i$, som tilhører koordinatringen $\Gamma(W)$. Hvis $w_1, \ldots, w_m$ betegner koordinatfunktionerne på W, så er $\Gamma(W) = k[w_1, \ldots, w_m]$, og værdierne er altså polynomier i w_j'erne. Ligningerne har altså formen,

$$\theta(v_i) = G_i(w_1, \ldots, w_m) \quad \text{for } i = 1, \ldots, n, \tag{2.8.1}$$

hvor G_i'erne er polynomier i m variable. Men det skal understreges, at disse ligninger ikke kan foreskrives vilkårligt. Betingelsen er, at højresiderne $g_i = G_i(w_1, \ldots, w_m)$ opfylder, at $F(g_1, \ldots, g_n) = 0$ for ethvert polynomium F i en mængde af polynomier $\mathfrak{F}$, der bestemmer V.

Bemærk, at hvis denne betingelse er opfyldt, så beskrives den tilhørende morfi $W \to V$ ud fra ligningerne (2.8.1) på følgende måde: Et punkt i W, med w-koordinaterne $(w_1, \ldots, w_m)$ afbildes på det punkt i V, hvis v-koordinater er bestemt ved ligningerne,

$$v_i = G_i(w_1, \ldots, w_m) \quad \text{for } i = 1, \ldots, n. \tag{2.8.2}$$

Her er der sket en forkastelig, men i praksis særdeles anvendelig, sammenblanding af notation: I (2.8.1) betegner w_j'erne og v_i'erne koordinatfunktioner, i (2.8.2) er disse betegnelser brugt om koordinaterne for et punkt i W og dets tilhørende billedpunkt i V. Vi vil naturligvis ofte anvende denne forkastelige sammenblanding, og sige, at morfien g er defineret ved ligningerne (2.8.2).

(2.9) Eksempel. Antag, at k er et uendeligt legeme. Polynomiumsringen $k[t]$ er da koordinatringen for mangfoldigheden $W = k$. Betragt yderligere mangfoldigheden V i k^2 med ligningen $Y^2 = X^3$. Idet x og y betegner de to koordinatfunktioner på V, er $y^2 = x^3$.

De to polynomier $g = t^2$ og $h = t^3$ i $\Gamma(k)$ bestemmer en morfi $k \to k^2$. Den associerede homomorfi af algebraer $k[X, Y] \to k[t]$ er bestemt ved $X \mapsto g$, $Y \mapsto h$. Øjensynlig er $h^2 = g^3$. Af Sætning (2.3)(3) følger derfor, at afbildningen afbilder ind i V. Afbildningen er altså en morfi $k \to V$. Den siges at være bestemt ved ligningerne,

$$x = t^2, \quad y = t^3.$$

Idealet svarende til billedmangfoldigheden er ifølge Sætning (2.3)(2) netop kernen for homomorfien $k[X, Y] \to k[t]$. Som nævnt vil kernen indeholde $Y^2 - X^3$; det er ikke svært at vise, at kernen netop er hovedidealet $(Y^2 - X^3)$. Af sætningen følger derfor, at dette hovedideal er et geometrisk ideal, og herefter videre, at hovedidealet netop er idealet $\mathcal{I}(V)$. Endelig følger det, at V netop er billedmangfoldigheden.

Bemærk, at morfien $k \to V$ er en bijektiv afbildning (hvorfor?), men ikke en isomorfi af mangfoldigheder (hvorfor?).

3. Nulpunktssætningen.

(3.1) Hilbert's Nulpunktssætning, version 2. *Antag, at legemet k er algebraisk afsluttet. Da gælder:* (1) *Maksimalidealerne i $k[X_1, \ldots, X_n]$ er netop idealerne af formen $\mathfrak{M}_p = (X_1 - p_1, \ldots, X_n - p_n)$ for $p \in k^n$.*

(2) *Hvis idealet $\mathfrak{I}$ ikke er hele polynomiumsringen $k[X_1, \ldots, X_n]$, så har polynomierne i $\mathfrak{I}$ et fælles nulpunkt.*

(3) *For hvert ideal $\mathfrak{I}$ i $k[X_1, \ldots, X_n]$ gælder formlen,*

$$\mathcal{I}(\mathcal{V}(\mathfrak{I})) = \operatorname{Rad}\mathfrak{I}.$$

Bevis. (1) Lad $\mathfrak{M}$ være et maksimalideal i $k[X_1, \ldots, X_n]$. Betragt kvotientringen $A := k[X_1, \ldots, X_n]/\mathfrak{M}$. På den ene side er A, som kvotient af polynomiumsringen, en endelig frembragt algebra over k. På den anden side er A et legeme, da $\mathfrak{M}$ er et maksimalideal. Af Hilbert's Nulpunktssætning, version 1, følger derfor, at A er endeligdimensional som vektorrum over k. Da k er et algebraisk afsluttet legeme, følger det videre, at A er lig med k, eller – mere præcist – at homorfien $k \to A$ er en isomorfi. Homomorfien er altså specielt surjektiv, så for $i = 1, \ldots, n$ vil restklasserne $\hat{X}_i$ i A derfor tilhøre billedet ved homomorfien. Der findes altså elementer p_i i k, så at $\hat{X}_i = \hat{p}_i$. Denne ligning i A betyder, at restklassen af $X_i - p_i$ modulo $\mathfrak{M}$ er lig med 0. Altså er $X_i - p_i$ element i $\mathfrak{M}$. Det følger, at idealet $\mathfrak{M}_p$ er indeholdt i $\mathfrak{M}$. Da $\mathfrak{M}_p$ øjensynlig er et maksimalideal, følger det endelig, at $\mathfrak{M}_p = \mathfrak{M}$, som ønsket.

(2) Antag, at idealet $\mathfrak{I}$ ikke er hele polynomiumsringen. Ifølge Eksistenssætningen findes da et maksimalideal $\mathfrak{M}$ i $k[X_1, \ldots, X_n]$, således at $\mathfrak{I} \subseteq \mathfrak{M}$. Ifølge (1) er $\mathfrak{M} = \mathfrak{M}_p$ for et punkt p i k^n. Inklusionen $\mathfrak{I} \subseteq \mathfrak{M}_p$ betyder netop at p er fælles nulpunkt for alle polynomierne i $\mathfrak{I}$, jfr Observation (1.4). Hermed er (2) bevist.

(3) Sæt $V := \mathcal{V}(\mathfrak{I})$. Ligningens venstreside er da idealet $\mathcal{I}(V)$ af polynomier, der forsvinder på V. Først vises, at ligningens højreside er indeholdt i venstresiden. Antag, at F tilhører højresiden $\operatorname{Rad}\mathfrak{I}$, altså at der findes en potens F^n som tilhører $\mathfrak{I}$. Ifølge (1.5.3) er $\mathfrak{I} \subseteq \mathcal{I}(V)$. Da $F^n \in \mathfrak{I}$, vil potensen F^n altså forsvinde i alle punkter af V. For hvert punkt p er $F^n(p) = F(p)^n$ og da værdien $F(p)$ tilhører legemet k, er $F(p) = 0$ hvis og kun hvis $F(p)^n = 0$. Da potensen F^n forsvinder i alle punkter af V, vil altså også F forsvinde i alle punkter af V. Og det betyder netop, at F tilhører ligningens venstreside.

Den modsatte inklusion vises således. Antag, at polynomiet F ikke tilhører højresiden $\operatorname{Rad}\mathfrak{I}$. Da vil ingen af potenserne F^i tilhøre idealet $\mathfrak{I}$. Betragt kvotienten $R := k[X_1, \ldots, X_n]/\mathfrak{I}$, og lad $f \in R$ betegne restklassen af F modulo $\mathfrak{I}$. Da er alle potenserne f^i forskellige fra 0. Brøkringen R_f er altså forskellig fra nulringen. Ifølge Eksistenssætningen findes derfor et maksimalideal $\mathfrak{m}$ i R_f. Ifølge Lokaliseringsprincippet kontraheres $\mathfrak{m}$ til et primideal i R, som ikke indeholder f, og ifølge Kvotientprincippet kontraheres dette primideal i kvotienten R til et primideal $\mathfrak{P}$ i $k[X_1, \ldots, X_n]$, som indeholder $\mathfrak{I}$ og ikke indeholder F. Altså er

$$\mathfrak{I} \subseteq \mathfrak{P} \quad \text{og} \quad F \notin \mathfrak{P}. \qquad (*)$$

På den anden side er kvotienten $R_f/\mathfrak{m}$ et legeme og en endelig frembragt algebra over k (nemlig frembragt af billederne af X_i og af brøken $1/f$). Af Hilbert's Nulpunktssætning, version 1, følger derfor at kvotienten $R_f/\mathfrak{m}$ er endeligdimensional over k. Da k er algebraisk afsluttet følger det videre, at kvotienten $R_f/\mathfrak{m}$ er lig med k. Specielt findes for $i = 1, \ldots, n$ elementer $p_i \in k$ således at X_i og p_i har samme billede ved den sammensatte homomorfi,

$$k[X_1, \ldots, X_n] \to R \to R_f \to R_f/\mathfrak{m}\,.$$

Kernen for denne sammensatte homomorfi er netop kontraktionen $\mathfrak{P}$. Polynomierne $X_i - p_i$ tilhører derfor $\mathfrak{P}$. Heraf følger, at $\mathfrak{M}_p \subseteq \mathfrak{P}$. Da $\mathfrak{M}_p$ er et maksimalideal, følger det videre, at $\mathfrak{P} = \mathfrak{M}_p$.

Nu viser den første relation i $(*)$ at $\mathfrak{I} \subseteq \mathfrak{M}_p$, og den anden at $F \notin \mathfrak{M}_p$. Heraf følger, at p tilhører V og at $F(p) \neq 0$. Polynomiet F forsvinder derfor ikke i alle punkter af V. Altså er F ikke element i venstresiden.

Hermed er den modsatte inklusion vist, og beviset for Nulpunktssætningen afsluttet. ∎

(3.2) Korollar. *Antag, at k er algebraisk afsluttet. Da er de geometriske idealer netop radikalidealerne i $k[X_1, \ldots, X_n]$, dvs de idealer, der er lig med deres eget radikal. Ved den bijektive forbindelse fra* (1.7) *svarer primidealerne i $k[X_1, \ldots, X_n]$ netop til de irreducible mangfoldigheder i k^n, og de uforkortelige fremstillinger af mangfoldigheder som forening af endelig mange irreducible mangfoldigheder svarer til uforkortelige fremstillinger af radikalidealer som endelig fællesmængde af primidealer.*

Bevis. Påstanden følger umiddelbart af Nulpunktssætningen, idet primidealer øjensynlig er radikalidealer. ∎

(3.3) Definition. En mangfoldighed H i k^n, der kan beskrives som mængden af nulpunkter, $H = \mathcal{V}(F)$, af ét ikke-konstant polynomium F i $k[X_1, \ldots, X_n]$ kaldes, når k er algebraisk afsluttet, en (reduceret) *hyperflade*.

Det følger af Nulpunktssætningen, at en hyperflade ikke kan være den tomme mangfoldighed. Da et algebraisk afsluttet legeme er uendeligt, er k^n ikke selv en hyperflade i k^n. (Men k^n kan naturligvis opfattes som hyperfladen i k^{n+1} bestemt ved ligningen $X_{n+1} = 0$.)

(3.4) Sætning. *Antag, at k er algebraisk afsluttet. De irreducible hyperflader i k^n er netop mangfoldighederne af formen $\mathcal{V}(P)$, hvor P er et irreducibelt polynomium. Lad $H = \mathcal{V}(F)$ være hyperfladen bestemt ved et polynomium F med primopløsningen,*

$$F = P_1^{m_1} \cdots P_q^{m_q}$$

(hvor P_j'erne er forskellige (ikke-associerede) irreducible polynomier og $m_j \geq 1$). Da er H's komponenter hyperfladerne $\mathcal{V}(P_j)$, og idealet $\mathcal{I}(H)$ er lig med hovedidealet $(P_1 \cdots P_q)$.

Bevis. Det er velkendt, at polynomiumsringen $k[X_1, \ldots, X_n]$ er en faktoriel ring. Heraf følger, at hovedidealet (P) frembragt af et irreducibelt polynomium P er et primideal. Det følger videre af den entydige primopløsning, at

$$\mathrm{Rad}(F) = (P_1 \cdots P_q) = (P_1) \cap \cdots \cap (P_q).$$

Korollar (3.2) viser nu først, at hyperfladen $\mathcal{V}(P)$ bestemt ved et irreducibelt polynomium P er irreducibel, og videre, at

$$\mathcal{V}(F) = \mathcal{V}(P_1) \cup \cdots \cup \mathcal{V}(P_q)$$

er fremstillingen af $\mathcal{V}(F)$ som foreningsmængde af irreducible mangfoldigheder. Heraf følger de resterende påstande let. ∎

(3.5) Bemærkning. Lad V være en mangfoldighed i k^n, og betragt ringen $\Gamma(V)$ af polynomiumsfunktioner på V. For hver delmængde $U \subseteq V$ kan vi da betragte idealet $\mathcal{I}_V(U)$ af de funktioner i $\Gamma(V)$, der forsvinder på U, og for hvert ideal $\mathfrak{I}$ i $\Gamma(V)$ kan vi betragte mængden $\mathcal{V}(\mathfrak{I})$ af fælles nulpunkter for funktionerne i $\mathfrak{I}$. Herved etableres en bijektiv forbindelse mellem på den ene side de mangfoldigheder W, der er indeholdt i V, og på den anden side visse (såkaldte) geometriske idealer i $\Gamma(V)$. Mere præcist: $\Gamma(V) = k[X_1, \ldots, X_n]/\mathcal{I}(V)$, så ifølge Noether's anden Isomorfisætning svarer idealer i $\Gamma(V)$ til idealer $\mathfrak{I} \supseteq \mathcal{I}(V)$, og ved denne forbindelse svarer geometriske idealer i $\Gamma(V)$ til geometriske idealer i $k[X_1, \ldots, X_n]$, som omfatter $\mathcal{I}(V)$.

Til et punkt p i V svarer specielt maksimalidealet $\mathfrak{M}_{V,p}$ bestående af de funktioner i $\Gamma(V)$, der forsvinder i p. Brøkringen, der fremkommer ved lokalisering af $\Gamma(V)$ i maksimalidealet $\mathfrak{M}_{V,p}$, kaldes *den lokale ring for V i punktet p*, og den betegnes $\mathcal{O}_{V,p}$. Den består af brøker f/g, hvor f og g er funktioner i $\Gamma(V)$ og $g(p) \neq 0$. Ifølge Lokaliseringsprincippet er $\mathcal{O}_{V,p}$ en lokal ring, og maksimalidealet består af brøker der kan skrives på formen f/g, hvor $f(p) = 0$. Maksimalidealet i $\mathcal{O}_{V,p}$ betegnes også $\mathfrak{m}_{V,p}$. Bemærk, at restklasselegemet $\mathcal{O}_{V,p}/\mathfrak{m}_{V,p}$ er lig med k, idet $\Gamma(V)/\mathfrak{M}_{V,p}$ var legemet k.

Hvert ideal $\mathfrak{I}$ i $\Gamma(V)$ har en extension til brøkringen $\mathcal{O}_{V,p}$. Hvis $\mathfrak{I}$ ikke er indeholdt i $\mathfrak{M}_{V,p}$, dvs hvis idealet indeholder en funktion g således at $g(p) \neq 0$, så bliver extensionen hele ringen $\mathcal{O}_{V,p}$. I modsat fald, dvs hvis alle funktioner i $\mathfrak{I}$ forsvinder i punktet p, så er extensionen indeholdt i $\mathfrak{m}_{V,p}$. For et geometrisk ideal i $\Gamma(V)$ svarende til en mangfoldighed $W \subseteq V$ er den sidste betingelse, at $p \in W$. Det er ikke svært at vise, at mangfoldigheder W således at $p \in W \subseteq V$ herved svarer bijektivt til visse (geometriske) idealer i $\mathcal{O}_{V,p}$.

Hvis k er algebraisk afsluttet, forenkles denne forbindelse: Der er en bijektiv forbindelse mellem primidealer $\mathfrak{P}$ i $\Gamma(V)$ og irreducible mangfoldigheder $W \subseteq V$, og yderligere en bijektiv forbindelse mellem primidealer $\mathfrak{p}$ i $\mathcal{O}_{V,p}$ og irreducible mangfoldigheder W således at $p \in W \subseteq V$. Disse påstande følger af Kvotientprincippet og Lokaliseringsprincippet under brug af Korollar (3.2).

4. Skemaer.

(4.1) Definition. Ved et *punkt* i $\mathbf{A}^n$ forstås i det følgende et maksimalideal i polynomiumsringen $k[X_1, \ldots, X_n]$.

Maksimalidealerne af formen $\mathfrak{M}_p$ for $p \in k^n$ er ifølge definitionen punkter i $\mathbf{A}^n$. De kaldes også *rationale punkter* i $\mathbf{A}^n$. Hvis legemet k er algebraisk afsluttet, så følger det af Hilbert's Nulpunktssætning, version 2, at alle punkter er rationale.

På trods af ordlyden i definitionen vil vi aldrig opfatte et punkt i $\mathbf{A}^n$ som værende et maksimalideal i $k[X_1, \ldots, X_n]$. Definitionen skal opfattes således at den fastlægger en bijektiv forbindelse mellem på den ene side punkter i $\mathbf{A}^n$ og på den anden side maksimalidealer i $k[X_1, \ldots, X_n]$. Punkterne p i k^n opfattes herved som de rationale punkter i $\mathbf{A}^n$. I analogi med betegnelsen for rationale punkter vil maksimalidealet, der svarer til et givet punkt p i $\mathbf{A}^n$, blive betegnet $\mathfrak{M}_p$.

Lad p være et punkt i $\mathbf{A}^n$. Da idealet $\mathfrak{M}_p$ er et maksimalideal, er kvotienten,

$$\boldsymbol{\kappa}(p) := k[X_1, \ldots, X_n]/\mathfrak{M}_p,$$

et legeme. Dette legeme kaldes *restklasselegemet* for punktet p. Restklasselegemet er en k-algebra, og specielt et vektorrum over k. Vektorrumsdimensionen af $\boldsymbol{\kappa}(p)$ kaldes også *graden af punktet* p, og betegnes $|p : k|$, altså

$$|p : k| := \dim_k \boldsymbol{\kappa}(p).$$

De rationale punkter er karakteriseret ved at homomorfien $k \to \boldsymbol{\kappa}(p)$ er en isomorfi eller, ækvivalent, at graden er lig med 1. Hvis legemet k er algebraisk afsluttet, har alle punkter grad 1.

(4.2) Definition. Ved et *skema* X i $\mathbf{A}^n$ forstås i det følgende en kvotient af polynomiumsringen $k[X_1, \ldots, X_n]$.

Igen vil vi på trods af ordlyden aldrig opfatte et skema som værende en kvotientring af $k[X_1, \ldots, X_n]$. Definitionen skal opfattes således at den fastlægger en bijektiv forbindelse mellem på den ene side skemaer i $\mathbf{A}^n$ og på den anden side kvotienter af $k[X_1, \ldots, X_n]$. Den kvotient af $k[X_1, \ldots, X_n]$, der herved svarer til et givet skema X, kaldes skemaets *koordinatring*, og den betegnes $\Gamma(X)$. En kvotient kan naturligvis lige så vel bestemmes ved et ideal i polynomiumsringen: der er en bijektiv forbindelse mellem idealer og kvotienter. Idealet, der svarer til et givet skema X, betegnes $\mathcal{I}(X)$. Omvendt bestemmer hvert ideal $\mathfrak{I}$ et skema, svarende til kvotienten $k[X_1, \ldots, X_n]/\mathfrak{I}$. Hvis idealet er frembragt af polynomier F_α siges skemaet også at være defineret ved polynomierne F_α, eller ved ligningerne $F_\alpha = 0$. Bemærk, at ligningen,

$$k[X_1, \ldots, X_n]/\mathcal{I}(X) = \Gamma(X),$$

blot udtrykker, at kvotienter er noget der defineres ved hjælp af idealer.

Skemaet bestemt ved idealet (0) betegnes $\mathbf{A}^n$, og skemaet, hvis koordinatring er nul-ringen, betegnes $\emptyset$ og kaldes det *tomme* skema. Koordinatringen $\Gamma(\mathbf{A}^n)$ er altså ringen $k[X_1, \ldots, X_n]$, og koordinatringen $\Gamma(\emptyset)$ er altså nul-ringen.

(4.3) Definition. Lad X være et skema i $\mathbf{A}^n$. Et punkt p i $\mathbf{A}^n$ siges at *ligge på skemaet*, eller at *tilhøre skemaet*, hvis $\mathcal{I}(X) \subseteq \mathfrak{M}_p$. At dette er tilfældet udtrykkes også ved skrivemåden,

$$p \in X.$$

Hvis X er skemaet defineret ved et ideal $\mathfrak{I}$ i $k[X_1, \ldots, X_n]$, så følger det, at de rationale punkter på X netop er elementerne i delmængden $\mathcal{V}(\mathfrak{I})$. Udover disse rationale punkter vil et skema sædvanligvis indeholde andre punkter. Men det skal understreges, at et skema ikke må opfattes som værende „mængden af sine punkter".

Ifølge definitionen svarer punkterne p på X til de maksimalidealer $\mathfrak{M}_p$, der indeholder $\mathcal{I}(X)$. Det følger derfor af Kvotientprincippet, at punkterne på X svarer bijektivt til samtlige maksimalidealer i kvotienten $\Gamma(X) = k[X_1, \ldots, X_n]/\mathcal{I}(X)$; idet $\mathfrak{M}_{X,p}$ betegner det til $\mathfrak{M}_p$ svarende maksimalideal i $\Gamma(X)$, følger det yderligere, at kvotienten $\Gamma(X)/\mathfrak{M}_{X,p}$ er isomorf med restklasselegemet $\boldsymbol{\kappa}(p)$.

(4.4) Notation. Lad X være et skema i $\mathbf{A}^n$, og lad p være et punkt på X. Den *lokale ring*, der fremkommer ved lokalisering af $\Gamma(X)$ i maksimalidealet $\mathfrak{M}_{X,p}$, betegnes $\mathcal{O}_{X,p}$ og maksimalidealet i $\mathcal{O}_{X,p}$ betegnes $\mathfrak{m}_{X,p}$. Det følger af Lokaliseringsprincippet, at restklasselegemet for den lokale ring, dvs kvotienten $\mathcal{O}_{X,p}/\mathfrak{m}_{X,p}$, er isomorf med restklasselegemet $\boldsymbol{\kappa}(p)$.

(4.5) Hilbert's Nulpunktssætning. (1) *For hvert punkt p i $\mathbf{A}^n$ er restklasselegemet $\boldsymbol{\kappa}(p)$ af endelig dimension over k. Graden $|p{:}k|$ er altså endelig.*

(2) *På ethvert ikke-tomt skema X findes et punkt.*

(3) *Lad X være skemaet bestemt ved et ideal $\mathfrak{I}$ i $k[X_1, \ldots, X_n]$. Da gælder formlen,*

$$\mathrm{Rad}(\mathfrak{I}) = \bigcap_{p \in X} \mathfrak{M}_p.$$

Bevis. (1) Ifølge definitionen svarer et punkt i $\mathbf{A}^n$ til et maksimalideal $\mathfrak{M}$ i ringen $k[X_1, \ldots, X_n]$ og restklasselegemet er kvotienten $k[X_1, \ldots, X_n]/\mathfrak{M}$. Denne kvotient er et legeme og en endeligt frembragt algebra over k. Af Hilbert's Nulpunktssætning, version 1, fremgår derfor at kvotienten er endeligdimensional over k.

(2) For et ikke-tomt skema X er koordinatringen $\Gamma(X)$ ikke nul-ringen. Følgelig findes maksimalidealer i $\Gamma(X)$. Disse maksimalidealer svarer til punkter på X.

(3) Beviset er næsten identisk med beviset for Hilbert's Nulpunktssætning, version 2. Formlens højreside er fællesmængden af de maksimalidealer $\mathfrak{M}$, som omfatter $\mathfrak{I}$. Det er derfor klart, at venstresiden er indeholdt i højresiden.

For at vise den omvendte inklusion betragtes et polynomium F, som ikke tilhører venstresiden. Det antages altså at $F^n \notin \mathfrak{I}$ for alle n. Idet f betegner restklassen af F i $R := \Gamma(X)$ følger det, at $f^n \neq 0$ for alle n. Brøkringen R_f er derfor ikke nulringen. Følgelig findes et maksimalideal $\mathfrak{m}$ i brøkringen R_f. Lad $\mathfrak{M}$ betegne kontraktionen af $\mathfrak{m}$ til $k[X_1, \ldots, X_n]$. Da er $\mathfrak{M}$ et primideal, $F \notin \mathfrak{M}$, og $\mathfrak{M} \supseteq \mathfrak{I}$. Det er nok at vise,

at $\mathfrak{M}$ er et maksimalideal, thi så er $\mathfrak{M}$ blandt maksimalidealerne på højresiden, og da $F \notin \mathfrak{M}$ er F således ikke element i højresiden.

Det skal vises, at $\mathfrak{M}$ er et maksimalideal i $k[X_1, \ldots, X_n]$, altså at kvotienten $\boldsymbol{\kappa} := k[X_1, \ldots, X_n]/\mathfrak{M}$ er et legeme. Det følger af Hilbert's Nulpunktssætning, version 1, at kvotienten $R_f/\mathfrak{m}$ er endeligdimensional over k. Da denne kvotient indeholder kvotienten $\boldsymbol{\kappa}$, er også $\boldsymbol{\kappa}$ endeligdimensional over k. Altså er $\boldsymbol{\kappa}$ hel over legemet k og et integritetsområde. Heraf følger som bekendt, at $\boldsymbol{\kappa}$ er et legeme, som påstået.

Hermed er de tre påstande i Nulpunktssætningen bevist. ∎

(4.6) Definition. Lad Z og X være skemaer i $\mathbf{A}^n$. Hvis $\mathcal{I}(Z) \supseteq \mathcal{I}(X)$, siges Z også at være et skema *i* X eller et *delskema* i X. Betingelsen udtrykkes ved skrivemåden,

$$Z \subseteq X.$$

Bemærk, at relationen, der udtrykkes ved inklusionen ovenfor, ikke er ensbetydende med en inklusion mellem punkterne. Af definitionerne følger umiddelbart, at hvis $Z \subseteq X$, så er hvert punkt på Z også et punkt på X. Men det omvendte kan ikke sluttes. Mere præcist følger det af Nulpunktssætningen, at hvert punkt på Z også er et punkt på X, hvis og kun hvis radikalet af $\mathcal{I}(Z)$ omfatter radikalet af $\mathcal{I}(X)$.

Ifølge definitionen svarer delskemaer i X til de idealer i $k[X_1, \ldots, X_n]$, som omfatter $\mathcal{I}(X)$. Det følger derfor af kvotientprincippet, at delskemaer Z i X svarer bijektivt til idealerne i koordinatringen $\Gamma(X)$.

Lad X og Z være skemaer i $\mathbf{A}^n$. Ved fællesmængden, eller *snitskemaet*, forstås da skemaet $Z \cap X$ defineret ved idealet $\mathcal{I}(Z) + \mathcal{I}(X)$. Tilsvarende defineres foreningsmængden $Z \cup X$ ved idealet $\mathcal{I}(Z) \cap \mathcal{I}(X)$.

Et (maksimal)ideal $\mathfrak{M}$ omfatter $\mathfrak{I} + \mathfrak{J}$, hvis og kun hvis $\mathfrak{M}$ omfatter både $\mathfrak{I}$ og $\mathfrak{J}$. Med andre ord, et punkt p i $\mathbf{A}^n$ ligger på snittet $Z \cap X$, hvis og kun hvis det ligger på begge skemaer Z og X.

Det er velkendt, at et maksimalideal $\mathfrak{M}$ omfatter $\mathfrak{I} \cap \mathfrak{J}$, hvis og kun hvis $\mathfrak{M}$ omfatter et af idealerne $\mathfrak{I}$ eller $\mathfrak{J}$. Der gælder altså tilsvarende, at et punkt p ligger på foreningen $Z \cup X$, hvis og kun hvis det ligger på et af skemaerne Z og X.

(4.7) Definition. Et skema X kaldes et *integritetsskema*, hvis koordinatringen $\Gamma(X)$ er et integritetsområde.

Koordinatringen $\Gamma(X)$ er et integritetsområde, hvis og kun hvis det tilhørende ideal $\mathcal{I}(X)$ er et primideal. Integritetsskemaer i $\mathbf{A}^n$ svarer altså bijektivt til primidealer i $k[X_1, \ldots, X_n]$. Mere generelt ses, at integritetsskemaer i et givet skema X svarer bijektivt til primidealer i koordinatringen $\Gamma(X)$.

Det følger af Nulpunktssætningen, at et integritetsskema er „bestemt ved sine punkter“. Hvis X er et integritetsskema, er idealet $\mathcal{I}(X)$ et primideal og dermed lig med sit eget radikal. Følgelig er $\mathcal{I}(X)$ lig med fællesmængden af maksimalidealerne $\mathfrak{M}_p$ for $p \in X$.

(4.8) Definition. Lad X være et skema i $\mathbf{A}^n$ og lad Y være et skema i $\mathbf{A}^m$. Ved en *morfi af skemaer* $\varphi\colon Y \to X$ forstås en homomorfi af k-algebraer $\theta\colon \Gamma(X) \to \Gamma(Y)$.

Lad q være et punkt i Y svarende til maksimalidealet $\mathfrak{M}_{Y,q}$ i $\Gamma(Y)$. Kontraktionen til $\Gamma(X)$, dvs originalmængden $\mathfrak{M} := \theta^{-1}(\mathfrak{M}_{Y,q})$, er da et maksimalideal i $\Gamma(X)$. Kontraktionen er nemlig kernen for den sammensatte homomorfi,

$$\Gamma(X) \to \Gamma(Y) \to \Gamma(Y)/\mathfrak{M}_{Y,q} = \boldsymbol{\kappa}(q),$$

så kvotienten $\Gamma(X)/\mathfrak{M}$ er isomorf med billedet ved denne homomorfi. Billedet er en delalgebra af $\boldsymbol{\kappa}(q)$. Da $\boldsymbol{\kappa}(q)$ er endeligdimensional over k ifølge Nulpunktssætningen, er også billedet endeligdimensionalt over k. Da billedet også er et integritetsområde, sluttes at billedet er et legeme. Følgelig er $\mathfrak{M}$ et maksimalideal i $\Gamma(X)$. Punktet i X, svarende til kontraktionen $\mathfrak{M} = \theta^{-1}(\mathfrak{M}_{Y,q})$, kaldes *billedpunktet* ved morfien φ, og det betegnes φq.

Det fremgår af konstruktionen, at restklasselegemet $\boldsymbol{\kappa}(\varphi q)$ for billedpunktet er et dellegeme af $\boldsymbol{\kappa}(q)$. Specielt er graden af billedpunktet φq en divisor i graden af q. Mere præcist: Som vektorrum over $\boldsymbol{\kappa}(\varphi q)$ er legemet $\boldsymbol{\kappa}(q)$ af endelig dimension, betegnet $|q : \varphi q|$, og for graderne gælder formlen,

$$|q : k| = |q : \varphi q| \cdot |\varphi q : k|.$$

(4.9) Definition. Lad X og Y være skemaer med koordinatringene $A := \Gamma(X)$ og $B := \Gamma(Y)$. Lad videre $\varphi\colon Y \to X$ være en morfi af skemaer, svarende til homomorfien af k-algebraer $\theta\colon A \to B$. Lad endelig $Z \subseteq X$ og $W \subseteq Y$ være delskemaer svarende til idealerne $\mathfrak{I}$ i A og $\mathfrak{J}$ i B. Ved *billedskemaet* φW forstås skemaet i X svarende til kontraktionen $A \cap \mathfrak{J}$ i A, og ved *originalskemaet* $\varphi^{-1}Z$ forstås skemaet i Y svarende til extensionen $\mathfrak{I}B$ i B.

Morfien $\varphi\colon Y \to X$ siges at være en *dominerende morfi*, hvis billedskemaet φY er lig med skemaet X.

Et punkt p i X svarer til et maksimalideal $\mathfrak{M}_{X,p}$ i A, og det kan derfor opfattes som et delskema af X. Originalskemaet $\varphi^{-1}p$ er skemaet defineret ved ekstensionen $\mathfrak{M}_{X,p}B$. Det kaldes også *fiberen* i punktet p for morfien φ.

(4.10) Observation. Det er let at se, at et punkt q i Y tilhører originalskemaet $\varphi^{-1}Z$, hvis og kun hvis billedpunktet φq tilhører Z. Specielt er punkterne på fiberen $\varphi^{-1}p$ netop de punkter q i Y for hvilke $\varphi q = p$. Videre er det klart, at hvis q tilhører W, så vil billedpunktet φq tilhøre billedskemaet φW; men i almindelighed vil billedskemaet φW også indeholde punkter, der ikke er billedpunkter.

Skemaet Y, som delskema i Y, svarer til idealet (0) i $\Gamma(Y)$. Billedskemaet φY er derfor delskemaet i X, hvis ideal er kontraktionen til $\Gamma(X)$ af (0). Denne kontraktion er blot kernen for homomorfien $\Gamma(X) \to \Gamma(Y)$. Morfien $Y \to X$ er således dominerende, hvis og kun hvis homomorfien $\Gamma(X) \to \Gamma(Y)$ er injektiv.

Bemærk, at for et integritetsskema W i Y er billedskemaet φW et integritetsskema i X. Dette følger af at kontraktion af et primideal er et primideal.

(4.11) Note. Det skal understreges, at definitionerne i dette afsnit i sig selv er ret indholdsløse. De fastlægger blot at der anvendes en geometrisk sprogbrug ved beskrivelsen af visse fænomener knyttet til polynomiumsringen $k[X_1, \ldots, X_n]$.

5. Endelige skemaer og endelige morfier. Dimension.

(5.1) Sætning. *For et skema X er følgende betingelser ækvivalente:*

(i) *Skemaet X indeholder kun endelig mange punkter.*
(ii) *Alle primidealer i $\Gamma(X)$ er maksimalidealer.*
(iii) *Ringen $\Gamma(X)$ har endelig længde.*
(iv) *Algebraen $\Gamma(X)$ er af endelig dimension som vektorrum over k.*

Er disse betingelser opfyldt, og er $p_1, \ldots, p_r$ de endelig mange punkter på X, så findes en naturlig isomorfi,

$$\Gamma(X) \xrightarrow{\sim} \mathcal{O}_{X,p_1} \times \cdots \times \mathcal{O}_{X,p_r}. \tag{5.1.1}$$

Bevis. Antag, at X er defineret ved idealet $\mathfrak{I}$ i $k[X_1, \ldots, X_n]$. Da gælder ifølge Hilbert's Nulpunktssætning, at $\operatorname{Rad}\mathfrak{I}$ er fællesmængden af maksimalidealerne $\mathfrak{M}_p$ for $p \in X$. I kvotientringen $\Gamma(X)$ gælder derfor, at $\operatorname{Rad}(0)$ er fællesmængden af maksimalidealerne $\mathfrak{M}_{X,p}$ for $p \in X$.

Antag, at betingelsen (i) er opfyldt. Da er fællesmængden ovenfor en endelig fællesmængde. Lad $\mathfrak{p}$ være et primideal i $\Gamma(X)$. Da vil $\mathfrak{p}$ indeholde radikalet $\operatorname{Rad}(0)$, og dermed den endelige fællesmængde af maksimalidealerne $\mathfrak{M}_{X,p}$. Heraf følger som bekendt, at $\mathfrak{p}$ indeholder et af idealerne $\mathfrak{M}_{X,p}$. Af $\mathfrak{p} \supseteq \mathfrak{M}_{X,p}$ følger videre, at $\mathfrak{p} = \mathfrak{M}_{X,p}$. Følgelig er $\mathfrak{M}_{X,p}$'erne samtlige primidealer i $\Gamma(X)$. Altså gælder betingelsen (ii).

Det er et korollar til Filtrationssætningen, at betingelserne (ii) og (iii) er ækvivalente, og yderligere, at betingelserne medfører, at $\Gamma(X)$ kun har endelig mange maksimalidealer. Da disse maksimalidealer svarer bijektivt til punkterne på X, følger det at betingelserne (ii) eller (iii) medfører (i).

Betingelsen (iv) medfører (iii), idet der trivielt gælder $\operatorname{long}\Gamma(X) \leq \dim_k \Gamma(X)$. Antag omvendt, at (iii) er opfyldt, altså at ringen $\Gamma(X)$ har endelig længde. Da har $\Gamma(X)$ en filtration hvor de successive kvotienter er simple, altså af formen $\Gamma(X)/\mathfrak{M}_i$, hvor $\mathfrak{M}_i$'erne er maksimalidealer i $\Gamma(X)$. Maksimalidealerne har formen $\mathfrak{M}_i = \mathfrak{M}_{X,p_i}$, hvor p_i er et punkt på X, og kvotienterne er altså restklasselegemerne $\boldsymbol{\kappa}(p_i)$. Kvotienterne er derfor af endelig dimension over k ifølge Hilbert's Nulpunktssætning. Følgelig er også $\Gamma(X)$ af endelig dimension over k. Altså gælder (iv).

Hermed er ækvivalensen bevist. Den anførte isomorfi er et velkendt korollar til Filtrationssætningen. ∎

(5.2) Definition. Et skema X, der opfylder de ækvivalente betingelser i Sætning (5.1), kaldes et *endeligt skema*.

Lad X være et endeligt skema og lad p være et punkt på X. Den lokale ring $\mathcal{O}_{X,p}$ har da endelig længde. Dette følger af Filtrationssætningen, og det er også en konsekvens af isomorfien i (5.1.1), idet det fremgår, at $\mathcal{O}_{X,p}$ er af endelig dimension over k. Længden af den lokale ring $\mathcal{O}_{X,p}$ kaldes *multipliciteten af punktet p* på skemaet X, og den betegnes $\operatorname{mult}_p(X)$.

(5.3) Korollar. *Lad X være et endeligt skema. Da gælder formlen*

$$\dim_k \Gamma(X) = \sum_{p \in X} |p:k| \cdot \mathrm{mult}_p(X). \tag{5.3.1}$$

Bevis. Venstresiden i formlen er dimensionen af venstresiden i isomorfien (5.1.1). Dimensionen af højresiden af denne isomorfi er øjensynlig summen af dimensionerne af $\mathcal{O}_{X,p}$ for $p \in X$. Det er derfor nok at vise for $p \in X$, at

$$\dim_k \mathcal{O}_{X,p} = |p:k| \cdot \mathrm{mult}_p(X). \tag{5.3.2}$$

Multipliciteten $m := \mathrm{mult}_p(X)$ er længden af ringen $\mathcal{O} := \mathcal{O}_{X,p}$. Denne ring er lokal med maksimalidealet $\mathfrak{m} := \mathfrak{m}_{X,p}$, og den har altså en filtration med m kvotienter, der alle er isomorfe med kvotienten $\mathcal{O}/\mathfrak{m}$. Den sidste kvotient er restklasselegemet $\boldsymbol{\kappa}(p)$. Dimensionen af $\mathcal{O}$ er derfor m gange dimensionen af $\boldsymbol{\kappa}(p)$. Den sidste dimension er lig med graden $|p:k|$. Følgelig gælder formlen (5.3.2). Hermed er det ønskede bevist. ∎

(5.4) Note. Formlen udsiger for et endeligt skema X, at vektorrumsdimensionen $\dim_k \Gamma(X)$ er lig med antallet af punkter på X, „talt med multiplicitet“. Denne multiplicitet omfatter dels punktets multiplicitet $\mathrm{mult}_p(X)$, dels graden $|p:k|$. Hvis k er algebraisk afsluttet (eller mere generelt, hvis alle skemaets punkter er rationale punkter), så er alle disse grader lig med 1.

(5.5) Definition. En morfi af skemaer $\varphi\colon Y \to X$, svarende til homomorfien af k-algebraer $\theta\colon \Gamma(X) \to \Gamma(Y)$, siges at være en *endelig morfi*, hvis $\Gamma(Y)$ er endeligt frembragt som modul over $\Gamma(X)$.

(5.6) Eksempel. Lad X være et ikke-tomt skema. Da findes en endelig, dominerende morfi $\varphi\colon X \to \mathbf{A}^d$, thi ifølge Noether's Normaliseringslemma er $\Gamma(X)$ endeligt frembragt som modul over en delalgebra $k[y_1, \ldots, y_d]$ frembragt af et sæt af d algebraisk uafhængige elementer $y_1, \ldots, y_d$. Delalgebraen er altså isomorf med polynomiumsringen $k[Y_1, \ldots, Y_d]$, og inklusionen af delalgebraen svarer til en injektiv homomorfi $k[Y_1, \ldots, Y_d] \to \Gamma(X)$. „Oversat“ til skemaer er dette den søgte morfi.

(5.7) Sætning. *Lad $\varphi\colon Y \to X$ være en endelig morfi af skemaer. For hvert punkt p i X er fiberen $\varphi^{-1}p$ da et endeligt skema. Antag yderligere, at φ er dominerende. Da gælder:*

(1) *Ethvert punkt p i X er billede af et punkt i Y.*
(2) *Ethvert integritetsskema Z i X er billede af et integritetsskema W i Y.*
(3) *Hvis W og W' er integritetsskemaer i Y således at $W \subset W'$, da er $\varphi W \subset \varphi W'$.*

Bevis. Sæt $A := \Gamma(X)$ og $B := \Gamma(Y)$. Ifølge forudsætningen svarer morfien φ da til en homomorfi $A \to B$, således at B er endeligt frembragt som A-modul. Lad $\mathfrak{m} := \mathfrak{M}_{X,p}$ være maksimalidealet i A svarende til et punkt p på X. Fiberen $\varphi^{-1}p$ er

da, som delskema af Y, bestemt ved idealet $\mathfrak{m}B$ i B, og koordinatringen $\Gamma(\varphi^{-1}p)$ er kvotienten $B/\mathfrak{m}B$. Det skal vises, jfr betingelse (iv) i Sætning (5.1), at $B/\mathfrak{m}B$ er af endelig dimension over k. Hertil bemærkes, at B er endeligt frembragt som A-modul, og følgelig er $B/\mathfrak{m}B$ endeligt frembragt som modul over $\boldsymbol{\kappa}(p) = A/\mathfrak{m}$. Yderligere er restklasselegemet $\boldsymbol{\kappa}(p)$ af endelig dimensions over k. Heraf følger det ønskede.

Antag nu yderligere, at φ er dominerende, altså at homomorfien $A \to B$ er injektiv. For at vise (1), skal det vises, at fiberen $\varphi^{-1}(p)$ ikke er det tomme skema, altså at extensionen $\mathfrak{m}B$ er forskellig fra B. Da homomorfien $A \to B$ er injektiv, fås ved lokalisering i $\mathfrak{m}$ en injektiv homomorfi $A_\mathfrak{m} \to B_\mathfrak{m}$. Da den lokale ring $A_\mathfrak{m}$ ikke er nulringen følger det, at $B_\mathfrak{m}$ er forskellig fra 0. Videre er B endeligt frembragt som modul over A, og $B_\mathfrak{m}$ er derfor endeligt frembragt som modul over $A_\mathfrak{m}$. Af Nakayama's Lemma følger derfor, at kvotienten $B_\mathfrak{m}/\mathfrak{m}B_\mathfrak{m}$ er forskellig fra 0. Ifølge Lokaliseringsprincippet er denne kvotient isomorf med den modul der fremkommer ved lokalisering i $\mathfrak{m}$ af kvotienten $B/\mathfrak{m}B$. Denne sidste kvotient er derfor forskellig fra 0. Følgelig er idealet $\mathfrak{m}B$ et ægte ideal i B, som ønsket.

(2) Et irreducibelt delskema Z af X svarer til et primideal $\mathfrak{p}$ i A. Det skal vises at der findes et primideal $\mathfrak{q}$ i B, således at $A \cap \mathfrak{q} = \mathfrak{p}$.

Ved lokalisering fås inklusionen $A_\mathfrak{p} \to B_\mathfrak{p}$. Ganske som i beviset for (1) følger det, at maksimalidealet $\mathfrak{p}A_\mathfrak{p}$ i den lokale ring $A_\mathfrak{p}$ er kontraktion af et primideal i $B_\mathfrak{p}$. Dette sidste primideal kontraheres til et primideal $\mathfrak{q}$ i B, hvis kontraktion til A er lig med $\mathfrak{p}$, som ønsket.

(3) De givne integritetsskemaer $W \subset W'$ i Y svarer til primidealer $\mathfrak{q} \supset \mathfrak{q}'$ i B. Det skal vises for kontraktionerne, at $A \cap \mathfrak{q} \supset A \cap \mathfrak{q}'$.

Betragt kontraktionen $\mathfrak{p} := A \cap \mathfrak{q}'$. Da er $\mathfrak{p}$ kernen for den sammensatte homomorfi $A \to B \to B/\mathfrak{q}'$, og $A/\mathfrak{p}$ er derfor (isomorf med) en delring af $B/\mathfrak{q}'$. Primidealet $\mathfrak{q}$ svarer til et primideal forskelligt fra (0) i kvotienten $B/\mathfrak{q}'$. Ved at erstatte B med kvotienten $B/\mathfrak{q}'$ og A med $A/\mathfrak{p}$ kan det derfor antages, at A og B er integritetsområder og at $\mathfrak{q} \neq (0)$. Det skal så vises, at $A \cap \mathfrak{q}$ er forskellig fra (0).

Vælg hertil et element $b \neq 0$ i $\mathfrak{q}$. Ifølge antagelsen er B endeligt frembragt som A-modul. Specielt er B hel over A. Der findes derfor en helhedsrelation for b over A. Denne relation kan skrives på formen,

$$b(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) = -a_n,$$

hvor a_i'erne tilhører A. Vælg nu denne relation så at n er mindst mulig. Da er $a_n \neq 0$. I modsat fald var nemlig produktet på venstresiden lig med 0; da faktorerne tilhører integritetsområdet B og $b \neq 0$ ville den anden faktor så være lig med 0, og dette ville være en helhedsrelation af grad $n-1$, i modstrid med valget af n. Elementet a_n i A er altså forskelligt fra 0. Af relationen fremgår, at a_n tilhører idealet i B frembragt af b. Da $b \in \mathfrak{q}$, er altså $a_n \in \mathfrak{q}$. Følgelig er a_n et element forskelligt fra 0 i $A \cap \mathfrak{q}$. Altså er $A \cap \mathfrak{q} \neq (0)$, som ønsket.

Hermed er sætningens tre påstande bevist. ∎

(5.8) Definition. Lad X være et skema. Ved *dimensionen* af X forstås da det største antal skarpe inklusionener, der kan være i en kæde,

$$Z_d \subset \cdots \subset Z_1 \subset Z_0 \subseteq X, \tag{5.8.1}$$

af integritetsskemaer Z_i i X. Dimensionen af X betegnes $\dim X$.

Det tomme skema tillægges sædvanligvis dimensionen -1.

(5.9) Observation. For et givet skema X svarer integritetsskemaer Z i X bijektivt til primidealer $\mathfrak{p}$ i $\Gamma(X)$, og kæder (5.8.1) af integritetsskemaer i X svarer til kæder,

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_d, \tag{5.9.1}$$

af primidealer i $\Gamma(X)$. Dimensionen er et supremum over sådanne d'er. At dimensionen er mindre end 1 betyder således, at der ikke i $\Gamma(X)$ findes primidealer $\mathfrak{p} \subset \mathfrak{p}'$, eller ækvivalent, at alle primidealer i $\Gamma(X)$ er maksimalidealer. Af betingelsen (5.1)(ii) følger derfor, at skemaerne af dimension 0 netop er de ikke-tomme, endelige skemaer.

For at bestemme dimensionen af X er det nok at betragte kæder (5.9.1) af primidealer i $\Gamma(X)$ hvor $\mathfrak{p}_0$ er et minimalt primideal og $\mathfrak{p}_d$ er et maksimalideal. Da $\Gamma(X)$ er noethersk, er der som bekendt kun endelig mange minimale primidealer i $\Gamma(X)$. Disse primidealer svarer til integritetsskemaer i X, der er maksimale. Disse endelig mange maksimale integritetsskemaer i X kaldes også *komponenterne af skemaet* X.

(5.10) Sætning. (1) *Skemaet* $\mathbf{A}^n$ *har dimension* n.

(2) *Lad* $\varphi\colon Y \to X$ *være en endelig, dominerende morfi. Da er* $\dim Y = \dim X$.

(3) *Lad* X *være et integritetsskema. Da er* $\dim X = \operatorname{tdeg}_k \Gamma(X)$.

Bevis. (1) Det skal vises for polynomiumsringen $k[X_1, \ldots, X_n]$, at for enhver kæde af primidealer (5.9.1) er $d \leq n$, og at der eksisterer en kæde med $d = n$. Eksistensen indses ved at betragte kæden defineret ved $\mathfrak{p}_i = (X_1, \ldots, X_i)$.

Uligheden vises således: Kvotienten $A_i := k[X_1, \ldots, X_n]/\mathfrak{p}_{i-1}$ er en endeligt frembragt k-algebra og et integritetsområde, og har derfor en endelig transcendensgrad over k. I kvotienten A_i svarer $\mathfrak{p}_i$ til et primideal forskelligt fra (0). Det er velkendt, at transcendensgraden går ned, når der divideres med et primideal forskelligt fra (0). Polynomiumsringen $k[X_1, \ldots, X_n]$ har transcendensgrad n, og transcendensgraden kan derfor højst gå ned n gange. Følgelig indeholder kæden (5.9.1) højst n skarpe inklusioner.

(2) De to uligheder $\dim Y \geq \dim X$ og $\dim X \geq \dim Y$ følger af resultaterne (2) og (3) i Lemma (5.7).

Betragt nemlig først en vilkårlig kæde (5.8.1) i X. Af (5.7)(2) følger, at der findes et integritetsskema W_0 i Y således at $\varphi W_0 = Z_0$. Øjensynlig definerer φ en endelig, dominerende morfi $W_0 \to Z_0$. Anvendt på denne morfi, og integritetsskemaet Z_1 i Z_0, følger det tilsvarende, at der findes et integritetsskema W_1 i W_0 således at $\varphi W_1 = Z_1$. Efter d gentagelser af argumentet ses, at der findes en kæde af integritetsskemaer W_i

i Y med d skarpe inklusioner. Følgelig er $\dim Y \geq d$. Da (5.8.1) var en vilkårlig kæde, sluttes at $\dim Y \geq \dim X$.

Betragt omvendt en kæde af integritetsskemaer W_i i Y med e skarpe inklusionener. Af (5.7)(3) sluttes, at billedskemaerne φW_i er en kæde af integritetsskemaer i X med e skarpe inklusioner. Heraf sluttes, at $\dim X \geq \dim Y$.

(3) Ifølge Noether's Normaliseringslemma findes i $\Gamma(X)$ et sæt af d algebraisk uafhængige elementer $y_1, \ldots, y_d$ således at $\Gamma(X)$ er endeligt frembragt som modul over delalgebraen $k[y_1, \ldots, y_d]$. Antallet d er som bekendt transcendensgraden $\operatorname{tdeg}_k \Gamma(X)$. Inklusionen af $k[y_1, \ldots, y_d]$ i $\Gamma(X)$ svarer til en endelig, dominerende morfi $X \to \mathbf{A}^d$. Af de foregående resultater (1) og (2) følger derfor, at $\dim X = d$, som ønsket.

Hermed er de tre påstande bevist. ∎

(5.11) Note. Lad $\varphi\colon Y \to X$ være en endelig morfi, og lad p være et punkt i X. Fiberen $\varphi^{-1}p$ er da delskemaet af Y defineret ved idealet $\mathfrak{M}_{X,p}\Gamma(Y)$, og koordinatringen for fiberen er altså kvotienten $\Gamma(\varphi^{-1}p) = \Gamma(Y)/\mathfrak{M}_{X,p}\Gamma(Y)$. Da $\Gamma(Y)$ er endeligt frembragt som modul over $\Gamma(X)$, er kvotienten $\Gamma(\varphi^{-1}p)$ endeligt frembragt som modul over kvotienten $\Gamma(X)/\mathfrak{M}_{X,p}$. Den sidste kvotient er legemet $\boldsymbol{\kappa}(p)$, så $\Gamma(\varphi^{-1}p)$ er et vektorrum af endelig dimension over $\boldsymbol{\kappa}(p)$. Denne dimension kaldes *graden af morfien* φ i punktet p, og den betegnes $\deg_p \varphi$. Vektorrummet $\Gamma(\varphi^{-1}p)$ er af endelig dimension over $\boldsymbol{\kappa}(p)$, og dermed også af endelig dimension over k; mere præcist gælder, at

$$\dim_k \Gamma(\varphi^{-1}p) = |p:k| \cdot \deg_p \varphi. \tag{5.11.1}$$

Specielt er fibrene for φ altså endelige skemaer. For hvert punkt q i fiberen $\varphi^{-1}p$ gælder $|q:k| = |q:p| \cdot |p:k|$, jfr Definition (4.8). Af formel (5.11.1) og Korollar (5.3) fås derfor formlen,

$$\deg_p \varphi = \sum_{q \mapsto p} |q:p| \cdot \operatorname{mult}_q(\varphi^{-1}p),$$

hvor summationen er over alle punkter q i fiberen $\varphi^{-1}p$. Graden af φ i p angiver altså, „talt med multiplicitet", antallet af punkter i fiberen $\varphi^{-1}p$.

(5.12) Note. For en endelig morfi $\varphi\colon Y \to X$ kan graden i et punkt $p \in X$ yderligere fortolkes på følgende måde.

Sæt $A := \Gamma(X)$ og $B := \Gamma(Y)$. Morfien svarer da til en homomorfi $A \to B$, således at B er endeligt frembragt som A-modul. Lad p være et punkt i X, sæt $\mathfrak{M} := \mathfrak{M}_{X,p}$. Koordinatringen for fiberen $\varphi^{-1}p$ er da kvotienten $B/\mathfrak{M}B$. Graden af φ i p er dimensionen af kvotienten som vektorrum over $\boldsymbol{\kappa}(p) = A/\mathfrak{M}$. Hvis B er frembragt som A-modul af e elementer, så er kvotienten frembragt som $\boldsymbol{\kappa}(p)$-modul billederne af disse e elementer; følgelig er graden $\deg_p \varphi$ mindre end eller lig med e. Specielt ses, at graden i (det vilkårlige punkt) p er begrænset opad af det mindste antal elementer, der frembringer B som A-modul.

Dette resultat kan forstærkes. Ved lokalisering af A i maksimalidealet $\mathfrak{M}$ fås nemlig den lokale ring $\mathcal{O} := \mathcal{O}_{X,p}$. Det følger af Lokaliseringsprincippet at kvotienten $B/\mathfrak{M}B$

er isomorf med kvotienten af $B_{\mathfrak{M}}$ modulo idealet $\mathfrak{M}B_{\mathfrak{M}}$. Her er $B_{\mathfrak{M}}$ en endeligt frembragt modul over den lokale ring $\mathcal{O}$. Graden af φ, dvs dimensionen af kvotienten som vektorrum over $\boldsymbol{\kappa}(p)$, er derfor ifølge Nakayama's Lemma lig med det minimale antal elementer, som frembringer $\mathcal{O}$-modulen $B_{\mathfrak{M}}$.

Et sæt af e elementer, der frembringer $B_{\mathfrak{M}}$ som $\mathcal{O}$-modul, svarer til en surjektiv $\mathcal{O}$-lineær afbildning $\mathcal{O}^e \to B_{\mathfrak{M}}$. Det kan antages, at de e elementer er brøker med nævner 1, således at sættet svarer til en A-lineær afbildning $A^e \to B$. At sættet frembringer $B_{\mathfrak{M}}$ betyder at homomorfien $A^e \to B$ efter lokalisering i $\mathfrak{M}$ bliver surjektiv.

Betragt nu en vilkårlig A-lineær afbildning $A^e \to B$, og lad Q betegne kokernen. Af Isomorfisætningen for Brøkmoduler følger da, at homomorfien bliver surjektiv efter lokalisering i $\mathfrak{M}$, hvis og kun hvis $Q_{\mathfrak{M}} = 0$, altså hvis og kun hvis $\mathfrak{M}$ ikke tilhører støtten for A-modulen Q. Primidealerne i støtten for Q er som bekendt netop primidealerne, der omfatter annullatoren for Q. Annullatoren er et ideal i A, og svarer altså til et skema Z i X. Homomorfien $A^e \to B$ er altså surjektiv efter lokalisering i $\mathfrak{M}$, hvis og kun hvis p ikke tilhører skemaet Z.

Af disse overvejelser følger: *Lad e være graden af φ i et givet punkt p i X. Da findes et delskema Z i X således at $p \notin Z$ og således at graden af φ er mindre end eller lig med e for alle punkter i komplementærmængden $X \backslash Z$.*

(5.13) Note. Det foregående resultat er specielt simpelt, når X er et integritetsskema af dimension 1. Hertil bemærkes, at under denne forudsætning er ethvert skema Z i X, således at $Z \subset X$, nødvendigvis et endeligt skema, idet dimension af Z må være strengt mindre end dimensionen af X. For en endelig morfi $\varphi\colon Y \to X$ må graden antage sin mindste værdi, e. Anvendes resultatet i (5.12) på et punkt i X, hvori denne mindste værdi e antages, sluttes det, at *graden* $\deg_p \varphi$ *er lig med e på nær eventuelt i endelig mange punkter p på X.*

For $X := \mathbf{A}^1$ gælder yderligere: *Lad Y være et integritetsskema, og lad $\varphi\colon Y \to \mathbf{A}^1$ være en endelig, dominerende morfi. Da er graden* $\deg_p \varphi$ *konstant som funktion af punkter p i $\mathbf{A}^1$.*

For at vise påstanden betragtes den til φ hørende homomorfi $A \to B$, hvor $A = k[T]$ er koordinatringen for $\mathbf{A}^1$ og og $B = \Gamma(Y)$. Ifølge forudsætningen er denne homomorfi injektiv, og B er endelig frembragt som A-modul. Videre er B et integritetsområde. Heraf følger øjensynlig, at annullatoren i A af et element forskelligt fra 0 i B kun består af nul-elementet i A. Da A som bekendt er et hovedidealområde, følger det af Struktursætningen for moduler over hovedidealområder, at B har en basis som A-modul. Der findes altså en A-lineær isomorfi $B \to A^e$. Af overvejelserne (5.11) sluttes nu for hvert punkt p i $\mathbf{A}^1$, at koordinatringen for fiberen, $\Gamma(\varphi^{-1}p) = B/\mathfrak{M}_p B$, som modul over $A/\mathfrak{M}_p = \boldsymbol{\kappa}(p)$ er isomorf med $\boldsymbol{\kappa}(p)^e$. Graden $\deg_p \varphi$ er derfor lig med e for det vilkårlige punkt $p \in \mathbf{A}^1$.

6. Plane kurver.

(6.1) Lemma. *Hvert primideal $\mathfrak{P}$ i $k[X_1, X_2]$ falder i netop én af følgende tre klasser: Klassen bestående alene af primidealet (0), klassen bestående af hovedidealer (P) frembragt af irreducible polynomier P, og klassen af maksimalidealer.*

Bevis. Da $k[X_1, X_2]$ er en faktoriel ring, er hovedidealet (P), hvor P er et irreducibelt polynomium, et primideal.

Det påstås først, at et sådant primideal (P) ikke kan være et maksimalideal. Antag, indirekte, at (P) er et maksimalideal. Maksimalidealet svarer da til et punkt i $\mathbf{A}^2$, og kvotienten $A := k[X_1, X_2]/(P)$ er restklasselegemet for dette punkt. Af Hilbert's Nulpunktssætning (4.5)(1) følger så, at kvotienten A er endeligdimensional over k. I kvotienten A er altså restklassen x_i af X_i modulo (P) derfor algebraisk over k. Der findes altså for $i = 1, 2$ normerede polynomier f_i således at $f_i(x_i) = 0$. Ligningen $f_1(x_1) = 0$ i kvotienten betyder, at $f_1(X_1) \in (P)$, altså at P er divisor i $f_1(X_1)$. Heraf følger, at X_2 ikke forekommer i polynomiet P. Tilsvarende ses, at X_1 ikke forekommer i P. Følgelig er P konstant, i modstrid med at P er antaget at være et irreducibelt polynomium.

Det skal dernæst vises, at et givet primideal $\mathfrak{P}$ nødvendigvis tilhører en af de tre klasser. Antag, at $\mathfrak{P} \neq 0$. Da findes et polynomium forskelligt fra 0 i $\mathfrak{P}$. Dette polynomium er et produkt af irreducible polynomier, og da $\mathfrak{P}$ er et primideal følger det at en af de irreducible faktorer P tilhører $\mathfrak{P}$. Altså er $(P) \subseteq \mathfrak{P}$. Antag nu yderligere, at $\mathfrak{P}$ ikke tilhører den anden klasse. Da er

$$(0) \subset (P) \subset \mathfrak{P}.$$

Det påstås, at $\mathfrak{P}$ så er et maksimalideal. Det er velkendt, at ringen $k[X_1, X_2]$ har transcendensgrad 2 over k. Heraf følger, at kvotienten $k[X_1, X_2]/(P)$ har transcendensgrad højst 1 over k, og videre, at kvotienten $A := k[X_1, X_2]/\mathfrak{P}$ har transcendensgrad højst 0 over k. Følgelig har A transcendensgrad 0 over k. Med andre ord er A algebraisk over k, og dermed specielt hel over k. Altså er A er et integritetsområde og helt over legemet k. Heraf følger som bekendt, at A er et legeme. Da A var kvotienten $k[X_1, X_2]/\mathfrak{P}$, er $\mathfrak{P}$ et maksimalideal, som påstået. ∎

(6.2) Definition. Ved en *plan kurve* forstås et skema C i $\mathbf{A}^2$ defineret ved et ikke-konstant polynomium F i $k[X_1, X_2]$. Kurvens ideal $\mathcal{I}(C)$ er altså hovedidealet (F), og koordinatringen $\Gamma(C)$ er kvotienten $k[X_1, X_2]/(F)$. Graden af polynomiet F kaldes også *graden af kurven* C, og denne grad betegnes også $\deg C$.

Betragt primopløsningen,

$$F = P_1^{n_1} \cdots P_r^{n_r}, \tag{6.2.1}$$

af polynomiet F. Som bekendt gælder da, at primidealerne (P_i) netop er de minimale primidealer for kvotienten $k[X_1, X_2]/(F)$. Kurverne C_i defineret ved polynomierne P_i er altså de maksimale integritetsskemaer i C. De kaldes også *komponenterne af kurven* C, jfr Observation (5.9). Eksponenten n_i kaldes også *multipliciteten af komponenten* C_i.

(6.3) Observation. En kurve C indeholder uendelig mange punkter. Polynomiet F, der definerer C har nemlig en irreducibel divisor P. Følgelig er $(F) \subseteq (P)$, så primidealet (P) svarer til et primideal i $\Gamma(C)$. Ifølge Lemma (6.1) er dette primideal ikke er et maksimalideal. Af betingelsen (5.1)(ii) følger derfor at C ikke kan være et endeligt skema.

Lad p være et punkt på kurven C. Den lokale ring $\mathcal{O}_{C,p}$ afhænger da kun af de komponenter, der indeholder p. Antag nemlig mere præcist, at C er bestemt ved polynomiet F med primopløsningen (6.2.1). Antag videre, at p tilhører komponenten C_i for $i = 1, \ldots, t$ og ikke for $i = t+1, \ldots, r$. Lad D være kurven defineret ved polynomiet $G := P_1^{n_1} \cdots P_t^{n_t}$. Det påstås, at de lokale ringe $\mathcal{O}_{C,p}$ og $\mathcal{O}_{D,p}$ er isomorfe. Ifølge definitionen er $\Gamma(C) = k[X_1, X_2]/(F)$ og $\Gamma(D) = k[X_1, X_2]/(G)$. Af Kvotientprincippet følger derfor, at

$$\mathcal{O}_{C,p} = k[X_1, X_2]_{\mathfrak{M}_p}/(F) \quad \text{og} \quad \mathcal{O}_{D,p} = k[X_1, X_2]_{\mathfrak{M}_p}/(G).$$

Nu var $F = HG$, hvor de irreducible faktorer i H netop er P_i'erne, som ikke tilhører $\mathfrak{M}_p$. Polynomiet H tilhører derfor ikke $\mathfrak{M}_p$, og følgelig er H invertibel i den lokale ring $k[X_1, X_2]_{\mathfrak{M}_p}$. I denne lokale ring er hovedidealerne frembragt af $F = HG$ og G derfor ens, hvoraf påstanden følger.

(6.4) Definition. Ethvert polynomium F i $k[X_1, X_2]$ har en fremstilling,

$$F = F_0 + F_1 + F_2 + \cdots \tag{6.4.1}$$

som en (endelig) sum af homogene polynomier F_i af grad i, kaldet de *homogene led* i F. Leddet F_0 er konstantleddet i F. Leddet F_1 er førstegradspolynomiet $(\partial F/\partial X_1)(o)X_1 + (\partial F/\partial X_2)(o)X_2$, hvor de partielle afledede er taget i det rationale punkt $o = (0, 0)$. Det største i for hvilket $F_i \neq 0$ er graden af polynomiet F. Det mindste i for hvilket $F_i \neq 0$ kaldes polynomiets *orden* eller *multiplicitet i punktet* o. Ordenen er øjensynlig positiv, hvis og kun hvis o er et nulpunkt for F. Bemærk, at ordenen h er mindre end eller lig med graden d, hvis F ikke er nulpolynomiet, og at fremstillingen (6.4.1) i så fald er en fremstilling,

$$F = F_h + \cdots + F_d. \tag{6.4.2}$$

Nulpolynomiet tillægges sædvanligvis orden $+\infty$. Bemærk, at potensen $\mathfrak{M}^h$ af maksimalidealet $\mathfrak{M} := (X, Y)$ netop består af polynomier af orden mindst h.

Mere generelt defineres multipliciteten af F i et vilkårligt punkt $(p_1, p_2) \in k^2$ som multipliciteten i $o = (0, 0)$ af polynomiet $F(X_1 + p_1, X_2 + p_2)$.

Lad C være kurven defineret ved polynomiet F, og lad $p = (p_1, p_2)$ være et rationalt punkt på C. Ved *multipliciteten i punktet* p af kurven C forstås da multipliciteten af F i punktet p. Multipliciteten i p betegnes $\mathrm{mult}_p(C)$. Den er positiv, hvis og kun hvis punktet p tilhører C. Det er ofte bekvemt at udstrække definitionen og sætte multipliciteten til 0 i punkter p, der ikke ligger på kurven.

(6.5) Sætning. *Lad p være et rationalt punkt på kurven C, og lad $\mathfrak{m}$ betegne maksimalidealet i den lokale ring $\mathcal{O}_{C,p}$. Da er*

$$\mathrm{mult}_p(C) = \dim_k \mathfrak{m}^i/\mathfrak{m}^{i+1} \text{ for } i \gg 0. \tag{6.5.1}$$

Bevis. Det er nok at vise påstanden for $p = o$. Parallelforskydning $x \mapsto x+p$ definerer nemlig en isomorfi $\mathbf{A}^2 \to \mathbf{A}^2$, så der findes en kurve C' der ved parallelforskydningen føres over i C. Herved svarer punktet o på C' til punktet p på C. Venstresiden i ligningen er ifølge definitionen multipliciteten af C' i punktet o, og højresiden ændres ikke, når ringen $\mathcal{O}_{C,p}$ erstattes med den isomorfe ring $\mathcal{O}_{C',o}$.

Antag altså, at $p = o$. Venstresiden i ligningen i (6.5.1) er altså ordenen h af polynomiet F, betragtet i (6.4.2). Betragt nu for $\mathcal{O} := \mathcal{O}_{C,p}$ den eksakte følge,

$$0 \to \mathfrak{m}^i/\mathfrak{m}^{i+1} \to \mathcal{O}/\mathfrak{m}^{i+1} \to \mathcal{O}/\mathfrak{m}^i \to 0.$$

Højresiden i ligningen (6.5.1) er dimensionen af vektorrummet $\mathfrak{m}^i/\mathfrak{m}^{i+1}$, og altså lig med differensen mellem dimensionerne af det midterste vektorrum og det efterfølgende. Det er derfor nok at vise, at der findes en konstant h_1 således at

$$\dim_k \mathcal{O}/\mathfrak{m}^i = hi + h_1 \text{ for } i \gg 0. \tag{6.5.2}$$

Den lokale ring $\mathcal{O}$ fremkommer ved lokalisering af $\Gamma(C)$ i maksimalidealet $\mathfrak{M}_{C,o}$. Af en velkendt egenskab ved maksimalidealer følger derfor, at kvotienten $\mathcal{O}/\mathfrak{m}^i$ er isomorf med kvotienten $\Gamma(C)/\mathfrak{M}^i_{C,o}$.

Sæt nu videre $\mathfrak{M} := \mathfrak{M}_o = (X_1, X_2)$. Det følger da af Noether's anden Isomorfisætning, at kvotienten $\Gamma(C)/\mathfrak{M}^i_{C,o}$ er isomorf med $k[X_1, X_2]/(\mathfrak{M}^i, F)$.

Endelig består idealet $\mathfrak{M}^i$ af polynomier af orden mindst i. Antag, at $i \geq h$. Da definerer multiplikationen $G \mapsto FG$ en k-lineær afbildning, og FG tilhører $\mathfrak{M}^i$, hvis og kun hvis G tilhører $\mathfrak{M}^{i-h}$. Heraf udledes let den exakte følge,

$$0 \to k[X_1, X_2]/\mathfrak{M}^{i-h} \xrightarrow{F} k[X_1, X_2]/\mathfrak{M}^i \to k[X_1, X_2]/(\mathfrak{M}^i, F) \to 0.$$

Af exaktheden følger, at dimensionen af det midterste vektorrum er summen af dimensionerne af de to omgivende. Det er let at se, at kvotienten $k[X_1, X_2]/\mathfrak{M}^i$ har dimension $\binom{i+1}{2}$. Af de fundne isomorfier følger derfor for $i \geq h$, at

$$\dim_k \mathcal{O}/\mathfrak{m}^i = \binom{i+1}{2} - \binom{i-h+1}{2} = hi - \frac{h(h-1)}{2}.$$

Heraf fremgår resultatet (6.5.2) (med $h_1 := -h(h-1)/2$), som ønsket. ∎

(6.6) Note. Lad p være et punkt på et skema X. Betragt den lokale ring $\mathcal{O} := \mathcal{O}_{X,p}$ med maksimalidealet $\mathfrak{m} := \mathfrak{m}_{X,p}$. Det er klart, at for hvert i har kvotienten $\mathcal{O}/\mathfrak{m}^i$ endelig længde. Sæt $\lambda(i) := \operatorname{long} \mathcal{O}/\mathfrak{m}^i$.

Antag først, at X er et endelig skema. I dette tilfælde er multipliciteten af X i p defineret som længden af ringen $\mathcal{O}$. Da længden er endelig, gælder $\mathfrak{m}^i = \mathfrak{m}^{i+1}$, når $i \gg 0$, og så følger af Nakayama's Lemma, at $\mathfrak{m}^i = (0)$, når $i \gg 0$. Med andre ord: Når $i \gg 0$ er funktionen $\lambda(i)$ konstant og lig med $\operatorname{mult}_p(X)$.

Antag dernæst, at X er en plan kurve og at p er et rationalt punkt på X. Da er $\mathcal{O}/\mathfrak{m} = k$, og følgelig er $\lambda(i) = \dim_k \mathcal{O}/\mathfrak{m}^i$. Af beviset for den foregående sætning følger derfor, at for $i \gg 0$ er $\lambda(i) = hi + h_1$, hvor h er kurvens multiplicitet i punktet p. Når $i \gg 0$ er funktionen $\lambda(i)$ altså et førstegradspolynomium.

I almindelighed (dvs for et vilkårligt punkt p på et vilkårligt skema X) kan man vise, at funktionen $\lambda(i)$ for $i \gg 0$ er et polynomium, dvs er af formen

$$\lambda(i) = hi^d + h_1 i^{d-1} + \cdots + h_d;$$

multipliciteten af skemaet X i p defineres som højrestegradskoefficienten h ganget med $d!$. Hvis X er et integritetsskema er tallet d lig med dimensionen af X.

(6.7) Sætning. *Lad C være en plan kurve defineret ved polynomiet F og lad p være et rationalt punkt på C. Da er følgende fem betingelser ækvivalente:*

(i) *Kurven C har multiplicitet 1 i punktet p.*
(ii) *En af de partielle afledede $\partial F/\partial X_i$ er forskellig fra 0 i punktet p.*
(iii) *Den lokale ring $\mathcal{O}_{C,p}$ er et integritetsområde, ikke et legeme, og maksimalidealet $\mathfrak{m}_{C,p}$ er et hovedideal.*
(iv) *Den lokale ring $\mathcal{O}_{C,p}$ er en valuationsring, dvs et integritetsområde, ikke et legeme, hvori idealerne er totalt ordnede.*
(v) *Den lokale ring $\mathcal{O}_{C,p}$ er et hovedidealområde, ikke et legeme.*

Bevis. Det er velkendt for noetherske ringe, at betingelserne (iii), (iv) og (v) er ækvivalente, og denne ækvivalens antages i det følgende.

Ifølge definitionen bestemmes multipliciteten i p ved at betragte de homogene led G_i af polynomiet $G(X_1, X_2) = F(X_1 + p_1, X_2 + p_2)$. Konstantleddet G_0 er $G(o) = F(p)$, som er 0 da p tilhører F, og

$$G_1 = \frac{\partial F}{\partial X_1}(p)X_1 + \frac{\partial F}{\partial X_2}(p)X_2.$$

At multipliciteten er lig med 1 betyder, at $G_1 \neq 0$. Det er herefter klart, at (i) og (ii) er ækvivalente. For at bevise den fulde ækvivalens kan det antages, jfr beviset for Sætning (6.5), at p er punktet $o = (0, 0)$. Det er nok at vise, at (i) medfører (iii) og at (iv) medfører (i).

Antag først, at (i) (og dermed også (ii)) er opfyldt. Det kan yderligere antages, at F er et irreducibelt polynomium. I almindelighed er F nemlig et produkt, $F =$

$P_1 \cdots P_t$, hvor P_i'erne er (ikke nødvendigvis forskellige) irreducible polynomier. Udfra definitionen er det klart, at F's orden i o er summen af P_i'ernes orden i o. Da F's orden ifølge antagelsen er lig med 1, har netop ét af P_i'erne orden 1, og de øvrige P_i'er har orden 0. Antag fx at $P = P_1$ har orden 1, og lad D være kurven bestemt ved polynomiet P. Af Observation (6.3) følger nu, at den lokale ring $\mathcal{O}_{C,o}$ ikke ændres når C erstattes med D. I stedet for at erstatte C med D (og F med P), kan vi følgelig antage, at F er et irreducibelt polynomium.

Idealet (F) er nu et primideal, og koordinatringen $\Gamma(C) = k[X_1, X_2]/(F)$ er derfor et integritetsområde. Den lokale ring $\mathcal{O}$ fremkommer af $\Gamma(C)$ ved at lokalisere i $\mathfrak{M}_{C,o}$, og den er derfor ligeledes et integritetsområde, og øjensynlig ikke et legeme. Idealet $\mathfrak{M}_o$ er frembragt af X_1 og X_2, så maksimalidealet $\mathfrak{m} := \mathfrak{m}_{C,o}$ er frembragt af billederne x_1 og x_2 af X_1 og X_2. Det påstås, at maksimalidealet $\mathfrak{m}$ i $\mathcal{O}$ er frembragt af ét af x_i'erne. Mere præcist følger det af (ii), at en af de afledede $a_i := (\partial F/\partial X_i)(o)$ er forskellig fra 0. Antag fx at $a_2 \neq 0$. Det påstås, at billedet x_1 så frembringer idealet $\mathfrak{m}$.

Ifølge antagelsen er F en sum, $F = a_1X_1 + a_2X_2 + \cdots$, hvor de tre prikker betegner en sum af led af grad mindst 2. Summen grupperes, idet vi først samler alle led, der indeholder X_2, og dernæst sætter X_1 uden for parentes i de resterende. Herved fremkommer en ligning,

$$F = SX_2 + TX_1, \quad \text{hvor } S = a_2 + \cdots,\ T = a_1 + \cdots.$$

Modulo (F) er venstresiden lig med 0, så i $\mathcal{O}$ fås ligningen $0 = sx_2 + tx_1$, hvor s og t betegner billederne af S og T. Ifølge antagelsen er $S(o) = a_2$ forskellig fra 0. Polynomiet S tilhører derfor ikke $\mathfrak{M}_o$, så billedet s er invertibelt i $\mathcal{O}$. Af ligningen $sx_2 + tx_1 = 0$ følger derfor, at der i brøkringen $\mathcal{O}$ gælder at $x_2 \in \mathcal{O}x_1$. Som nævnt var maksimalidelet $\mathfrak{m}$ frembragt af x_1 og x_2. Af det viste følger, at frembringeren x_2 er overflødig. Altså er $\mathfrak{m}$ lig med hovedidealet $\mathcal{O}x_1$.

Hermed er det vist, at den lokale ring $\mathcal{O}$ opfylder betingelsen (iii). Betingelsen (i) medfører altså (iii). Omvendt vil (iv) medføre (i). Når $\mathcal{O}$ er en valuationsring, er det nemlig klart, at $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ er et 1-dimensionalt vektorrum over restklasselegemet $\mathcal{O}/\mathfrak{m}$. Her er $\mathcal{O}/\mathfrak{m} = k$, da punktet o er et rationalt punkt. Af Sætning (6.5) følger derfor, at multipliciteten af C i punktet o er lig med 1.

Hermed er ækvivalensen af de fem betingelser eftervist. ∎

(6.8) Definition. Lad p være et rationalt punkt på kurven C. Kurven siges da at være *glat i punktet* p, hvis de ækvivalente betingelser i Sætning (6.7) er opfyldt. Hvis C er glat i punktet $p = (p_1, p_2)$ siges „linien" L med ligningen,

$$(\partial F/\partial X_1)(p)(X_1 - p_1) + (\partial F/\partial X_2)(p)(X_2 - p_2) = 0,$$

også at være kurvens *tangent* i punktet p.

Bemærk, at „glathed" herved kun er defineret for rationale punkter på C. Hvis punktet p på C ikke er et rationalt punkt, siges C at være glat i p, hvis den lokale ring $\mathcal{O}_{C,p}$ er en valuationsring. Punkter p, hvori kurven ikke er glat, kaldes også *singulære* eller *multiple* punkter på kurven.

(6.9) Eksempel. En *linie*, også kaldet en førstegradkurve, er en kurve givet ved et polynomium $a_1X_1 + a_2X_2 + b$, hvor a_1 og a_2 ikke begge er 0. Den er øjensynlig glat i ethvert af sine rationale punkter, og i ethvert sådant punkt er linien selv tangenten. Man kan vise, at en linie faktisk er glat i alle sine punkter.

(6.10) Eksempel. Betragt dernæst et *keglesnit* C, også kaldet en andengradskurve, dvs en kurve givet ved et andetgradspolynomium F. Hvis legemet k ikke er algebraisk afsluttet kan det ikke udelukkes, at C slet ikke indeholder rationale punkter. Antag nu, at der findes et rationalt punkt, hvori kurven ikke er glat. Efter en parallelforskydning kan det antages, at dette multiple punkt er punktet $o = (0, 0)$. Da er $F_0 = F_1 = 0$, så polynomiet F har formen,

$$F = aX_1^2 + bX_1X_2 + cX_2^2.$$

Antag i det følgende, at legemet k ikke har karakteristik 2. Lad $d = b^2 - 4ac$ betegne diskriminanten af polynomiet F. Hvis $a \neq 0$, så gælder ligningen,

$$4aF = (2aX_1 + bX_2)^2 - dX_2^2.$$

Heraf, og af et par trivielle overvejelser hvis $a = 0$, fås følgende klassifikation:

$d = 0$. I dette tilfælde er F, bortset fra en konstant faktor, kvadratet på et førstegradspolynomium. Dette førstegradspolynomium svarer til en linie som er komponent med multiplicitet 2 af C. Alle rationale punkter på C er multiple.

$d \neq 0$ og d er et kvadrat i k. I dette tilfælde er F et produkt af 2 førstegradspolynomier, svarende til at C's komponenter er to forskellige linier gennem o, begge med multiplicitet 1. Øjensynlig er C er glat i alle rational punkter, på nær liniernes skæringspunkt o.

$d \neq 0$ og d er ikke kvadratet på et element i k. I dette tilfælde er o det eneste rationale punkt på C.

Bemærk, at hvis et andetgradspolynomium er reducibelt, så er det et produkt af to førstegradspolynomier, og for det tilsvarende keglesnit er komponenterne to linier. Dette er situationen i de første to tilfælde behandlet ovenfor. Ud over disse tilfælde kunne de to komponenter være parallelle linier.

(6.11) Eksempel. Betragt endelig en *kubisk kurve* C, dvs en kurve defineret ved et polynomium F af grad 3. Antag fx, at $F = X_2^2 - f(X_1)$, hvor f er et polynomium af grad 3 (i én variabel). De partielle afledede er $\partial F/\partial X_1 = -f'(X_1)$ og $\partial F/\partial X_2 = 2X_2$. Antag, at karakteristikken for k ikke er 2. Da er $\partial F/\partial X_2$ forskellig fra 0 i alle punkter (p_1, p_2), hvor $p_2 \neq 0$. Kurven er altså glat i alle rationale punkter, der ikke ligger på X_1-aksen. Betragt dernæst et rationalt punkt på X_1-aksen, dvs et punkt af formen $(p_1, 0)$. Punktet ligger på kurven, hvis og kun hvis $f(p_1) = 0$, dvs hvis og kun hvis p_1 er rod i f, og kurven er glat i punktet, hvis og kun hvis der yderligere gælder at $f'(p_1) \neq 0$. De to betingelser, $f(p_1) = 0$ og $f'(p_1) \neq 0$, er som bekendt opfyldt, netop hvis p_1 er en simpel rod i f. Trediegradspolynomiet f kan højst have én multipel rod. Følgelig er C glat i alle sine rationale punkter, på nær eventuelt i ét punkt af formen $(p_1, 0)$ svarende til en multipel rod p_1 i f.

7. Snit af kurver.

(7.1) Definition. Lad C og D være to plane kurver definerede ved polynomier F og G. Snittet $C \cap D$ er da skemaet defineret ved idealet (F, G) i $k[X_1, X_2]$, og et punkt p tilhører snittet, hvis og kun hvis det tilhører begge kurver. For hvert punkt p i $C \cap D$ defineres *snitmultipliciteten* i p som tallet

$$i_p(C.D) := \operatorname{long} \mathcal{O}_{C\cap D,p}.$$

Snitmultipliciteten kan være ∞; den er endelig, når den lokale ring på højresiden har endelig længde. Det er sædvane at sætte $i_p(C.D) := 0$ for punkter p, som ikke tilhører snittet $C \cap D$.

Hvis snittet $C \cap D$ er et endeligt skema, så er snitmultipliciteterne endelige, idet $i_p(C.D) = \operatorname{mult}_p(C \cap D)$, jfr Definition (5.2).

Ofte lader man polynomierne indgå i betegnelserne, og skriver $i_p(F.G) = i_p(C.D)$. Yderligere udstrækkes denne betegnelse til tilfældet hvor et eller begge polynomier er konstant: Hvis et af polynomierne F, G ikke tilhører $\mathfrak{M}_p$, sættes $i_p := 0$. Hvis de begge tilhører $\mathfrak{M}_p$ og et af dem er nulpolynomiet, sættes $i_p := \infty$.

(7.2) Observation. Antag, at p tilhører snittet $C \cap D$. Restklasselegemet for den lokale ring $\mathcal{O}_{C\cap D,p}$ er da legemet $\boldsymbol{\kappa}(p)$, jfr (4.4). Ifølge Hilbert's Nulpunktssætning (4.5) er restklasselegemet $\boldsymbol{\kappa}(p)$ af endelig dimension over k. Heraf ses, at den lokale ring har endelig længde, hvis og kun hvis den har endelig dimension som vektorrum over k, jfr beviset for Korollar (5.3). Specielt ses, at snitmultipliciteten $i_p(C.D)$ er endelig, hvis og kun hvis den lokale ring $\mathcal{O}_{C\cap D,p}$ er af endelig dimension over k.

(7.3) Observation. Lad p være et punkt i $C \cap D$. Koordinatringen for snittet $C \cap D$ er kvotienten $\Gamma(C \cap D) = k[X_1, X_2]/(F, G)$. Følgelig er $\Gamma(C \cap D)$ isomorf med kvotienten af $\Gamma(C) = k[X_1, X_2]/(F)$ modulo idealet frembragt af billedet af G. Idet (G) også – sjusket, men praktisk – betegner hovedidealet i $\Gamma(C)$ frembragt af billedet af G, er altså

$$\Gamma(C \cap D) = \Gamma(C)/(G).$$

Herved svarer maksimalidealet $\mathfrak{M}_{C\cap D,p}$ i kvotienten $\Gamma(C \cap D)$ til maksimalidealet $\mathfrak{M}_{C,p}$ i $\Gamma(C)$. Ved lokalisering af $\Gamma(C)$ i $\mathfrak{M}_{C,p}$ fremkommer den lokale ring $\mathcal{O}_{C\cap D,p}$, og ved lokalisering af $\Gamma(C \cap D)$ i $\mathfrak{M}_{C\cap D,p}$ fremkommer den lokale ring $\mathcal{O}_{C,p}$. Af Kvotientprincippet fås derfor en isomorfi,

$$\mathcal{O}_{C\cap D,p} \simeq \mathcal{O}_{C,p}/(G),$$

hvor (G) på højresiden nu betegner hovedidealet frembragt af billedet af G i $\mathcal{O}_{C,p}$. Det følger specielt, jfr Observation (6.3), at snitmultipliciteten $i_p(C.D)$ kun afhænger af de af C's komponenter, der indeholder p. Med andre ord kan man ved bestemmelse af snitmultipliciteten $i_p(C.D)$ fra F fjerne de irreducible faktorer, der ikke tilhører $\mathfrak{M}_p$.

Det følger ligeledes af Kvotientprincippet, at den lokale ring $\mathcal{O}_{C\cap D,p}$ også kan fås som kvotienten af den lokale ring $k[X_1, X_2]_{\mathfrak{M}_p}$, dvs af $\mathcal{O}_{\mathbf{A}^2,p}$, modulo idealet (F, G) frembragt af F og G heri.

(7.4) Sætning. *Lad C og D være plane kurver bestemt ved polynomierne F og G. Da er snittet $C \cap D$ et endeligt skema, hvis og kun hvis C og D ikke har fælles komponenter, dvs hvis og kun hvis polynomierne F og G er primiske. Yderligere gælder for et punkt p på $C \cap D$, at snitmultipliciteten $i_p(C.D)$ er endelig, hvis og kun hvis de to kurver ikke har fælles komponenter, der indeholder p.*

Bevis. Hvis F og G har en ikke-triviel fælles divisor H, så er $(F, G) \subseteq (H)$. Snittet $C \cap D$, der er defineret ved idealet (F, G), vil altså indeholde kurven bestemt ved polynomiet H. Af Observation (6.3) følger derfor, at $C \cap D$ indeholder uendelig mange punkter.

Antag omvendt, at $C \cap D$ indeholder uendelig mange punkter. Af Sætning (5.1) følger så, at koordinatringen $k[X_1, X_2]/(F, G)$ indeholder et primideal, der ikke er et maksimalideal. Dette primideal svarer ifølge Kvotientprincippet til et primideal $\mathfrak{P}$ i $k[X_1, X_2]$, som ikke er et maksimalideal og som omfatter (F, G). Ifølge Lemma (6.1) er $\mathfrak{P}$ et hovedideal (P). Af $(F, G) \subseteq (P)$ følger nu, at P er en ikke-triviel fælles divisor i F og G, som ønsket.

Hermed er sætningens første påstand bevist. For at vise den anden påstand betragtes et punkt $p \in C \cap D$. Antag først, at de to kurver ikke har fælles komponenter, der indeholder p. Den lokale ring $\mathcal{O}_{C\cap D,p}$ afhænger kun af de komponenter, der indeholder p, jfr Observation (6.3). Følgelig kan det antages, at kurverne C og D ikke har fælles komponenter. Af det allerede viste følger, at $C \cap D$ så er et endeligt skema. Snitmultipliciteten er da $i_p(C.D) = \mathrm{mult}_p(C \cap D)$, og specielt er den endelig.

Antag dernæst, at de to kurver har en fælles komponent gennem p. Det er nok at vise, jfr Observation (7.2), at den lokale ring $\mathcal{O}_{C\cap D,p}$ er uendeligdimensional som vektorrum over k. Det følger af antagelsen, at polynomierne F og G har en irreducibel fælles divisor P, således at $P \in \mathfrak{M}_p$. Nu er $(F, G) \subseteq (P) \subseteq \mathfrak{M}_p$. Lad E være kurven bestemt ved P. Det følger af Kvotientprincippet, at den lokale ring $\mathcal{O}_{E,p}$ er lig med kvotienten af $\mathcal{O}_{C\cap D,p}$ modulo idealet frembragt af billedet af P. Det er således nok at vise, at den lokale ring $\mathcal{O}_{E,p}$ er uendeligdimensional. Denne lokale ring er en lokalisering af $\Gamma(E)$, og da $\Gamma(E)$ er et integritetsområde vil den lokale ring indeholde $\Gamma(E)$. Som nævnt i Observation (6.3) er E ikke et endeligt skema, og af betingelsen (5.1)(iv) følger derfor, at $\Gamma(E)$ er uendeligdimensional. Heraf følger påstanden.

Hermed er de to påstande i Sætningen bevist. ∎

(7.5) Sætning. *Lad p være et rationalt punkt, der tilhører begge kurver C og D. Da er snitmultipliciteten $i_p(C.D)$ lig med 1, hvis og kun hvis kurverne C og D er glatte i p med forskellige tangenter.*

Bevis. Det kan antages, at p er punktet $o = (0, 0)$. Lad F og G være polynomierne, der definerer C og D. Den lokale ring $\mathcal{O} := \mathcal{O}_{C\cap D,o}$ fremkommer ved lokalisering af $k[X_1, X_2]/(F, G)$ i maksimalidealet $\mathfrak{M}_o$ svarende til punktet o. Maksimalidealet $\mathfrak{M}_o$ er frembragt af X_1 og X_2, så maksimalidealet $\mathfrak{m}$ i $\mathcal{O}$ er frembragt af billederne x_1 og x_2 af X_1 og X_2. Snitmultipliciteten $i_o(C.D)$ er længden af den lokale ring $\mathcal{O}$. At snitmultipliciteten er lig med 1 er således ensbetydende med at $\mathfrak{m} = (0)$.

Da punktet o ligger på begge kurver findes på den anden side fremstillinger,

$$F = a_{11}X_1 + a_{12}X_2 + \cdots \text{ og } G = a_{21}X_1 + a_{22}X_2 + \cdots ,$$

hvor de tre prikker står for summer af led af grad mindst 2. Lad α betegne 2×2 matricen (a_{ij}). Det er klart, at begge kurver er glatte i o, med forskellige tangenter, hvis og kun hvis determinanten $\det \alpha$ er forskellig fra 0. Det skal altså vises, at $\det \alpha \neq 0$, hvis og kun hvis $\mathfrak{m} = (0)$.

Antag først, at $\det \alpha \neq 0$. Leddene af grad mindst 2 i fremstillingerne ovenfor tilhører $\mathfrak{M}_o^2$, og modulo (F, G) er venstresiderne lig med 0. Af fremstillingerne følger derfor, at søjlen $\alpha\binom{x_1}{x_2}$ tilhører $\mathfrak{m}^2$. Da matricen α er invertibel følger det, at søjlen $\binom{x_1}{x_2}$ tilhører $\mathfrak{m}^2$. Maksimalidealet er frembragt af x_1 og x_2. Af det viste følger derfor, at $\mathfrak{m} = \mathfrak{m}^2$. Af Nakayama's Lemma fås derfor, at $\mathfrak{m} = (0)$.

Antag omvendt, at $\mathfrak{m} = (0)$. Billedet x_i af X_i er altså lig med 0 i den lokale ring $\mathcal{O}$. Den lokale ring er en lokalisering af koordinatringen $k[X_1, X_2]/(F, G)$. Der findes derfor polynomier S_i i $k[X_1, X_2]$, så at $S_i(o) \neq 0$ og så at S_iX_i tilhører idealet (F, G). For $i = 1, 2$ findes derfor polynomier B_{i1} og B_{i2} så at

$$S_iX_i = B_{i1}F + B_{i2}G. \tag{7.5.1}$$

Lad s_i og b_{ij} betegne konstantleddene i polynomierne S_i og B_{ij}. Ved sammenligning af førstegradsleddene på de to sider af ligning (7.5.1) fås ligningen

$$s_iX_i = b_{i1}(a_{11}X_1 + a_{12}X_2) + b_{i2}(a_{21}X_1 + a_{22}X_2). \tag{7.5.2}$$

Lad β betegne 2×2 matricen (b_{ij}), og lad σ betegne diagonalmatricen med s_1 og s_2 i diagonalen. Ligningerne (7.5.2) for $i = 1, 2$ kan da sammenfattes til matrixligningen $\sigma = \beta\alpha$. Da $s_1s_2 \neq 0$, følger det af matrixligningen, at $\det \alpha \neq 0$.

Hermed er det ønskede bevist. ∎

(7.6) Note. Under forudsætningen i Sætning (7.5) kan man vise, at

$$i_p(C.D) \geq \text{mult}_p(C) \cdot \text{mult}_p(D),$$

altså at snitmultipliciten i p er større end eller lig med produktet af de to kurvers multiplicitet i p. Yderligere er det nemt at afgøre hvornår lighed indtræffer, idet der gælder følgende (som vi for letheds skyld formulerer for $p = o$): Ligheden $i_o(C.D) = \text{mult}_o(C) \cdot \text{mult}_o(D)$ gælder, hvis og kun hvis de homogene led af laveste orden i F og G er primiske.

(7.7) Hovedsætning. *Snitmultiplicitet $i_p(F.G)$, for punkter p i $\mathbf{A}^2$ og polynomier F, G i $k[X_1, X_2]$, har følgende egenskaber:*

(1) *Værdierne opfylder $0 \leq i_p(F.G) \leq \infty$. Værdien er positiv, hvis og kun hvis begge polynomier tilhører maksimalidealet $\mathfrak{M}_p$, og værdien er ∞, hvis og kun hvis de to polynomier har en fælles irreducibel divisor, som tilhører $\mathfrak{M}_p$.*

(2) *Snitmultiplicitet afhænger kun af idealet* (F, G). *Specielt er værdien* $i_p(F.G)$ *symmetrisk i* F *og* G, *og den afhænger kun af* G*'s restklasse modulo* (F).

(3) *Snitmultiplicitet adderes når funktioner multipliceres i den forstand at*

$$i_p(F.GH) = i_p(F.G) + i_p(F.H).$$

(4) *Snitmultiplicitet er invariant under isomorfi (specielt under parallelforskydning) af* $\mathbf{A}^2$. *For* $p = o$ *og* $F = X_2$ *er snitmultipliciteten* $i_o(X_2.G)$ *lig med ordenen af polynomiet* $G(X_1, 0)$.

Bevis. Påstanden (1) følger umiddelbart af Sætning (7.4). Påstand (2) følger af definitionen, jfr Observation (7.3).

For at vise additiviteten i (3) betragtes et produkt GH. Påstanden er triviel, hvis F er konstant, eller hvis G eller H er nul-polynomiet. Antag derfor, at F ikke er konstant og at G og H er forskellige fra nul-polynomiet. Ifølge Observation (7.3) kan det videre antages, at alle irreducible divisorer i F tilhører maksimalidealet $\mathfrak{M}_p$. Lad C være kurven defineret ved polynomiet F. Punktet p ligger så på C. Yderligere kan det antages, at ingen af polynomierne G og H har en ikke-triviel divisor fælles med F, idet additiviteten ellers er en konsekvens af (1). Lad nu $A = k[X_1, X_2]/(F)$ være koordinatringen for C, og sæt $\mathcal{O} := \mathcal{O}_{C,p}$. Den lokale ring $\mathcal{O}$ fås altså ved at lokalisere A i maksimalidealet $\mathfrak{M}_{C,p}$. Lad videre g og h betegne restklasserne af G og H modulo (F). De tre snitmultipliciteter er da ifølge Observation (7.3) længderne af følgende kvotienter: $\mathcal{O}/gh\mathcal{O}$, $\mathcal{O}/g\mathcal{O}$ og $\mathcal{O}/h\mathcal{O}$. Disse kvotienter fås ved lokalisering i $\mathfrak{M}_{C,p}$ af modulerne i følgen,

$$0 \to A/(h) \xrightarrow{g} A/(gh) \to A/(g) \to 0, \tag{7.7.1}$$

hvor den første homomorfi er induceret af multiplikation med g. Det er nok at vise, at følgen (7.7.1) er exakt, thi så er også den lokaliserede følge exakt, og den søgte additivitet følger af at længde af moduler er additiv på exakte følger.

Følgen (7.7.1) er trivielt exakt bortset fra at det kræver en overvejelse at multiplikation med g inducerer en injektiv homomorfi. Hertil bemærkes, at de tre midterste moduler i følgen øjensynlig er kokernerne for multiplikation i A med h, med gh, og med g. Bortset fra nul-modulen til venstre er følgen (7.7.1) altså den sidste del af kerne-kokerne følgen for den sammensatte multiplikation gh. Da kerne-kokerne følgen for en sammensat homomorfi som bekendt er exakt, er det derfor nok at vise, at kernen for multiplikation med g kun består af nul-elementet i A.

Antag altså, at $r \in A$ og at $gr = 0$. Ringen A er kvotientringen af $k[X_1, X_2]$ modulo (F), så r repræsenteres af et polynomium $R \in k[X_1, X_2]$. Produktet gr repræsenters da af polynomiet GR, så ifølge antagelsen er GR kongruent med 0 modulo (F). Altså er F divisor i GR. Da polynomiumsringen $k[X_1, X_2]$ er faktoriel og G var antaget primisk med F, følger det, at F er divisor i R. Restklassen r er derfor lig med nul-elementet i A. Hermed er det ønskede opnået, og additiviteten i (3) er eftervist.

Den første påstand i (4) følger af at den lokale ring, der definerer $i_p(F.G)$, erstattes med en isomorf, når der anvendes en isomorfi af $\mathbf{A}^2$. Antag endelig, at $p = o$ og at $F = X_2$. Ifølge (2) er snitmultipliciteten $i_p(X_2.G)$ uændret når G erstattes med et polynomium, der er kongruent med G modulo (X_2). Polynomiet G kan derfor erstattes med polynomiet $G(X_1, 0)$. Hvis dette sidste polynomium er nulpolynomiet, så er både orden og snitmultiplicitet lig med ∞. Hvis det sidste polynomium har endelig orden h, så kan det skrives $X_1^h\tilde{G}(X_1)$, hvor $\tilde{G}(o) \neq 0$. Af definitionen følger så umiddelbart, at $i_o(X_2, \tilde{G}) = 0$. Den multiplikative egenskab (3) giver derfor,

$$i_o(X_2, G) = hi_o(X_2, X_1) = h,$$

hvor den sidste ligning enten ses direkte af definitionen, eller ved brug af Sætning (7.5). Heraf aflæses den sidste påstand i (4).

Hermed er de fire egenskaber bevist. ∎

(7.8) Note. Snitmultipliciteten er i Definition (7.1) bestemt ved en simpel algebraisk formel. Denne definition kan ses som afslutningen på en lang diskussion, der foregik i det meste af forrige århundrede. Det skal understreges, at det i praksis er ganske let at bestemme snitmultipliciteten i et givet (rationalt) punkt alene ved brug af de i Hovedsætningen angivne egenskaber. Problemet er at give en definition, der tillader at udlede disse egenskaber.

Snitmultipliciteten i et rationalt punkt kan bestemmes ved en metode, der essentielt er Euklid's algoritme: Ved en simpel parallelforskydning kan det antages at punktet er $o = (0, 0)$. Bemærk, at snitmultipliciteten i_o umiddelbart kan bestemmes hvis et af polynomierne F og G kun afhænger af den variable X_2. Antag nemlig, at fx F kun afhænger af X_2. Hvis $F(o) \neq 0$ eller $G(o) \neq 0$, så er $i_o = 0$. Betragt derfor tilfældet, hvor $F(o) = G(o) = 0$. Hvis $F = 0$, så er $i_o = \infty$, og hvis $F \neq 0$, så har F specielt formen $F = X_2^dH$, hvor $H(o) \neq 0$; af reglerne (3), (4) og (1) følger så, at i_o er lig med d gange ordenen af polynomiet $G(X_1, 0)$.

Sæt nu $i := 0$ og gennemløb følgende algoritme:

A1. Hvis F eller G kun afhænger af X_2, så sættes $i := i + i_o(F.G)$ og algoritmen stoppes.

A2. Hvis begge polynomier er delelige med X_2, så sættes $i := \infty$ og algoritmen stoppes.

A3. Hvis et af polynomierne F eller G, fx G, er deleligt med X_2, så sættes $G := G/X_2$ og $i := i + i_o(F.X_2)$. Dette gentages indtil ingen af polynomierne er delelige med X_2.

A4. De to polynomier ordnes efter potenser af X_1,

$$F = fX_1^d + \cdots, \quad G = gX_1^e + \cdots,$$

hvor f og g er polynomier forskellige fra 0, der kun afhænger af X_2, og hvor de tre prikker står for polynomier, hvis grad i X_1 er mindre end henholdsvis d og e. Efter eventuel ombytning af F med G kan det antages, at $d \geq e$. Sæt nu først $F := gF$ og $i := i - i_o(g.G)$. Sæt dernæst $F := F - fX_1^{d-e}G$, og fortsæt med **A1**.

[Hvorfor stopper algoritmen? Hvorfor indeholder i den søgte snitmultiplicitet når algoritmen stopper?]

(7.9) Definition. Betragt to plane kurver C og D definerede ved polynomier F og G. Lad c og d være graderne af C og D, og lad F_c og G_d være de homogene led af højeste grad i de to polynomier. I det følgende vil vi sige, at C og D har *endelig skæring*, hvis polynomierne F_c og G_d er primiske.

Uden at vi her kan komme nærmere ind på den såkaldte projektive geometri skal det bemærkes, at de irreducible divisorer i højestegradsleddet F_c svarer til såkaldte „uendeligt fjerne" punkter på kurven C. Forudsætningen om endelig skæring betyder altså at de to kurver C og D ikke har fælles uendeligt fjerne punkter.

(7.10) Observation. Det er klart at endelig skæring medfører at polynomierne F og G er primiske, altså at snittet $C \cap D$ er et endeligt skema, jfr Sætning (7.4).

(7.11) Bezout's Sætning. *Lad C og D være plane kurver således at snittet $C \cap D$ er endeligt. Da gælder uligheden,*

$$\sum_{p \in C \cap D} |p : k| \cdot i_p(C.D) \leq (\deg C)(\deg D),$$

og denne ulighed er en lighed, hvis og kun hvis C og D skærer endeligt.

Bevis. Da $C \cap D$ ifølge forudsætningen er et endeligt skema, er snitmultipliciteten $i_p(C.D)$ lig med multipliciteten $\mathrm{mult}_p(C \cap D)$. Af Korollar (5.3) følger derfor, at ulighedens venstreside er lig med dimensionen af $\Gamma(C \cap D)$. Det skal således vises, at denne dimension er mindre eller lig med cd, og at lighed gælder, hvis og kun hvis højestegradsleddene F_c og G_d er primiske. Koordinatringen $\Gamma(C \cap D)$ er kvotienten $k[X_1, X_2]/(F, G)$, hvor F og G er polynomierne, der definerer C og D. Det fremgår derfor umiddelbart af det følgende Lemma, at den påståede lighed gælder hvis de homogene højestegradsled F_c og G_d er primiske. Uligheden og „kun hvis" kan indses ved en udbygning af Lemma'et. Det overlades til læseren. ∎

(7.12) Lemma. *Sæt $\Gamma := k[X_1, X_2]$, og lad $\Gamma_{\leq h}$ og Γ_h betegne underrummene i Γ bestående af polynomier, der er henholdsvis af grad mindre eller lig med h, og homogene af grad h. Lad F og G være polynomier af grad c og d således at de homogene højestegradsled F_c og G_d er primiske. Da gælder følgende ligninger:*

$$(F, G) \cap \Gamma_{\leq h} = \Gamma_{\leq h-c} F + \Gamma_{\leq h-d} G \text{ for alle } h, \text{ og} \tag{7.12.1}$$

$$= \Gamma_{\leq h-c} F \oplus \Gamma_{\leq h-d} G \text{ for } h < c + d, \tag{7.12.2}$$

$$\Gamma_{c+d-1} = \Gamma_{d-1} F_c \oplus \Gamma_{c-1} G_d, \tag{7.12.3}$$

$$\Gamma_h = \Gamma_{h-c} F_c + \Gamma_{h-d} G_d \text{ for } h \geq c + d - 1, \tag{7.12.4}$$

$$\Gamma = (F, G) + \Gamma_{\leq h} \text{ for } h \geq c + d - 2. \tag{7.12.5}$$

Endelig gælder, at $\dim_k \Gamma/(F, G) = cd$.

Bevis. Højresiden i (7.12.1) er øjensynlig indeholdt i venstresiden. Lad omvendt P være et polynomium, der tilhører venstresiden. Graden af P er altså højst h, og P har en fremstilling

$$P = AF + BG. \tag{$*$}$$

Det er nok at vise, at polynomierne A og B i en sådan fremstilling kan vælges således at A har grad højst $h-c$. Er dette nemlig opfyldt, så har AF højst grad h, og $BG = P - AF$ har derfor grad højst h; følgelig har B højst grad $h-d$, og så viser fremstillingen, at P tilhører højresiden af (7.12.1). Vælg nu fremstillingen $(*)$ således at A har mindst mulig grad a. Det er skal altså vises, at $a \leq h-c$. Antag, indirekte, at $a > h-c$. Produktet AF har da grad større end h, og h er større end eller lig med graden af P. Af $(*)$ følger derfor, at AF og BG har samme grad (større end h), og at der for de homogene højestegradsled gælder, at $0 = A_a F_c + B_b G_d$ (hvor $a+c = b+d$). Da F_c og G_d ifølge forudsætningerne er primiske medfører ligningen, at der findes et homogent polynomium K således at $A_a = KG_d$ og $B_b = -KF_c$. Af $(*)$ fås en ny fremstilling,

$$P = (A - KG)F + (B + KF)G,$$

og ifølge valget af K har differensen $A - KG$ en grad, der er mindre end graden af A. Hermed er den ønskede modstrid nået, idet fremstillingen $(*)$ var valgt således at graden af A var mindst mulig.

Ligningen (7.12.2) udsiger, at summen på højresiden af (7.12.1) er direkte, når $h < c+d$. Det er nok at vise, at de to underrum på højresiden kun har nul-polynomiet fælles. Et polynomium P i fællesmængden er deleligt med både F og G. Det følger af forudsætningerne, at F og G er primiske, og P er derfor deleligt med produktet FG. Hvis $P \neq 0$, er graden derfor specielt større end eller lig med $c+d$. På den anden side er graden af P højst lig med h, og $h < c+d$. Altså er $P = 0$, som påstået.

Betragt videre (7.12.3). Øjensynlig er de to underrum på højresiden indeholdt i venstresiden. Da F_c og G_d er primiske, følger det ganske som i beviset for (7.12.2), at de to underrum danner direkte sum. Det er derfor nok at vise, at de to sider har samme endelige dimension over k. Dette følger ved en simpel addition, idet underrummet Γ_h øjensynlig har dimension $h+1$.

For at vise ligningerne (7.12.4) er det nok at vise at hvert monomium $M = X_1^i X_2^j$, hvor $i+j = h \geq c+d-1$, tilhører højresiden. Et sådan monomium kan øjensynlig skrives som et produkt $M = M_1 M_2$ af et monomium M_1 af grad $h-(c+d-1)$ og et monomium M_2 af grad $c+d-1$. Af (7.12.3) følger, at M_2 har en fremstilling $M_2 = AF_c + BG_d$, hvor A og B er homogene polynomier af grad $d-1$ og $c-1$. Ved at multiplicere denne fremstilling med M_1 fås den ønskede fremstilling af M.

For endelig at eftervise (7.12.5) skal det vises, at hvert polynomium P modulo (F,G) er kongruent med et polynomium af grad højst h. Dette vises ved induktion efter graden l af polynomiet P. Hvis $l \leq h$ er polynomiet selv af grad højst h. Hvis $l > h$, så er specielt $l \geq c+d-1$. Det homogene højestegradsled P_l kan derfor ifølge (7.12.4) skrives på formen $P_l = AF_c + BG_d$, hvor A og B er homogene polynomier af grad $l-c$ og $l-d$. Modulo (F,G) er P kongruent med differensen $P - (AF + BG)$. Differensen har ifølge konstruktionen grad mindre end l, så ifølge induktionsantagelsen er differensen kongruent med et polynomium af grad højst h. Følgelig er P kongruent med et polynomium af grad højst h. Hermed er (7.12.5) bevist.

Den afsluttende formel for dimensionen er en konsekvens af ligningerne (7.12.2) og (7.12.5). Vælg en værdi af h for hvilke begge ligninger er opfyldt. Der er to muligheder, $h = c + d - 1$ og $h = c + d - 2$. Af (7.12.5) følger, at $\Gamma = (F, G) + \Gamma_{\leq h}$. Isomorfien i Noether's første Isomorfisætning er altså en isomorfi,

$$\Gamma/(F, G) \simeq \Gamma_{\leq h}/\big((F, G) \cap \Gamma_{\leq h}\big).$$

På højresiden er tælleren og nævneren endeligdimensionale over k. Tællerens dimension er lig med antallet af monomier $X_1^i X_2^j$ med $i + j \leq h$, og altså lig med $(h+1)(h+2)/2$. Nævnerens dimension kan beregnes af den direkte sum fremstilling i (7.12.2). Differensen af dimensionerne er dimensionen af kvotienten. Som resultat fås ligningerne,

$$\dim_k \Gamma/(F, G) = \binom{h+2}{2} - \binom{h-c+2}{2} - \binom{h-d+2}{2} = cd,$$

idet det sidste lighedstegn fås ved en simpel udregning når h har en af de to valgte værdier. Dette resultat er det ønskede. Hermed er Lemmaets påstande bevist. ∎

(7.13) Bemærkning. Bezout's Sætning udsiger, at kurver af grad c og d, under passende forudsætninger, skærer hinanden i cd punkter, talt med multiplicitet. Hvis legemet k ikke er algebraisk afsluttet kan nogen af skæringspunkterne naturligvis være ikke-rationale punkter, og graden af disse punkter skal så medregnes i multipliciteten.

For små værdier af c og d er det ofte muligt at sige noget yderligere om multiplicitet og grad af punkterne i $C \cap D$.

(7.14) Eksempel. Betragt to linier L_1 og L_2, definerede ved førstegradspolynomier. De to polynomier er primiske, netop når de ikke er proportionale. Ifølge Sætning (7.4) er snittet $L_1 \cap L_2$ derfor endeligt, netop når L_1 og L_2 er forskellige. Bemærk, at betingelsen om endelig skæring er at de to linier ikke er parallelle. Bezout's Sætning udsiger her, at snittet i dette tilfælde består af ét punkt, som endda må være et rationalt punkt. Men det er jo ingen overraskelse.

(7.15) Eksempel. Betragt dernæst en kurve C af grad n og en linie L, definerede ved et n-tegradspolynomium F og et førstegradspolynomium $a_1X_1+a_2X_2+b$. Snittet $C \cap L$ er da endeligt, netop hvis F ikke er delelig med $a_1X_1 + a_2X_2 + b$. Betingelsen om endelig skæring er her, at F_n ikke er delelig med $a_1X_1 + a_2X_2$. Bezout's Sætning udsiger, at snittet i dette tilfælde består af n punkter, talt med multiplicitet. Hvis p er et rationalt punkt på $C \cap L$, så følger det af Sætning (7.5), at p bidrager med multiplicitet 1, hvis og kun hvis C er glat i p og linien L ikke er tangenten; i alle andre tilfælde bidrager p med en multiplicitet større end 1.

Antag for eksempel, at $n = 2$, altså at C er et keglesnit. Her kan tallet 2, for punkterne i $C \cap L$ talt med multiplicitet, fremkomme på flere måder: Skæringen kan bestå af 2 rationale punkter; i hvert af disse må C være glat, og L er forskellig fra tangenten. Videre kan skæringen bestå af ét rationalt punkt p, hvori $i_p(C.L) = 2$;

det er tilfældet, hvis C er glat i p og L er tangenten, eller hvis p er et multipelt punkt på C, jfr Eksempel (6.10). Endelig kan skæringen bestå af ét ikke-rationalt punkt p, hvori nødvendigvis graden $|p:k|$ er lig med 2.

(7.16) Eksempel. Som fortsættelse af det foregående eksempel betragtes tilfældet, hvor C er den kubiske kurve defineret ved polynomiet $F = X_2^2 - f(X_1)$ i Eksempel (6.11). Det homogene højestegradsled i F er en konstant gange X_1^3. Skæringen $C \cap L$ er altså endelig, netop når $a_2 \neq 0$, dvs netop når linien L ikke er parallel med X_2-aksen. Lad p og q være rationale, glatte punkter på C og lad L være bestemt som linien gennem p og q, hvis p og q er forskellige, og som tangenten i p, hvis $p = q$. Antag, at L ikke er parallel med X_2-aksen, og betragt snittet $C \cap L$. Talt med multiplicitet er der 3 punkter i snittet.

Betragt først tilfældet, hvor $p \neq q$. Begge punkter bidrager med multiplicitet mindst 1 til summen 3. Enten bidrager begge med multiplicitet 1 til summen. I så fald består $C \cap L$ af yderligere ét punkt r, som bidrager med multiplicitet 1. Dette tredie punkt r må specielt være et glat og rationalt punkt på C (og L må være forskellig fra tangenten i r). Eller ét af punkterne bidrager med multiplicitet 2. I dette tilfælde består $C \cap L$ af 2 punkter, hvoraf ét skal tælles dobbelt, og L er tangenten til det „dobbelte“ punkt.

Betragt dernæst tilfældet, hvor $p = q$ og L er tangenten i p. Her bidrager p med $i_p(C.L)$ som mindst er 2. Enten er altså $i_p(C.L) = 3$; i dette tilfælde siges punktet p at være et *flexpunkt* på kurven: Snittet $C \cap L$ består kun af punktet p, som skal tælles med multiplicitet 3. Eller også er $i_p(C.L) = 2$. I dette tilfælde konkluderes, at $C \cap L$ består af yderligere ét punkt r, som bidrager med multiplicitet 1. Dette andet punkt r må specielt være et glat og rationalt punkt på C (og L må være forskellig fra tangenten i punktet r).

(7.17) Note. Lad C være en plan kurve af grad c defineret ved polynomiet F. Hvis C har en multipel komponent, jfr Definition (6.2), så følger det umiddelbart af definitionen, at alle rationale punkter på denne komponent er multiple punkter på C. Antag nu, at C er et integritetsskema, altså at polynomiet F er irreducibelt. Antag yderligere, at legemet k har karakteristik 0. Den sidste antagelse medfører at en af de partielle afledede af F, fx $\partial F/\partial X_1$, er forskellig fra 0. Sæt $F' := \partial F/\partial X_1$. Hvis F' er konstant, så er C glat i hvert af sine rationale punkter ifølge Sætning (6.7). Antag, at F' ikke er konstant, og lad C' være kurven defineret ved F'. Polynomiet F' har højst grad $c-1$, så det er primisk med det irreducible polynomium F. Af Sætning (7.4) følger derfor, at $C \cap C'$ kun har endelig mange punkter. I alle rationale punkter p som ligger på C, men ikke på C', er den partielle afledede F' forskellig fra 0. Følgelig er C glat i disse punkter. Specielt er der således kun endelig mange rationale punkter hvori C ikke er glat.

Mere præcist følger det af Bezout's Sætning, at snittet $C \cap C'$ højst indeholder $c(c-1)$ punkter talt med multiplicitet. Hvert rationalt punkt p, hvori C ikke er glat, tilhører snittet $C \cap C'$, og det bidrager med multiplicitet mindst 2. Følgelig gælder, at antallet af rationale, multiple punkter på C højst er $c(c-1)/2$.

8. Max Noether's Sætning.

(8.1) Definition. Ved en (punkt-)*cykel* i $\mathbf{A}^2$ forstås en formel, endelig heltalslinearkombination af punkter i $\mathbf{A}^2$. En cykel $\mathfrak{c}$ kan altså skrives på formen

$$\mathfrak{c} = \sum n_j p_j,$$

hvor p_j'erne er endelig mange forskellige punkter i $\mathbf{A}^2$ og n_j'erne er hele tal. Tallet n_j er cyklens koefficient i punktet p_j, og det betegnes $i_{p_j}(\mathfrak{c})$. Det er ikke udelukket, at nogle af n_j'erne kan være lig med 0, og det er faktisk bekvemt at sætte $i_p(\mathfrak{c}) := 0$ for hvert punkt p, der ikke er et af p_j'erne. Herved kan cyklen skrives

$$\mathfrak{c} = \sum_p i_p(\mathfrak{c})\, p\,,$$

hvor altså kun endelig mange af koefficienterne i_p er forskellige fra 0. Ved *graden af cyklen* forstås tallet

$$\deg \mathfrak{c} := \sum_p |p : k| \cdot i_p(\mathfrak{c}).$$

Graden er altså summen af koefficienterne, idet hvert punkt p vægtes med sin grad.

Cyklerne i $\mathbf{A}^2$ udgør, med en oplagt definition af addition, en kommutativ gruppe. Endvidere kan cyklerne ordnes partielt: Er $\mathfrak{c}'$ endnu en cykel skrives

$$\mathfrak{c} \prec \mathfrak{c}',$$

hvis der for alle punkter p gælder $i_p(\mathfrak{c}) \le i_p(\mathfrak{c}')$, og for mindst ét punkt gælder den skarpe ulighed.

Lad C og D være to plane kurver således at snittet $C \cap D$ er endeligt. Da defineres *snitcyklen* $C.D$ ved formlen,

$$C.D = \sum_{p \in C \cap D} \mathrm{mult}_p(C \cap D)\, p\,.$$

Snitcyklens koefficienter er med andre ord snitmultipliciteterne. Ifølge definitionen er graden af snitcyklen bestemt ved

$$\deg(C.D) = \sum_{p \in C \cap D} |p : k| \cdot i_p(C.D).$$

Bezout's Sætning udsiger med andre ord, at graden af snitcyklen er mindre end eller lig med produktet af kurvernes grader, og at lighed gælder, hvis skæringen er endelig.

(8.2) Max Noether's Sætning. *Lad C, D og E være plane kurver således at både D og E skærer C endeligt. Antag videre, at $C.D \prec C.E$. Antag endelig, at kurven C er glat i hvert punkt af $C \cap D$. Da findes en plan kurve E', som skærer C endeligt i differenscyklen $C.E - C.D$, dvs således at*

$$C.E' = C.E - C.D\,.$$

Bevis. Lad F, G og H være polynomier, som definerer kurverne C, D og E, og lad c, d og e betegne graderne. At $C.D \prec C.E$ betyder, at der for hvert punkt p på $C \cap D$ for snitmultipliciteterne gælder uligheden,

$$i_p(C.D) \leq i_p(C.E).$$

Snitmultipliciteten $i_p(C.D)$ er ifølge definitionen lig med længden af den lokale ring $\mathcal{O}_{C\cap D,p}$. Som nævnt i Observation (7.3) er denne lokale ring kvotienten $\mathcal{O}_{C,p}/G\mathcal{O}_{C,p}$. Længden af denne kvotient er altså ulighedens venstreside. Ulighedens højreside er tilsvarende længden af kvotienten $\mathcal{O}_{C,p}/H\mathcal{O}_{C,p}$. Det følger således af forudsætningerne, at der for alle punkter p i $C \cap D$ gælder uligheden,

$$\operatorname{long} \mathcal{O}_{C,p}/G\mathcal{O}_{C,p} \leq \operatorname{long} \mathcal{O}_{C,p}/H\mathcal{O}_{C,p}.$$

Uligheden medfører, at der for alle p i $C\cap D$ gælder følgende inklusion mellem idealer:

$$H\mathcal{O}_{C,p} \subseteq G\mathcal{O}_{C,p}.$$

Af forudsætningerne følger nemlig at ringen $\mathcal{O}_{C,p}$ er en valuationsring, så dens idealer er totalt ordnede. Følgelig vil uligheden mellem længderne af kvotienterne medføre den ønskede inklusion mellem idealerne.

Inklusionen mellem idealerne betyder, at billedet af H i kvotienten $\mathcal{O}_{C,p}/G\mathcal{O}_{C,p}$ er lig med 0 for alle punkter p i $C \cap D$. Denne kvotient er netop den lokale ring $\mathcal{O}_{C\cap D,p}$. Billedet af H i den lokale ring $\mathcal{O}_{C\cap D,p}$ er altså lig med 0 for alle punkter p i $C \cap D$. Ifølge Sætning (5.1) følger heraf, at H tilhører idealet $\mathcal{I}(C \cap D)$. Med andre ord er $H \in (F, G)$.

Polynomiet H har grad e. Da $H \in (F, G)$ følger det derfor af (7.12.1), at H kan skrives på formen

$$H = AF + BG, \qquad (*)$$

hvor graden af A er højst $e - c$ og graden af B er højst $e - d$. Bemærk, at differensen $e - d$ er positiv. Den forudsatte relation mellem snitcyklerne medfører nemlig den skarpe ulighed mellem deres grader, og graderne er ifølge Bezout's sætning cd og ce.

Videre bemærkes, at B har grad $e-d$. Ellers ville graden af B nemlig være mindre end $e - d$ og sammenligning af de homogene led af grad e på de to sider af $(*)$ ville give ligningen $H_e = A_{e-c}F_c$, som er i modstrid med at E og C har endelig skæring. Altså er B af grad $e - d$.

Lad E' være kurven bestemt ved polynomiet B. Det påstås, at E' opfylder de stillede krav. Sammenligning af de homogene led af grad e på de to sider af $(*)$ giver ligningen,

$$H_e = A_{e-c}F_c + B_{e-d}G_d.$$

Af denne ligning følger, at højestegradsleddene F_c og B_{e-d} er primiske, idet en fælles primdivisor også ville være fælles primdivisor for F_c og H_e, i modstrid med at C og E skærer endeligt. Følgelig skærer C og E' endeligt. Den anførte ligning mellem snitcyklerne udsiger, at der for alle punkter p gælder ligningen,

$$i_p(F.H) = i_p(F.G) + i_p(F.B).$$

Denne sidste ligning følger af $(*)$ under brug af egenskaberne (2) og (3) i Hovedsætning (7.7).

Hermed er vist, at kurven E' opfylder de anførte krav. ∎

(8.3) Korollar (Pascal's Sætning). *Betragt en sekskant indskrevet i et keglesnit D, dvs en følge af* 6 *(forskellige) rationale punkter $p_1, \ldots, p_6$ på D. Antag, at D er glat i hvert af de* 6 *punkter; hvis D består af* 2 *linier, antages yderligere at punkterne ligger skiftevis på de to linier. Antag endelig for hvert af de tre par af modstående sider i sekskanten, at de to sider skærer hinanden. Da ligger de tre skæringspunkter for de modstående par af sider på en ret linie.*

Bevis. Sekskantens 6 sider er linierne gennem p_i og p_{i+1} for $i = 1, \ldots, 6$ (her sættes $p_7 := p_1$). Siderne benævnes i rækkefølgen svarende til punkterne: C_1, E_3, C_2, E_1, C_3, E_2. Gennem hvert punkt p_i går én C-linie og én E-linie. De tre par af modstående sider er linierne C_j, E_j for $j = 1, 2, 3$. Ifølge forudsætningen skærer C_j og E_j hinanden. Lad q_j være skæringspunktet, for $j = 1, 2, 3$. Det er Sætningens påstand, at de 3 punkter q_j ligger på en ret linie.

Lad hertil C være kurven, hvis komponenter er de tre linier C_1, C_2 og C_3. Polynomiet for C er altså produktet af tre førstegradspolynomier, og specielt har C grad 3. Kurven C er altså glat i alle punkter, som ikke er skæringspunkter mellem C_j'erne. Specielt ligger de 6 punkter p_i på C, og C er glat i disse punkter. Lad tilsvarende E betegne trediegradskurven, hvis komponenter er E_i'erne.

Snittet $C \cap E$ indeholder ifølge Besout's Sætning 9 punkter, talt med multiplicitet. Blandt disse 9 punkter er de 6 punkter p_i. Hertil kommer de 3 skæringspunkter q_j, altså ialt 9 skæringspunkter. Snitcyklen $C.D$ er derfor disse 9 punkter, hvert talt med multiplicitet 1. Af disse 9 punkter udgør de 6 punkter p_i snitcyklen $C.D$. Differenscyklen $C.E - C.D$ består derfor af de tre punkter q_j. Af Max Noethers Sætning følger, at disse tre punkter ligger på en kurve E' af grad $3 - 2 = 1$, dvs på en linie.

Hermed er Pascal's Sætning bevist. ∎

(8.4) Note. Specialtilfældet, hvor keglesnittet består af 2 rette linier, kaldes også *Pappos' Sætning.*

Det er også muligt at drage konklusioner, hvis et eller flere par af modstående sider er parallelle. Hvis ét par af modstående sider er parallelle, kan man vise at dette par af sider er parallelle med linien gennem de to skæringspunkter for de to resterende par. Og hvis to par af modstående sider er parallelle kan man vise, at også det tredie par af sider er parallelle. Disse konklusioner nås bedst i den såkaldte projektive geometri.

(8.5) Note. Som endnu en anvendelse af Max Noether's Sætning betragtes den såkaldte addition på en kubisk kurve. Lad C være en kubisk kurve, fx som i Eksemplerne (6.11) og (7.16). Vi betragter udelukkende rationale punkter på C. Resultatet i Eksempel (7.16) kan udtrykkes således: Lad p og q være glatte punkter på C og lad L være bestemt som linien gennem p og q, hvis p og q er forskellige, og som tangenten i p, hvis $p = q$. Antag, at L ikke er parallel med X_2-aksen. Da findes netop ét glat punkt r på C, således at

$$C.L = p + q + r. \qquad (*)$$

Punktet r er „det tredie skæringspunkt" på linien gennem p og q. Det kan godt falde sammen med p og/eller q. Vælg nu et vilkårligt fast punkt e blandt de glatte punkter på C. For hvert glat punkt p på C betegnes med p^* det tredie skæringspunkt på linien gennem p og e. Definer nu en komposition i mængden af glatte punkter på følgende måde: lad p og q være glatte punkter. Bestem det tredie skæringspunkt r på linien gennem p og q, og sæt

$$p * q := r^*.$$

Det påstås, at *mængden af glatte punkter på C med denne komposition er en kommutativ gruppe.*

Det er en let følge af definitionen, at kompositionen er kommutativ, at e er neutralt element, og at det inverse til p er det tredie skæringspunkt på linien gennem p og e^*. Den ikke-trivielle påstand er at kompositionen er associativ. Lad hertil p, q og s være tre punkter på C. Betragt punktet $(p * q) * s$. Dette punkt bestemmes ved først at bestemme linien E_1 og punktet r, og dernæst linien E_2 og punktet t så at

$$C.E_1 = p + q + r, \quad C.E_2 = r^* + s + t.$$

Det søgte punkt er da t^*. På den anden side bestemmes punktet $p * (q * s)$ ved først at bestemme linien D_1 og punktet u, og dernæst linien L og punktet v således at

$$C.D_1 = q + s + u, \quad C.L = p + u^* + v.$$

Det søgte punkt er da v^*. Det er påstanden, at $t^* = v^*$, eller, ækvivalent, at $t = v$. Den sidste påstand er igen ækvivalent med at punkterne p, u^* og t ligger på en ret linie (nemlig L).

Hertil bemærkes, at ifølge definitionen ligger punkterne e, r og r^* på en linie D_2 og punkterne e, u og u^* ligger på en linie E_3. De 9 punkter, p q, r, s, r^*,

t, e, u^*, u ligger på linierne E_1, E_2 eller E_3, og de udgør derfor snitcyklen $C.E$, hvor E er trediegradskurven med med komponenter E_j. Af de 9 punkter ligger de 6 punkter q, s, u, e, r^*, r på linierne D_1 eller D_2, og de udgør derfor snitcyklen $C.D$, hvor D er andengradskurven med komponenterne D_1 og D_2. Af Max Noether's Sætning følger derfor, at de resterende punkter, dvs punkterne p, u^* og t, ligger på en førstegradskurve, som påstået.

Det skal afslutningsvis bemærkes, at påstanden (og derfor også beviset) har et væsentligt hul. Det tredie skæringspunkt på linien gennem p og q er jo slet ikke defineret, hvis denne linie er parallel med X_2-aksen. For at udfylde dette hul er det strengt taget nødvendigt at tilføje et uendeligt fjernt skæringspunkt i X_2-aksens retning. Dette hul udfyldes nemmest i den såkaldte projektive plan.

9. Appendix: Koszul-følgen i planen.

(9.1) Notation. I det følgende betegner Γ polynomiumsringen $\Gamma := k[X,Y]$ i to variable over legemet k. Med $\Gamma_{<n}$ betegnes underrummet i Γ bestående af polynomier af grad mindre end n. Videre sættes $\mathfrak{M} := \mathfrak{M}_o$. Maksimalidealet $\mathfrak{M} = (X,Y)$ består altså af de polynomier, der forsvinder i punktet $o = (0,0)$, og potensen $\mathfrak{M}^n$ består af polynomier af orden større end eller lig med n. Endelig betegnes med Γ^n kvotientringen $\Gamma^n := \Gamma/\mathfrak{M}^n$.

Bemærk, at $\Gamma_{<n}$ og $\mathfrak{M}^n$ er komplementære underrum i Γ: polynomierne af grad mindre end n er k-linearkombinationer af monomierne X^iY^j for $i+j<n$ og polynomierne i $\mathfrak{M}^n$ er k-linearkombinationer af monomierne X^iY^j for $i+j \geq n$. Det følger, at den sammensatte homomorfi $\Gamma_{<n} \to \Gamma \to \Gamma^n$ er en isomorfi af vektorrum over k. Specielt har de to vektorrum altså den samme endelige dimension,

$$\dim_k \Gamma_{<n} = \dim_k \Gamma^n = \binom{n+1}{2}. \tag{9.1.1}$$

For $n \leq 0$ er det naturligt at sætte $\Gamma_{<n} = (0)$ og $\mathfrak{M}^n = \Gamma$ (og dermed $\Gamma^n = 0$). Bemærk, at formlen ovenfor for dimensionen også gælder for $n = 0$ og $n = -1$, men ikke for $n < -1$.

(9.2) Definition. I det følgende betragtes i polynomiumsringen Γ to polynomier F og G forskellige fra 0. Svarende hertil betragtes følgen af Γ-lineære afbildninger,

$$0 \to \Gamma \xrightarrow{\alpha} \Gamma \oplus \Gamma \xrightarrow{\beta} \Gamma \xrightarrow{\kappa} \Gamma/(F,G) \to 0, \tag{9.2.1}$$

hvor α er afbildningen $H \mapsto (HG, -HF)$, hvor β er afbildningen $(A,B) \mapsto AF+BG$, og hvor κ er den kanoniske afbildning på kvotienten.

Følgen (9.2.1) kaldes *Koszul-følgen* knyttet til polynomierne F og G.

Lad c og d være graderne af F og G. For hvert n inducerer multiplikation med F da ved restriktion en k-lineær homomorfi $\Gamma_{<n-c} \to \Gamma_{<n}$, og multiplikation med G inducerer en k-lineær homomorfi $\Gamma_{<n-d} \to \Gamma_{<n}$. Koszul-følgen inducerer derfor en følge af k-lineære homomorfier,

$$0 \to \Gamma_{<n-c-d} \xrightarrow{\alpha_n} \Gamma_{<n-c} \oplus \Gamma_{<n-d} \xrightarrow{\beta_n} \Gamma_{<n} \xrightarrow{\kappa_n} \Gamma_{<n}/(F,G)_{<n} \to 0, \qquad (9.2.1_n)$$

hvor $(F,G)_{<n}$ betegner fællesmængden $(F,G) \cap \Gamma_{<n}$.

Betragt tilsvarende ordenerne f og g af polynomierne F og G. Multiplikation med F inducerer ved restriktion en homomorfi $\mathfrak{M}^{n-f} \to \mathfrak{M}^n$, og heraf induceres en homomorfi $\Gamma^{n-f} \to \Gamma^n$ mellem kvotienterne: restklassen modulo $\mathfrak{M}^{n-f}$ af et polynomium P afbildes på restklassen modulo $\mathfrak{M}^n$ af PF. Tilsvarende inducerer multiplikation med G en homomorfi $\Gamma^{n-g} \to \Gamma^n$. Koszul-følgen inducerer derfor en følge,

$$0 \to \Gamma^{n-f-g} \xrightarrow{\alpha^n} \Gamma^{n-f} \oplus \Gamma^{n-g} \xrightarrow{\beta^n} \Gamma^n \xrightarrow{\kappa^n} \Gamma/(\mathfrak{M}^n, F, G) \to 0. \qquad (9.2.1^n)$$

(9.3) Observation. Det er let at se, at Koszul-følgen er en nul-følge. Videre er κ surjektiv, og øjensynlig er $\operatorname{Im}\beta = \operatorname{Ker}\kappa$. Yderligere er α injektiv, når blot F eller G er forskellig fra 0. Endelig er $\operatorname{Im}\alpha = \operatorname{Ker}\beta$, hvis F og G er primiske, thi af $AF + BG = 0$ følger så, at A er et multiplum af G, altså $A = GH$, og ved indsættelse og division med G fås $B = -FH$. Hvis F og G er primiske, er Koszul-følgen altså exakt.

Da Koszul-følgen er en nulfølge, er det umiddelbart at se, at de inducerede følger $(9.2.1_n)$ og $(9.2.1^n)$ er nulfølger. Selv om Koszul-følgen er exakt, vil de inducerede følger imidlertid i almindelighed ikke være exakte.

(9.4) Lemma. *Antag, at polynomierne F og G er primiske, og lad c og d betegne deres grader. Betragt følgen $(9.2.1_n)$ for et fast $n \geq c + d - 1$. Da gælder:*
(1) *Følgen er exakt på nær at der kun gælder $\operatorname{Im}\beta_n \subseteq \operatorname{Ker}\gamma_n$.*
(2) *Følgende ulighed gælder: $\dim_k \Gamma_{<n}/(F,G)_{<n} \leq cd$.*
(3) *Følgende betingelser er ækvivalente:*
  (i) *Følgen er exakt.*
  (ii) $\Gamma_{<n-c}F + \Gamma_{<n-d}G = \Gamma_{<n} \cap (F,G)$.
  (iii) $\dim_k \Gamma_{<n}/(F,G)_{<n} = cd$.
  (iv) *De homogene led F_c og G_d af højeste grad er primiske.*

Bevis. Påstand (1) følger umiddelbart af at Koszul-følgen er exakt. Homomorfien α_n er blot restriktionen af α. Da α er injektiv, er også α_n injektiv. Betragt videre et par (A,B) i $\Gamma_{<n-c} \oplus \Gamma_{<n-d}$ således at $\beta_n(A,B) = 0$. Da Koszul-følgen er exakt, findes et polynomium H således at $(A,B) = (HG, -HF)$. Da $A = HG$ har grad mindre en $n - c$, må H have grad mindre end $n - c - d$. Altså er $H \in \Gamma_{<n-c-d}$, og følgelig er (A,B) element i $\operatorname{Im}\alpha_n$. Endelig er κ_n blot den kanoniske homomorfi på kvotienten, og derfor surjektiv.

For at vise påstanden (2) bemærkes, at vektorrummene i følgen er af endelig dimension over k. Af påstand (1) fås derfor ligningerne,

$$\begin{aligned}\dim \operatorname{Im}\beta_n &= \dim \Gamma_{<n-c} + \dim \Gamma_{<n-d} - \dim \Gamma_{<n-c-d},\\ \dim \operatorname{Ker}\kappa_n &= \dim \Gamma_{<n} - \dim \Gamma_{<n}/(F,G)_{<n},\end{aligned}$$

og videre, at venstresiden i den første ligning er mindre end eller lig med venstresiden i den anden ligning. Af ligningerne og denne sidste ulighed fås,

$$\begin{aligned}\dim \Gamma_{<n}/(F,G)_{<n} &\leq \dim \Gamma_{<n} - \dim \Gamma_{<n-c} - \dim \Gamma_{<n-d} + \dim \Gamma_{<n-c-d}\\ &= \binom{n+1}{2} - \binom{n-c+1}{2} - \binom{n-d+1}{2} + \binom{n-c-d+1}{2}\\ &= cd.\end{aligned}$$

idet den første ligning er observeret i (9.1) (her bruges, at $n \geq c + d - 1$), og den anden ligning følger ved simpel udregning. Hermed er uligheden i påstand (2) eftervist. Yderligere ses det af udledningen, at uligheden er en lighed, hvis og kun hvis $\dim \operatorname{Im}\beta_n = \dim \operatorname{Ker}\kappa_n$, dvs hvis og kun hvis følgen $(9.2.1_n)$ er exakt.

Endelig vises ækvivalensen af betingelserne i påstand (3). Betingelsen (ii) udtrykker blot, at $\operatorname{Im}\beta_n = \operatorname{Ker}\kappa_n$; det fremgår af (1), at denne ligning er ækvivalent med exaktheden i (i), og som det fremgår af beviset for (2) er ligningen også ækvivalent med ligheden i (iii). Betingelserne (i), (ii) og (iii) er altså ækvivalente. Nu vises, at betingelserne (ii) og (iv) er ækvivalente.

Antag først, at (iv) er opfyldt, altså at F_c og G_d er primiske. Det er nok at vise, at højresiden af ligningen i (ii) er indeholdt i venstresiden. Betragt altså et polynomium P af grad mindre end n i idealet (F, G). Da har P en fremstilling,

$$P = AF + BG, \qquad (*)$$

og det skal vises, at P har en sådan fremstilling med A af grad mindre end $n - c$ og B af grad mindre end $n - d$. Betragt hertil en fremstilling $(*)$ af P med polynomiet A af mindst mulig grad. Det er nok at vise, at med dette valg har polynomiet A grad mindre end $n - c$, thi så har $BG = P - AF$ grad mindre end n og følgelig har B grad mindre end $n - d$. Antag, indirekte, at A har en grad a, der mindst er lig med $n - c$. Produktet AF har da mindst grad n, og n er større end graden af P. Af fremstillingen følger derfor, at AF og BG har samme grad (nemlig $a + c \geq n$), og at der for de homogene led af højeste grad gælder, at $0 = A_a F_c + B_b G_d$ (hvor $a + c = b + d$). Da F_c og G_d ifølge forudsætningerne er primiske medfører ligningen, at der findes et homogent polynomium K således at $A_a = KG_d$ og $B_b = -KF_c$. Af $(*)$ fås en ny fremstilling,

$$P = (A - KG)F + (B + KF)G,$$

og ifølge valget af K har differensen $A - KG$ en grad, der er mindre end graden af A. Hermed er den ønskede modstrid nået, idet fremstillingen $(*)$ var valgt således at graden af A var mindst mulig.

Antag omvendt, at polynomierne F_c og G_d ikke er primiske, altså at de har en ikke-triviel fælles divisor K. Da er $F_c = F'K$ og $G_d = G'K$, hvor K er homogen af grad $k > 0$ og F' og G' er homogene af grader $c - k$ og $d - k$. Ifølge forudsætningen er $n \geq c + d - 1$. Tallet $m := n - c - d + k$ er altså større end eller lig med 0. Vælg nu et homogent polynomium M af grad m således at M ikke er et multiplum af K. Betragt polynomiet,

$$Q := MG'F - MF'G.$$

De to produkter på højresiden har samme grad, nemlig $m+(d-k)+c = n$, og samme homogene led af højeste grad, nemlig $MG'F'K$. Differensen Q har derfor grad mindre end n, og da Q øjensynlig tilhører (F, G) vil Q tilhøre højresiden i (ii). Det påstås, at Q ikke tilhører venstresiden. Antag, indirekte, at Q tilhører venstresiden i (ii), altså at Q har en fremstilling,

$$Q = AF + BG,$$

hvor A har grad mindre end $n - c$ og B har grad mindre end $n - d$. Ved subtraktion fås ligningen,

$$(MG' - A)F = (B + MF')G.$$

Da F og G ifølge forudsætningen er primiske, viser ligningen, at $B + MF'$ er et multiplum af F. Specielt er højestegradsleddet i $B + MF'$ et multiplum af F_c. Polynomiet B har grad mindre en $n - d$ og produktet MF' er homogent af grad lig med $m + (c - k) = n - d$. Højestegradsleddet er altså MF', og dette polynomium er altså et multiplum af $F_c = KF'$. Ved division sluttes, at M er et multiplum af K, i modstrid med valget af M. Hermed er den ønskede modstrid opnået, og det er således vist, at Q tilhører højresiden i (ii) og ikke venstresiden.

Hermed er også ækvivalensen af (ii) og (iv) vist, hvormed beviset for Lemmaet er fuldført. ∎

(9.5) Sætning. *Antag, at polynomierne F og G er primiske, og lad c og d betegne deres grader. Da gælder uligheden,*

$$\dim_k \Gamma/(F,G) \leq (\deg F)(\deg G),$$

og lighed gælder, hvis og kun hvis de homogene led F_c og G_d af højeste grad er primiske. Hvis de to homogene led er primiske, så gælder yderligere, at homomorfien,

$$\Gamma_{<c+d-1} \to \Gamma/(F,G),$$

er surjektiv.

Bevis. Betragt homomorfien $\Gamma_{<n} \to \Gamma/(F,G)$ for $n \geq c+d-1$. Billedet er et underrum i kvotienten $\Gamma/(F,G)$, og øjensynlig er kvotienten den voksende foreningsmængde (for n gående mod uendelig) af disse billeder. Homomorfiens kerne er $(F,G)_{<n}$, så billedet er kvotienten $\Gamma_{<n}/(F,G)_{<n}$. Det følger derfor af Lemma (9.4)(ii), at hvert af billederne er af endelig dimension, begrænset opad af cd. Heraf sluttes, at når $n \gg 0$, så er billedet hele kvotienten $\Gamma/(F,G)$. Følgelig gælder ulighederne,

$$\dim \Gamma_{<n}/(F,G)_{<n} \;\leq\; \dim \Gamma/(F,G) \;\leq\; cd\,, \tag{9.5.1}$$

og i den første ulighed gælder lighed, når $n \gg 0$. Sætningens påstande er nu en konsekvens af Lemma (9.4). Den påståede ulighed er nemlig vist ovenfor. Hvis F_c og G_d er primiske, så følger det af Lemma (9.4), anvendt på en vilkårlig værdi $n \geq c+d-1$, at begge uligheder i (9.5.1) må være ligheder; den anden lighed er den påståede lighed, og for $n = c+d-1$ viser den første lighed, at $\Gamma_{<c+d-1} \to \Gamma/(F;G)$ er surjektiv. Antag omvendt ligheden $\dim \Gamma/(F,G) = cd$. For $n \gg 0$ er så begge uligheder i (9.5.1) ligheder. Af Lemma (9.4) følger derfor, at F_c og G_d er primiske. ∎

(9.6) Lemma. *Antag, at polynomierne F og G er primiske, og lad f og g betegne deres ordener. Betragt følgen $(9.2.1^n)$ for et fast $n \geq f+g-1$. Da gælder:*

(1) *Følgen er exakt på nær at der kun gælder* $\operatorname{Im}\alpha^n \subseteq \operatorname{Ker}\beta^n$.
(2) *Følgende ulighed gælder:* $\dim_k \Gamma/(\mathfrak{M}^n, F, G) \geq fg$.
(3) *Følgende betingelser er ækvivalente:*
   (i) *Følgen er exakt.*
   (ii) $\mathfrak{M}^{n-f}F + \mathfrak{M}^{n-g}G = \mathfrak{M}^n \cap (F,G)$.
   (iii) $\dim_k \Gamma^n/(F,G)^n = fg$.
   (iv) *De homogene led F_f og G_g af laveste grad er primiske.*

Bevis. Påstand (1) om exakthed indses således: Homomorfien α^n er injektiv. Ved α^n afbildes nemlig klassen af H modulo $\mathfrak{M}^{n-f-g}$ på parret bestående af HG modulo $\mathfrak{M}^{n-f}$ og $-HF$ modulo $\mathfrak{M}^{n-g}$. Hvis klassen repræsenteret af HG er 0, er HG af orden mindst $n-f$, og følgelig er H af orden mindst $n-f-g$; altså repræsenterer H nul-elementet i Γ^{n-f-g}. Videre er $\operatorname{Im}\beta^n = \operatorname{Ker}\kappa^n$. Betragt nemlig i Γ^n en klasse i $\operatorname{Ker}\kappa^n$, og lad P være en repræsentant for klassen. Modulo $\mathfrak{M}^n$ er P da af formen $P = AF + BG$. Polynomierne A og B repræsenterer et par i $\Gamma^{n-f} \oplus \Gamma^{n-g}$, som ved β^n afbildes på den givne klasse repræsenteret af P. Endelig er κ^n øjensynlig surjektiv.

For at vise påstanden (2) bemærkes, at vektorrummene i følgen er af endelig dimension over k. Af påstand (1) fås derfor ligningerne,

$$\begin{aligned}\dim\operatorname{Im}\alpha^n &= \dim\Gamma^{n-f-g},\\ \dim\operatorname{Ker}\beta^n &= \dim\Gamma^{n-f} + \dim\Gamma^{n-g} - \dim\Gamma^n + \dim\Gamma/(\mathfrak{M}^n, F, G),\end{aligned}$$

og videre, at venstresiden i den første ligning er mindre end eller lig med venstresiden i den anden ligning. Af ligningerne og denne sidste ulighed fås, at

$$\begin{aligned}\dim\Gamma/(\mathfrak{M}^n, F, G)^n &\geq \dim\Gamma^n - \dim\Gamma^{n-f} - \dim\Gamma^{n-g} + \dim\Gamma^{n-f-g}\\ &= \binom{n+1}{2} - \binom{n-f+1}{2} - \binom{n-g+1}{2} + \binom{n-f-g+1}{2}\\ &= fg,\end{aligned}$$

idet den første ligning er observeret i (9.1) (her bruges, at $n \geq f+g-1$), og den anden ligning følger ved simpel udregning. Hermed er uligheden i påstand (2) eftervist. Yderligere ses det af udledningen, at uligheden er en lighed, hvis og kun hvis $\dim\operatorname{Im}\alpha^n = \dim\operatorname{Ker}\beta^n$, dvs hvis og kun hvis følgen $(9.2.1^n)$ er exakt.

Endelig vises ækvivalensen af betingelserne i (3). Af påstand (1) fremgår, at betingelsen (i) er opfyldt, hvis og kun hvis $\operatorname{Im}\alpha^n = \operatorname{Ker}\beta^n$. Af beviset for påstand (2) fremgår derfor, at (i) og (iii) er ækvivalente. Det følger videre, at ækvivalensen af (i) og (ii) kan udtrykkes således: Ligheden $\operatorname{Im}\alpha^n = \operatorname{Ker}\beta^n$ gælder, hvis og kun hvis homomorfien $\mu\colon \mathfrak{M}^{n-f} \oplus \mathfrak{M}^{n-g} \to \mathfrak{M}^n \cap (F, G)$ er surjektiv. For at vise ækvivalensen af (i) og (ii) betragtes derfor følgende kommutative diagram,

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathfrak{M}^{n-f} \oplus \mathfrak{M}^{n-g} & \longrightarrow & \Gamma \oplus \Gamma & \longrightarrow & \Gamma^{n-f} \oplus \Gamma^{n-g} & \longrightarrow & 0\\
 & & \downarrow{\scriptstyle \mu} & & \downarrow{\scriptstyle \nu} & & \downarrow{\scriptstyle \beta^n} & & \\
0 & \longrightarrow & \mathfrak{M}^n \cap (F, G) & \longrightarrow & (F, G) & \longrightarrow & \Gamma^n, & &
\end{array}$$

hvor de lodrette homomorfier er induceret af $(A, B) \mapsto AF + BG$. Diagrammets rækker er øjensynligt exakte, og homomorfien μ er surjektiv. Af Slangelemmaet fås en exakt følge mellem kerner og kokerner,

$$0 \to \operatorname{Ker}\mu \to \operatorname{Ker}\nu \to \operatorname{Ker}\beta^n \to \operatorname{Coker}\mu \to 0.$$

Da Koszul-følgen er exakt, er $\operatorname{Ker}\nu = \Gamma$, og heraf følger let, at $\operatorname{Ker}\mu = \mathfrak{M}^{n-f-g}$. Homomorfien $\operatorname{Ker}\mu \to \operatorname{Ker}\nu$ er blot inklusionen $\mathfrak{M}^{n-f-g} \to \Gamma$, der har kokernen Γ^{n-f-g}. Det er nu klart, at den exakte følge ovenfor svarer til en exakt følge,

$$0 \to \operatorname{Im}\alpha^n \to \operatorname{Ker}\beta^n \to \operatorname{Coker}\mu \to 0.$$

Heraf aflæses, at $\operatorname{Im}\alpha^n = \operatorname{Ker}\beta^n$, hvis og kun hvis homomorfien ν er surjektiv. Hermed er ækvivalensen af (i) og (ii) bevist.

Den manglende ækvivalens af (ii) og (iv) kan nu bevises helt analogt med beviset for den tilsvarende ækvivalens i Lemma (9.4).

Hermed er Lemmaets påstande godtgjort. ∎

(9.7) Sætning. *Antag, at polynomierne F og G er primiske, og lad f og g betegne deres ordener. Lad $\mathcal{O}$ betegne den lokale ring, der fremkommer ved lokalisering af Γ i maksimalidealet $\mathfrak{M}$. Da gælder uligheden,*

$$\dim_k \mathcal{O}/(F,G)\mathcal{O} \geq (\operatorname{mult}_o F)(\operatorname{mult}_o G),$$

og lighed gælder, hvis og kun hvis de homogene led F_f og G_g af laveste grad er primiske. Hvis de to homogene led er primiske, så gælder yderligere, at

$$\mathfrak{M}^{f+g-1} \subseteq (F,G)\mathcal{O}.$$

Bevis. Påstanden er triviel, hvis f eller g er lig med 0, dvs hvis et af polynomierne F og G ikke tilhører $\mathfrak{M}$. I så fald er nemlig et af polynomierne invertibelt i den lokale ring $\mathcal{O}$, og idealet $(F,G)\mathcal{O}$ er derfor hele ringen $\mathcal{O}$. Det kan derfor antages, at F og G tilhører $\mathfrak{M}$.

Betragt kvotientringene $\overline{\Gamma} := \Gamma/(F,G)$ og $\overline{\mathcal{O}} := \mathcal{O}/(F,G)\mathcal{O}$. Da $(F,G) \subseteq \mathfrak{M}$, svarer $\mathfrak{M}$ ifølge Kvotientprincippet til et maksimalideal $\overline{\mathfrak{M}}$ i $\overline{G}$, og kvotienten $\overline{\mathcal{O}}$ er den lokale ring der fremkommer ved lokalisering af $\overline{\Gamma}$ i maksimalidealet $\overline{\mathfrak{M}}$. Lad $\mathfrak{m}$ betegne maksimalidealet i den lokale ring $\overline{\mathcal{O}}$. Det er da velkendt, at kvotienten $\overline{\mathcal{O}}/\mathfrak{m}^n$ er isomorf med kvotienten $\overline{\Gamma}/\overline{\mathfrak{M}}^n$. Den sidste kvotient er ifølge Noether's anden Isomorfisætning isomorf med $\Gamma/(\mathfrak{M}^n, F, G)$. Der findes altså kanoniske isomorfier,

$$\Gamma/(\mathfrak{M}^n,F,G) \xrightarrow{\sim} \overline{\mathcal{O}}/\mathfrak{m}^n \xrightarrow{\sim} \mathcal{O}/(\mathfrak{M}^n,F,G)\mathcal{O}.$$

For alle $n \geq f+g-1$ gælder derfor ulighederne,

$$\dim \mathcal{O}/(F,G) = \dim \overline{\mathcal{O}} \geq \dim \overline{\mathcal{O}}/\mathfrak{m}^n = \dim \Gamma/(\mathfrak{M}^n,F,G) \geq fg, \tag{9.7.1}$$

idet den sidste ulighed følger af Lemma (9.6).

Dimensionen af kvotienten $\overline{\mathcal{O}}/\mathfrak{m}^n$ vokser med n. Det andet lighedstegn ovenfor viser, at dimensionen altid er begrænset opad af $\dim \Gamma/(F,G)$ (som er endelig ifølge Sætning (9.4)). For $n \gg 0$ er $\dim \overline{\mathcal{O}}/\mathfrak{m}^n$ altså konstant. Det påstås, at for disse

værdier af n er $\mathfrak{m}^n = (0)$. Af ligningen $\dim \overline{\mathcal{O}}/\mathfrak{m}^n = \dim \overline{\mathcal{O}}/\mathfrak{m}^{n+1}$ følger nemlig, at $\mathfrak{m}^n = \mathfrak{m}^{n+1}$, og af Nakayama's Lemma (anvendt på $\mathfrak{m}^n$ som modul over den lokale ring $\overline{\mathcal{O}}$) konkluderes, at $\mathfrak{m}^n = (0)$. Det fremgår derfor, at den første af de to uligheder ovenfor er en lighed, når $n \gg 0$.

Sætningens påstande er nu en konsekvens af Lemma (9.6). Den anførte ulighed er nemlig vist ovenfor. Hvis F_f og G_g er primiske, så følger det af Lemma (9.6), anvendt på en vilkårlig værdi $n \geq f+g-1$, at den anden ulighed i (9.7.1) må være en lighed; da den første ulighed er en lighed når $n \gg 0$, følger det, at begge uligheder må være ligheder for alle $n \geq f+g-1$. Specielt viser den første lighed for $n = f+g-1$, at $\mathfrak{M}^{f+g-1} \subseteq (F,G)\mathcal{O}$. Antag omvendt ligheden $\dim \overline{\mathcal{O}}/(F,G)\mathcal{O} = fg$. Det følger da specielt, at den sidste ulighed i (9.7.1) er en lighed. Af Lemma (9.6) følger derfor, at F_f og G_g er primiske. ∎

I. Index.

RM=Ringe og moduler, *E*=Endelighed, *N*=Noether, *AG*=Algebraisk geometri. Numrene refererer til afsnit, ikke til sidetal.