Kommutativ algebra II, 2005

Anders Thorup

Matematisk Afdeling
Københavns Universitet

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

Matematisk Afdeling
Universitetsparken 5
2100 København Ø

Indhold

Regulære følger, dybde
Cohen–Macaulay ringe

1. Regulære følger.

(1.1) Setup. I hele kapitlet betegner R en noethersk ring, $\mathfrak{a}$ betegner et ideal i R, og M betegner en endeligt frembragt R-modul. Specielt er M altså noethersk. I denne første paragraf er de noetherske forudsætninger dog ikke væsentlige.

(1.2) Definition. Et element f i R, der ikke er en nuldivisor, siges også at være et *regulært element*. Betingelsen er at multiplikation med f, dvs afbildningen $g \mapsto fg$, er injektiv. Mere generelt siges f at være *regulær* på modulen M, eller at være *M-regulær*, hvis multiplikationen $x \mapsto fx$, for $x \in M$, er en injektiv afbildning.

Ved en *M-regulær følge* forstås en endelig eller uendelig følge af elementer i R således at f_1 er regulær på modulen M og f_i er regulær på $M/(f_1, \dots, f_{i-1})M$ for $i = 2, 3, \dots$. Antallet af elementer i følgen kaldes også følgens *længde*. Den tomme følge kan opfattes som en M-regulær følge af længde 0.

(1.3) Eksempel. Følgen $(X_1, \dots, X_r)$ af variable i en polynomiumsring $R = k[X_1, \dots, X_r]$ er en regulær følge. Kvotienten $R/(X_1, \dots, X_{i-1})$ er nemlig isomorf med $k[X_i, \dots, X_r]$, så X_i er regulær på kvotienten, for $i = 1, \dots, r$.

(1.4) Lemma. *Hvis (f, g) er en M-regulær følge, altså f regulær på M og g regulær på M/fM, så er f regulær på M/gM.*

Hvis $(f_1, \dots, f_r)$ er en M-regulær følge, og g er regulær på $M/(f_1, \dots, f_i)M$ for $i = 1, \dots r$, så er $(f_1, \dots, f_r)$ en M/gM-regulær følge.

Bevis. For at vise den første påstand skal det vises, at hvis en klasse i M/gM ved multiplikation med f føres over i nul-klassen, så er klassen selv nul. Lad x være en repræsentant for klassen, og antag at fx repræsenterer nul-klassen, altså at $fx \in gM$. Der findes altså $y \in M$ således at $fx = gy$. Af denne ligning følger, da g er regulær på M/fM, at $y \in fM$. Altså findes $z \in M$ således at $y = fz$. Ved indsættelse fås $fx = gfz$, og da f er antaget M-regulær, følger det, at $x = gz$. Altså repræsenterer x nul-klassen i M/gM.

Den anden påstand vises ved induktion efter r. For $r = 1$ er det den første påstand. Antag, at $r > 1$. Induktivt følger det så at følgen $(f_1, \dots, f_{r-1})$ er regulær på $M' = M/gM$, så vi mangler at vise, at f_r er regulær på $M'/(f_1, \dots, f_{r-1})M'$. Sæt $M'' := M/(f_1, \dots, f_{r-1})M$. Da gælder øjensynlig,

$$M'/(f_1, \dots, f_{r-1})M' = M''/gM''$$

Ifølge forudsætningerne er f_r regulær på M'' og g er regulær på $M''/f_r M''$. Den manglende påstand fås derfor ved at anvende Lemma'ets første påstand på følgen (f_r, g) og modulen M''. □

(1.5) Bemærkning. Det er klart, at man under forudsætningerne Lemma (1.4) ikke kan slutte, at g er regulær på M, og altså ikke kan slutte, at følgen (g, f) er M-regulær. For eksempel er følgen $(1, 0)$ altid M-regulær, men følgen $(0, 1)$ er kun M-regulær, når $M = 0$. En permutation af en M-regulær følge vil således normalt ikke være M-regulær.

Hvis R er lokal (noethersk), og $(f_1, \dots, f_r)$ er en M-regulær følge i maksimalidealet $\mathfrak{m}$, så vil enhver permutation af følgen igen være M-regulær. Hertil er det nok at vise, jfr Lemma (1.4), at hvis (f, g) er en M-regulær følge i $\mathfrak{m}$, så er g regulær på M. Antag altså, at $x \in M$ og at $gx = 0$. Da g er regulær på M/fM, følger det, at $x \in fM$, altså at der findes $x_1 \in M$ så at $x = fx_1$. Ved indsættelse fås $gfx_1 = 0$, og da f er M-regulær fås $gx_1 = 0$. Af $gx = 0$ følger altså at $x = fx_1$, hvor $gx_1 = 0$. Idet argumentet nu kan anvendes på x_1 osv, fås en følge x_n således at $x_{n-1} = fx_n$ og $gx_n = 0$. Specielt er altså $x = f^n x_n$, og følgelig er $x \in \bigcap f^n M$. Da $f \in \mathfrak{m}$, er x således element i $\bigcap \mathfrak{m}^n M$, og af Krull's Snitsætning følger derfor, at $x = 0$.

Bemærk, at forudsætningen om at R er lokal er væsentlig i det sidste argument. Lad fx R være polynomiumsringen $k[X, Y, Z]$ med koefficienter i et legeme k, og betragt i maksimalidealet (X, Y, Z) polynomierne $f_1 = (1 - Y)X$, $f_2 = Y$, $f_3 = (1 - Y)Z$. Da er (f_1, f_2, f_3) en R-regulær følge, men (f_1, f_3, f_2) er ikke R-regulær.

(1.6) Nøgleresultat. *Lad $\mathbf{f} = (f_1, \dots, f_r)$ og $\mathbf{g} = (g_1, \dots, g_r)$ være to M-regulære følger i idealet $\mathfrak{a}$, af samme endelige længde. Da findes en isomorfi af R-moduler,*

$$\mathrm{Hom}_R(R/\mathfrak{a},\ M/\mathbf{f}M) \simeq \mathrm{Hom}_R(R/\mathfrak{a},\ M/\mathbf{g}M),$$

hvor $\mathrm{Hom}_R(P, Q)$ betegner R-modulen af R-lineære afbildninger fra P til Q.

Vi viser i det følgende, at modulen på venstresiden er isomorf med en modul, der kun afhænger af tallet r og ellers er uafhængig af den regulære følge. Denne modul betegnes $E^r(M)$, og den defineres således: Betragt en fast eksakt følge,

$$\cdots \xrightarrow{\partial_3} R^{d_2} \xrightarrow{\partial_2} R^{d_1} \xrightarrow{\partial_1} R^{d_0} \xrightarrow{\varepsilon} R/\mathfrak{a} \longrightarrow 0. \tag{1.6.1}$$

For at konstruere en såden følge vælges et sæt af d_0 elementer der frembringer $R/\mathfrak{a}$. Lad $\varepsilon\colon R^{d_0} \to R/\mathfrak{a}$ være den tilsvarende surjektive homomorfi, og lad $B_0 \subseteq R^{d_0}$ være homomorfiens kerne (det oplagte valg er naturligvis $d_0 = 1$ (svarende til at $R/\mathfrak{a}$ er frembragt af restklassen af 1), hvorved $B_0 = \mathfrak{a}$; men dette valg er irrelevant for det følgende). Vælg nu et sæt af d_1 frembringere for undermodulen B_0 i R^{d_0}, lad $R^{d_1} \to B_0$ være den tilsvarende surjektive homomorfi, og lad $B_1 \subseteq R^{d_1}$ være kernen. Idet vi fortsætter således fås for $n = 0, 1, \dots$ en surjektiv homomorfi $R^{d_n} \to B_{n-1}$ med kernen B_n . For $n = 1, 2, \dots$ betegnes med $\partial_n\colon R^{d_n} \to R^{d_{n-1}}$ den sammensatte homomorfi $R^{d_n} \twoheadrightarrow B_{n-1} \hookrightarrow R^{d_{n-1}}$. Det er klart, at med denne konstruktion er følgen (1.6.1) eksakt.

For $n < 0$ sætter vi $d_n := 0$ (og dermed $R^{d_n} = 0$). Herved fremkommer et kompleks F, hvor $F_n = R^{d_n}$ og hvor differentialet ∂_n er nul-homomorfien for $n \leqslant 0$. Den eneste homologimodul, der ikke er 0, er H_0. Homomorfien ∂_0 er nul-homomorfien, så $Z_0 = R^{d_0}$, og B_0 er ifølge konstruktionen kernen for den surjektive homomorfi $R^{d_0} \to R/\mathfrak{a}$. Altså er $H_0 = Z_0/B_0 = R/\mathfrak{a}$.

For hver R-modul M danner vi nu komplekset $X = X(M)$ defineret ved at

$$X^n := \operatorname{Hom}_R(R^{d_n},\ M)$$

Differentialerne i komplekset er homomorfierne $X^n \to X^{n+1}$ defineret ved $\varphi \mapsto \varphi\partial_{n+1}$. Det er klart, at X er et kompleks. Med $E^n(M)$ betegnes den n'te homologimodul for komplekset $X(M)$. Nøgleresultatet vil fremgå af Sætningen herunder. Inden vi kan bevise denne sætning må vi i nogle lemma'er udlede nogle egenskaber ved $E^r(M)$ som funktion af modulen M.

Når disse lemma'er, og den efterfølgende sætning, er bevist, er også nøgleresultatet bevist. $\square$

(1.7) Lemma. *Betragt komplekset F defineret i* (1.6). *Lad f være et element i idealet $\mathfrak{a}$. Familien (f_n), hvor f_n er multiplikation med f på F_n, er da en nul-homotop endomorfi af komplekset F.*

Bevis. Vi skal bestemme en familie (s_n) af homomorfier $s_n\colon F_n \to F_{n+1}$ således at der for alle n gælder:

$$f_n = \partial_{n+1}s_n + s_{n-1}\partial_n. \tag{1}$$

Homomorfierne s_n konstrueres induktivt. For $n < 0$ er $F_n = 0$, så s_n er nødvendigvis nul-homomorfien. Med dette valg er (1) opfyldt for $n < 0$. For $n = 0$ er $Z_0 = F_0$ og $H_0 = F_0/B_0$ er isomorf med $R/\mathfrak{a}$ ifølge konstruktionen af F. Multiplikation med f afbilder derfor F_0 ind i B_0. Da F_0 er en fri modul og B_0 er billedet for ∂_1, følger det at der findes en homomorfi $s_0\colon F_0 \to F_1$ så at $\partial_1 s_0 = f_0$. Med dette valg af s_0 er (1) opfyldt for $n \leqslant 0$.

Antag nu, at $m > 0$ og at homomorfierne s_n er bestemt for $n < m$ således at (1) er opfyldt. Vi skal bestemme homomorfien $s_m\colon F_m \to F_{m+1}$ så at (1) også er opfyldt for $n = m$. Betragt hertil differensen, $f_m - s_{m-1}\partial_m$. Da ∂_m er R-lineær, gælder $\partial_m f_m = f_{m-1}\partial_m$. Ved anvendelse af (1) for $n = m - 1$ fås derfor, at

$$\partial_m(f_m - s_{m-1}\partial_m) = (f_{m-1} - \partial_m s_{m-1})\partial_m = s_{m-2}\partial_{m-1}\partial_m = 0.$$

Denne ligning viser, at differensen $f_m - s_{m-1}\partial_m$ afbilder ind i Z_m. Da vi har antaget, at $m > 0$, er $Z_m = B_m$. Differensen afbilder altså ind i billedet for ∂_{m+1}. Da F_m er en fri modul, følger det at der findes en homomorfi $s_m\colon F_m \to F_{m+1}$ så at differensen $f_m - s_{m-1}\partial_m$ er lig med $\partial_{m+1}s_m$. Denne lighed betyder netop, at (1) er opfyldt for $n = m$. Hermed er det induktive skridt i konstruktionen gennemført, hvormed eksistensen af den søgte familie (s_n) er godtgjort. $\square$

(1.8) Lemma. *Ethvert element i idealet $\mathfrak{a}$ annullerer alle modulerne $E^n(M)$.*

Bevis. Lad f tilhøre $\mathfrak{a}$. Modulen $E^n(M)$ er den n'te homologimodul af komplekset $X = X(M)$. Betragt en klasse i $E^n(X)$, repræsenteret ved en n-cykel φ, dvs ved en homomorfi $\varphi\colon F_n \to M$ så at $\varphi\partial_{n+1} = 0$. Det skal vises, at n-cyklen $f\varphi$ er en rand, altså at der findes en homomorfi $\psi\colon F_{n-1} \to M$ så at

$$f\varphi = \psi\partial_n. \tag{1}$$

Hertil bemærkes, at da φ er R-lineær, er $f\varphi$ lig med den sammensatte homomorfi φf_n, hvor f_n er multiplikation med f på modulen F_n. Ifølge Lemma (1.7) findes homomorfier s_n og s_{n-1} således at $f_n = \partial_{n+1}s_n + s_{n-1}\partial_n$. Ved indsættelse fås ligningerne,

$$f\varphi = \varphi f_n = \varphi\partial_{n+1}s_n + \varphi s_{n-1}\partial_n = \varphi s_{n-1}\partial_n.$$

Ligningen (1) er derfor opfyldt med $\psi := \varphi s_{n-1}$. ∎

(1.9) Lemma. *En kort eksakt følge* $0 \to M' \to M \to M'' \to 0$ *inducerer en lang eksakt følge,*

$$E^{n-1}(M') \longrightarrow E^{n-1}(M) \longrightarrow E^{n-1}(M'') \xrightarrow{\delta} E^n(M') \longrightarrow E^n(M) \longrightarrow E^n(M''). \tag{1.9.1}$$

Bevis. Vi kan antage, at $M' \to M$ er inklusionen i af en undermodul M' i M og at $M \to M''$ er den tilhørende kanoniske homomorfi p af M på kvotienten. Nu bemærkes først, at vi for enhver fri modul $F = R^d$ har en eksakt følge,

$$0 \to \operatorname{Hom}_R(F, M') \to \operatorname{Hom}_R(F, M) \to \operatorname{Hom}_R(F, M'') \to 0.$$

Uden forudsætninger om modulen F er det nemlig klart, at hvis en homomorfi $\varphi\colon F \to M'$ opfattet som homomorfi $F \to M$ er nul, så er φ selv nul, og videre, at en homomorfi $\psi\colon F \to M$ ved sammensætning med $p\colon M \to M/M'$ giver nul, hvis og kun hvis ψ afbilder ind i undermodulen M'. For endelig at vise, at følgen er eksakt i $\operatorname{Hom}_R(F, M'')$ bruges at F er fri og $p\colon M \to M''$ er surjektiv.

Ifølge definitionen i (1.6) er $E^n(M)$ den n'te homologimodul af komplekset $X(M)$, hvor $X^n(M) = \operatorname{Hom}_R(F_n, M)$. Idet bemærkningen ovenfor anvendes på F_n for alle n, fås en kort eksakt følge af komplekser, $0 \to X(M') \to X(M) \to X(M'') \to 0$. Den lange eksakte følge (1.9.1) er nu blot den inducerede lange eksakte følge af homologimoduler. ∎

(1.10) Sætning. *Lad M være en R-modul og lad $\mathbf{f} = (f_1, \dots, f_r)$ være en M-regulær følge i idealet $\mathfrak{a}$. Da er $E^n(M) = 0$ for $n < r$ og*

$$E^r(M) = \operatorname{Hom}_R(R/\mathfrak{a}, M/\mathbf{f}M).$$

Bevis. Påstanden vises ved induktion efter r. For $r = 0$ er påstanden, at $E^n(M) = 0$ for $n < 0$ og

$$E^0(M) = \operatorname{Hom}_R(R/\mathfrak{a}, M).$$

For $n < 0$ er $X^n(M) = 0$, og følgelig er også $E^n(M) = 0$. Modulen $E^0(M)$ bestemmes ud fra nul-følgen,

$$\mathrm{Hom}_R(F_{-1}, M) \to \mathrm{Hom}_R(F_0, M) \to \mathrm{Hom}_R(F_1, M).$$

Her er den første modul lig med nul (da $F_{-1} = 0$), og $E^0(M)$ er altså kernen for den anden homomorfi. Ved denne anden homomorfi afbildes $\varphi\colon F_0 \to M$ på $\varphi\partial_1$. Homomorfien φ tilhører altså kernen, hvis og kun hvis $\varphi\partial_1 = 0$. Da følgen $F_1 \xrightarrow{\partial_1} F_0 \longrightarrow R/\mathfrak{a} \longrightarrow 0$ ifølge konstruktionen af komplekset F er eksakt, slutter vi, at homomorfierne φ i kernen netop svarer til samtlige homomorfier $R/\mathfrak{a} \to M$. Hermed er vist, at $E^0(M) = \mathrm{Hom}_R(R/\mathfrak{a}, M)$, og følgelig gælder påstanden for $r = 0$.

Antag, at $r > 0$. Sæt $M' := M/f_1M$. Følgen $\mathbf{f}' = (f_2, \dots, f_r)$ er da en M'-regulær følge i $\mathfrak{a}$ af længde $r - 1$, så det kan antages, at påstanden gælder for denne følge. Yderligere er f_1 regulær på M, så vi har en eksakt følge $0 \to M \xrightarrow{f_1} M \to M' \to 0$. Idet vi anvender resultatet i Lemma (1.7) udleder vi en exact følge,

$$E^{n-1}(M) \xrightarrow{f_1} E^{n-1}(M) \longrightarrow E^n(M') \xrightarrow{\delta} E^n(M) \xrightarrow{f_1} E^n(M).$$

Her er yderligere multiplikationerne med f_1 lig med nul-homomorfien ifølge Lemma (1.8). Altså får vi den eksakte følge,

$$0 \longrightarrow E^{n-1}(M) \longrightarrow E^{n-1}(M') \xrightarrow{\delta} E^n(M) \longrightarrow 0.$$

For $n < r$ er den midterste modul nul ifølge induktionsforudsæningen, og for modulen til højre gælder derfor også $E^n(M) = 0$. For $n = r$ er modulen til venstre lig med nul ifølge det lige viste. Af eksaktheden fås derfor den første lighed i ligningerne,

$$E^r(M) = E^{r-1}(M') = \mathrm{Hom}_R(R/\mathfrak{a}, M'/\mathbf{f}'M') = \mathrm{Hom}_R(R/\mathfrak{a}, M/\mathbf{f}M).$$

Den anden lighed følger af induktionsantagelsen og den sidste af ligheden $M'/\mathbf{f}'M' = M/\mathbf{f}M$.

Hermed er de ønskede ligheder vist for r. □

(1.11) Bemærkning. Det her givne bevis for Nøgleresultatet er ved hjælp af metoder fra homologisk algebra. De konstruerede moduler $E^n(M)$ betegnes her mere udførligt $\mathrm{Ext}^n_R(R/\mathfrak{a}, M)$, og de kaldes også *Ext*-modulerne svarende til $R/\mathfrak{a}$ og M. De kan også defineres når R-modulen $R/\mathfrak{a}$ erstattes med en vilkårlig R-modul N.

Det er klart, at definitionerne i (1.2) ikke forudsætter, at R er noethersk og at M er endeligt frembragt. Resultaterne i denne paragraf gælder også uden denne forudsætning. I beviserne er det nemlig om komplekset F konstrueret i (1.6) kun benyttet, at hvert F_n er en fri R-modul, dvs en modul med en (ikke nødvendigvis endelig) basis, og det er let at se, at konstruktionen i (1.6) i det almindelige tilfælde kan gennemføres med frie moduler F_n.

2. Dybde af noetherske ringe.

(2.1) Setup. Vi minder om, at R betegner en noethersk ring, $\mathfrak{a}$ betegner et ideal i R, og M betegner en endeligt frembragt R-modul. Et element f i R er som bekendt M-regulært, hvis og kun hvis f ikke tilhører noget associeret primideal for M.

(2.2) Definition. Ved $\mathfrak{a}$-*dybden* af M, betegnet $\operatorname{depth}_{\mathfrak{a}} M$, forstås den største længde af en M-regulær følge af elementer i $\mathfrak{a}$. Mere præcist er $\mathfrak{a}$-dybden uendelig, hvis der i $\mathfrak{a}$ findes M-regulære følger af vilkårlig stor længde; specielt er den uendelig, hvis der i $\mathfrak{a}$ findes uendelige M-regulære følger. Bemærk, at nul-modulen har uendelig dybde, idet $(0, 0, \dots)$ er en regulær følge på nul-modulen.

En M-regulær følge i $\mathfrak{a}$ kaldes *maksimal*, hvis den er uendelig, eller er endelig og ikke kan fortsættes til en M-regulær følge i $\mathfrak{a}$ af større længde. Det er klart, at enhver M-regulær følge i $\mathfrak{a}$ kan fortsættes til en maksimal. Vi viser herunder, at alle maksimale M-regulære følger i $\mathfrak{a}$ har samme længde. Specielt er $\mathfrak{a}$-dybden altså kun uendelig, når der findes en uendelig M-regulær følge i $\mathfrak{a}$.

Hvis ringen R er lokal med maksimalidealet $\mathfrak{m}$, så kaldes $\mathfrak{m}$-dybden blot for *dybden* af M, og den betegnes $\operatorname{depth} M$.

(2.3) Observation. Dybden $\operatorname{depth}_{\mathfrak{a}} M$ er lig med 0, hvis og kun hvis $\mathfrak{a}$ er indeholdt i et associeret primideal for M. Specielt gælder når R er lokal med maksimalidealet $\mathfrak{m}$, at dybden $\operatorname{depth} M$ er lig med 0, hvis og kun hvis $\mathfrak{m}$ er associeret primideal for M.

Foreningsmængden af de associerede primidealer for M er nemlig netop komplementærmænden til de M-regulære elementer, og dybden er således 0, netop når $\mathfrak{a}$ er indeholdt i denne forening. Videre er der kun er endelig mange associerede primidealer for M, og så gælder som bekendt, at $\mathfrak{a}$ er indeholdt i foreningen af dem, netop hvis $\mathfrak{a}$ er indeholdt i et af dem.

(2.4) Lemma. *Hvis $\mathfrak{a}M \subset M$, så findes ingen uendelige M-regulære følger i $\mathfrak{a}$.*

Bevis. Antag, at $\mathfrak{a}M \subset M$. Antag indirekte, at der findes en uendelig M-regulær følge $(f_1, f_2, \dots)$ i $\mathfrak{a}$. Sæt $\mathbf{f}_i := (f_1, \dots, f_i)$ for $i = 0, 1, \dots$. Vi har da en uendelig kæde af undermoduler i M,

$$(0) \subseteq \mathbf{f}_1 M \subseteq \mathbf{f}_2 M \subseteq \cdots .$$

Øjensynlig er $\mathbf{f}_i M \subseteq \mathfrak{a}M$, så det følger af antagelsen, at $M/\mathbf{f}_i M \neq 0$. Yderligere er antaget, at multiplikation med f_{i+1} en injektiv afbildning af $M/\mathbf{f}_i M$ ind i sig selv. Billedet ved denne multiplikation er altså ikke nul. Det er klart at billedet, som undermodul i $M/\mathbf{f}_i M$ er undermodulen $\mathbf{f}_{i+1} M/\mathbf{f}_i M$. Denne sidste modul er altså ikke nul, og følgelig er $\mathbf{f}_i M \subset \mathbf{f}_{i+1} M$. I den uendelige kæde derfor alle inklusionerne skarpe, i modstrid med at M er noethersk. ▯

(2.5) Lemma. *Der findes ingen M-regulære elementer i $\mathfrak{a}$, altså* $\operatorname{depth}_{\mathfrak{a}} M = 0$, *hvis og kun hvis* $\operatorname{Hom}_R(R/\mathfrak{a}, M) \neq 0$.

Bevis. At der ikke findes M-regulære elementer i $\mathfrak{a}$ betyder, at hvert element tilhører et associeret primideal for M, altså at $\mathfrak{a}$ er indeholdt i foreningsmængden af de associerede primidealer for M. Dette indtræffer, hvis og kun hvis $\mathfrak{a}$ er indeholdt i et associeret primideal for M. De associerede primidealer for M er primidealerne blandt annullatorerne $\operatorname{Ann} x$ for $x \in M$, $x \neq 0$, og som bekendt er enhver sådan annullator indeholdt i et associeret primideal. Heraf ses, at $\mathfrak{a}$ ikke indeholder M-regulære elementer, hvis og kun hvis $\mathfrak{a}$ er indeholdt i en annullator $\operatorname{Ann} x$ for $x \neq 0$ i M. Den sidste betingelse er ensbetydende med at $\operatorname{Hom}_R(R/\mathfrak{a}, M) \neq 0$, idet homomorfier $\varphi\colon R/\mathfrak{a} \to M$ øjensynlig svarer bijektivt til elementer $x \in M$ hvor $\mathfrak{a} \subseteq \operatorname{Ann} x$. $\square$

(2.6) Sætning. *En endelig M-regulær følge $\mathbf{f} = (f_1, \dots, f_r)$ i $\mathfrak{a}$ er maksimal, hvis og kun hvis $\operatorname{Hom}_R(R/\mathfrak{a}, M/\mathbf{f}M) \neq 0$.*

Bevis. Påstanden følger umiddelbart ved at anvende Lemma (2.5) på $M/\mathbf{f}M$. $\square$

(2.7) Korollar. *Alle maksimale M-regulære følger i $\mathfrak{a}$ har samme længde, nemlig* $\operatorname{depth}_{\mathfrak{a}} M$.

Bevis. Hvis der ikke findes en endelig maksimal M-regulær følge i $\mathfrak{a}$, har alle maksimale M-regulære følger uendelig længde.

Antag, at der findes en maksimal M-regulær følge $\mathbf{f} = (f_1, \dots, f_r)$ i $\mathfrak{a}$. Det er nok at vise, at der for enhver anden M-regulær følge $(g_1, \dots, g_t)$ i $\mathfrak{a}$ gælder $t \leqslant r$. Antag indirekte, at $t > r$. Da er delfølgen $\mathbf{g} := (g_1, \dots, g_r)$ en M-regulær følge, der ikke er maksimal. Af Lemma (2.6) følger nu for modulerne $\operatorname{Hom}_R(R/\mathfrak{a}, M/\mathbf{f}M)$ og $\operatorname{Hom}_R(R/\mathfrak{a}, M/\mathbf{g}M)$, at den første er forskellig fra 0 og den anden er lig med 0. Dette er øjensynlig i modstrid at de to moduler er isomorfe ifølge Nøgleresultatet (1.6). $\square$

(2.8) Korollar. *Dybden* $\operatorname{depth}_{\mathfrak{a}} M$ *er endelig, hvis og kun hvis $\mathfrak{a}M \subset M$. Specielt gælder når R er lokal, at dybden* $\operatorname{depth} M$ *er endelig, hvis og kun hvis $M \neq 0$.*

Bevis. Den sidste påstand er en konsekvens af den første ifølge Nakayama's Lemma.

Hvis $\mathfrak{a}M \subset M$, så følger det af Lemma (2.4), at der findes en endelig maksimal M-regulær følge i $\mathfrak{a}$. Altså er $\operatorname{depth}_{\mathfrak{a}} M < \infty$.

Antag omvendt, at $\mathfrak{a}M = M$, altså at kvotiente $M/\mathfrak{a}M$ er lig med nul. Da M er endeligt frembragt, består støtten for kvotienten $M/\mathfrak{a}M$ af de primidealer, som omfatter $\operatorname{Ann}(M)$ og $\mathfrak{a}$. Da $M/\mathfrak{a}M = 0$, er støtten tom. Der findes altså ingen primidealer, som omfatter idealet $\mathfrak{a} + \operatorname{Ann} M$, og følgelig er $\mathfrak{a} + \operatorname{Ann} M = R$. Skriv nu $1 = f + n$, hvor $f \in \mathfrak{a}$ og $n \in \operatorname{Ann} M$. Multiplikation med f på M er da den identiske afbildning. Specielt er f et M-regulært element i $\mathfrak{a}$, og $M/fM = 0$. Alle elementer er regulære på nul-modulen, så følgen med det ene element f kan udvides med en vilkårlig følge af elementer i $\mathfrak{a}$ (fx til følgen $(f, 0, 0, \dots)$) til en uendelig M-regulær følge i $\mathfrak{a}$. Altså er dybden uendelig. $\square$

(2.9) Korollar. *Lad $\mathbf{f} = (f_1, \dots, f_r)$ være en M-regulær følge i $\mathfrak{a}$. Da er*

$$\operatorname{depth}_{\mathfrak{a}} M/\mathbf{f}M = \operatorname{depth}_{\mathfrak{a}} M - r.$$

Bevis. Det er klart, at en følge $(f_1, \dots, f_r, g_1, \dots, g_t)$ i $\mathfrak{a}$ er M-regulær, hvis og kun hvis følgen $\mathbf{f} = (f_1, \dots, f_r)$ er M-regulær og følgen $(g_1, \dots, g_t)$ er $M/\mathbf{f}M$-regulær. Da enhver regulær M-regulær følge kan udvides til en maksimal M-regulær følge, følger påstanden af Korollar (2.7). $\square$

(2.10) Sætning. *Følgende ulighed gælder:*

$$\operatorname{depth}_{\mathfrak{a}} M \leqslant \operatorname{ht}_M(\mathfrak{a}) = \inf_{\mathfrak{p}\in\operatorname{Supp} M,\ \mathfrak{p}\supseteq\mathfrak{a}} \dim M_{\mathfrak{p}}. \tag{2.10.1}$$

Specielt gælder, at enhver M-regulær følge er en M-højdefølge.

For et primideal $\mathfrak{p}$ er $\operatorname{depth}_{\mathfrak{p}} M \leqslant \operatorname{depth} M_{\mathfrak{p}}$, *og hvis* $\mathfrak{p} \in \operatorname{Supp} M$ *er* $\operatorname{depth} M_{\mathfrak{p}} \leqslant \dim M_{\mathfrak{p}}$.

Bevis. Det afsluttende lighedstegn i (2.10.1) er blot definitionen af M-højden. Ulighedens venstreside er et supremum og dens højreside et infimum. Det skal altså vises, at når $(f_1, \dots, f_r)$ er en M-regulær følge i $\mathfrak{a}$ og $\mathfrak{p}$ et et primideal i $\operatorname{Supp} M$ med $\mathfrak{p} \supseteq \mathfrak{a}$, så er $r \leqslant \dim M_{\mathfrak{p}}$.

Sættes $\mathbf{f}_i := (f_1, \dots, f_i)$, har vi eksakte følger,

$$0 \to M/\mathbf{f}_{i-1}M \xrightarrow{f_i} M/\mathbf{f}_{i-1}M \longrightarrow M/\mathbf{f}_i M \longrightarrow 0.$$

Ved lokalisering i $\mathfrak{p}$ følger det derfor, at billederne af $f_1, \dots, f_r$ i $R_{\mathfrak{p}}$ er en $M_{\mathfrak{p}}$-regulær følge. Disse billeder ligger i maksimalidealet $\mathfrak{p}R_{\mathfrak{p}}$, da $\mathfrak{a} \subseteq \mathfrak{p}$. Vi kan derfor antage, at R er lokal, og at følgen ligger i maksimalidealet $\mathfrak{m}$ for R. Yderligere er så $M \neq 0$, idet $\mathfrak{p}$ lå i støtten for M.

Når f_1 er M-regulær, vil f_1 ikke ligge i noget associeret primideal for M. Specielt vil f_1 ikke tilhøre nogen af de minimale primidealer $\mathfrak{q}$ for M for hvilke $\dim R/\mathfrak{q} = \dim M$. Altså er $\dim M/f_1M < \dim M$. Ved gentagen anvendelse heraf ses, at $\dim M/\mathbf{f}M \leqslant \dim M - r$. Altså er $r \leqslant \dim M$. Hermed er (2.10.1) bevist.

Lad nu $(f_1, \dots, f_r)$ være en M-regulær følge, og lad $\mathfrak{a}$ være idealet frembragt af de første i elementer i følgen. Disse i elementer udgør så en M-regulær følge i $\mathfrak{a}$, så $\operatorname{depth}_{\mathfrak{a}} M \geqslant i$. Uligheden (2.10.1) medfører derfor, at $i \leqslant \operatorname{ht}_M(f_1, \dots, f_i)$. Altså er den givne følge en M-højdefølge.

Betragt endelig et primideal $\mathfrak{p}$. Som nævnt i begyndelsen af beviset vil en M-regulær følge i $\mathfrak{p}$ lokaliseres til en $M_{\mathfrak{p}}$-regulær følge i maksimalidealet $\mathfrak{p}R_{\mathfrak{p}}$. Heraf fås uligheden $\operatorname{depth}_{\mathfrak{p}} M \leqslant \operatorname{depth} M_{\mathfrak{p}}$. Hvis $M_{\mathfrak{p}} \neq 0$, så fås uligheden $\operatorname{depth} M_{\mathfrak{p}} \leqslant \dim M_{\mathfrak{p}}$ ved at anvende (2.10.1) på $R_{\mathfrak{p}}$-modulen $M_{\mathfrak{p}}$ og $\mathfrak{a} := \mathfrak{p}R_{\mathfrak{p}}$.

Hermed er alle påstande bevist. □

(2.11) Bemærkning. For et primideal $\mathfrak{p}$ gælder der ikke nødvendigvis lighedstegn i uligheden $\operatorname{depth}_{\mathfrak{p}} M \leqslant \operatorname{depth} M_{\mathfrak{p}}$. Det er nemlig ikke svært at konstruere et eksempel på en endeligt frembragt modul M og primidealer $\mathfrak{p} \subset \mathfrak{q}$ således at $\mathfrak{p}$ ligger i $\operatorname{Supp} M$ men ikke i $\operatorname{Ass} M$ og $\mathfrak{q}$ ligger i $\operatorname{Ass} M$. (Et sådant $\mathfrak{q}$ er nødvendigvis et indlejret primideal for M.) For et sådant eksempel gælder $\operatorname{depth}_{\mathfrak{p}} M = 0$ og $\operatorname{depth} M_{\mathfrak{p}} > 0$.

(2.12) Sætning. *Følgende ligheder gælder:*

$$\operatorname{depth}_{\mathfrak{a}} M = \inf_{\mathfrak{p}\supseteq\mathfrak{a}} \operatorname{depth} M_{\mathfrak{p}} = \inf_{\mathfrak{p}\supseteq\mathfrak{a}} \operatorname{depth}_{\mathfrak{p}} M.$$

Bevis. Tallet i midten er som nævnt mindst lig med tallet til højre, og tallet til højre er trivielt mindst lig med tallet til venstre. Det er derfor nok at vise den første lighed.

Lad $i(M)$ betegne tallet i midten. Betragt først tilfældet, hvor $i(M) = \infty$. Det følger så af Korollar (2.8), at $M_\mathfrak{p} = 0$ for alle $\mathfrak{p} \supseteq \mathfrak{a}$, eller ækvivalent, at støtten for $M/\mathfrak{a}M$ er tom. Altså er $\operatorname{depth}_\mathfrak{a} M = \infty$, igen ifølge Korollar (2.8).

Når $i(M)$ er endelig, vises ligheden ved induktion efter $i = i(M)$. For et primideal $\mathfrak{p}$ gælder, at $\operatorname{depth} M_\mathfrak{p} = 0$, hvis og kun hvis maksimalidealet $\mathfrak{p}R_\mathfrak{p}$ er associeret til $M_\mathfrak{p}$. Det sidste indtræffer som bekendt hvis og kun hvis $\mathfrak{p}$ er associeret til M. Heraf ses, at $i(M) = 0$, hvis og kun hvis $\operatorname{depth}_\mathfrak{a} M = 0$.

Specielt gælder altså ligheden når $i = 0$. Antag, at $i > 0$. Da er også $\operatorname{depth}_\mathfrak{a} M > 0$. Følgelig findes i $\mathfrak{a}$ et M-regulært element f. For hvert $\mathfrak{p} \supseteq \mathfrak{a}$ er billedet af f i $R_\mathfrak{p}$ et $M_\mathfrak{p}$-regulært element i maksimalidealet $\mathfrak{p}R_\mathfrak{p}$. Af Korollar (2.9) følger derfor, at $\operatorname{depth}_\mathfrak{a} M/fM = \operatorname{depth}_\mathfrak{a} M - 1$ og $i(M/fM) = i(M) - 1$. Altså er

$$\operatorname{depth}_\mathfrak{a} M = \operatorname{depth}_\mathfrak{a} M/fM + 1 = i(M/fM) + 1 = i(M),$$

idet det midterste lighedstegn følger induktivt. □

(2.13) Lemma. *Lad $\mathfrak{p}$ være et associeret primideal for M, og lad f være et M-regulært element. Ethvert primideal $\mathfrak{q}$, som er isoleret primideal for $\mathfrak{p} + (f)$, vil da være associeret primideal for kvotienten M/fM.*

Bevis. Lad $\mathfrak{p}_1 = \mathfrak{p}, \mathfrak{p}_2, \dots, \mathfrak{p}_t$ være samtlige associerede primidealer for M, og betragt en uforkortelig primærdekomposition af undermodulen (0) i M,

$$(0) = N_1 \cap \cdots \cap N_t,$$

hvor N_j er $\mathfrak{p}_j$-primær i M (dvs. $\operatorname{Ass}(M/N_j) = \{\mathfrak{p}_j\}$). Lad Q være fællesmængden $N_2 \cap \cdots \cap N_t$. Da er $Q \neq (0)$, da dekompositionen er uforkortelig. Den sammensatte homomorfi $Q \to M \to M/N_1$ har kernen $N_1 \cap Q = (0)$, og den er derfor injektiv. Altså er $\operatorname{Ass} Q \subseteq \operatorname{Ass} M/N_1 = \{\mathfrak{p}_1\}$, og heraf følger videre, at $\operatorname{Ass} Q = \{\mathfrak{p}_1\}$. På den anden side har homomorfien $M \to M/N_2 \oplus \cdots M/N_t$ kernen Q. Heraf følger ved anvendelse af en sætning om associerede primidealer, $\operatorname{Ass} M/Q$ er en delmængde af mængden $\{\mathfrak{p}_2, \dots \mathfrak{p}_t\}$, og videre, at delmængden ikke kan være ægte. Der gælder altså, at

$$\operatorname{Ass} Q = \{\mathfrak{p}\}, \quad \operatorname{Ass} M/Q = \{\mathfrak{p}_2 \cdots, \mathfrak{p}_t\}.$$

Specielt består støtten af Q af de primidealer, der omfatter $\mathfrak{p}$. Heraf følger, at $\operatorname{Supp} Q/fQ$ består af de primidealer, der omfatter $\mathfrak{p} + (f)$. Det givne primideal $\mathfrak{q}$ er ifølge antagelsen minimalt blandt sådanne primidealer. Altså er $\mathfrak{q}$ et minimalt primideal for Q/fQ. Specielt er $\mathfrak{q}$ associeret til Q/fQ.

Nu var f regulært på M, og følgelig er f ikke element i noget $\mathfrak{p}_i$. Specielt er f derfor regulær på M/Q. Heraf følger (fx ved hjælp af Slangelemmaet), at den kanoniske homomorfi $Q/fQ \to M/fM$ er injektiv. Da $\mathfrak{q}$ var associeret til Q/fQ, er $\mathfrak{q}$ også associeret til M/fM, som ønsket. □

(2.14) Dybde-uligheden. *Lad $\mathfrak{p} \supseteq \mathfrak{q}$ være primidealer, og antag, at $\mathfrak{q}$ er associeret primideal for M. Da gælder uligheden,*

$$\operatorname{depth}_{\mathfrak{p}} M \leqslant \operatorname{ht} \mathfrak{p}/\mathfrak{q}.$$

Bevis. Uligheden vises ved fuldstændig induktion efter $h = \operatorname{ht} \mathfrak{p}/\mathfrak{q}$. Antag først $h = 0$. Da er $\mathfrak{p} = \mathfrak{q}$ et associeret primideal for M. Følgelig er $\operatorname{depth}_{\mathfrak{q}} M = 0$. Altså gælder uligheden (nødvendigvis som en lighed) når $h = 0$.

Antag, at $h > 0$. Uligheden er trivielt opfyldt, hvis venstresiden er lig med 0. Antag derfor, at $\operatorname{depth}_{\mathfrak{p}} M > 0$. Da findes i $\mathfrak{p}$ et M-regulært element f. Primidealet $\mathfrak{p}$ vil nu indeholde idealet $\mathfrak{q} + (f)$. Der findes derfor et primideal $\mathfrak{q}' \subseteq \mathfrak{p}$ som er isoleret for $\mathfrak{q} + (f)$. Ifølge det foregående Lemma er $\mathfrak{q}'$ associeret primideal for M/fM. Yderligere er $\mathfrak{q}' \supset \mathfrak{q}$, idet $f \notin \mathfrak{q}$, så specielt er $\operatorname{ht} \mathfrak{p}/\mathfrak{q}' < \operatorname{ht} \mathfrak{p}/\mathfrak{q}$. Af Korollar (2.7) og induktion anvendt på $\mathfrak{p} \supseteq \mathfrak{q}'$ og M/fM fås derfor ulighederne,

$$\operatorname{depth}_{\mathfrak{p}} M = \operatorname{depth}_{\mathfrak{p}} M/fM + 1 \leqslant \operatorname{ht} \mathfrak{p}/\mathfrak{q}' + 1 \leqslant \operatorname{ht} \mathfrak{p}/\mathfrak{q}.$$

Hermed er Dybde-uligheden bevist. $\square$

3. Lokale Cohen–Macaulay ringe.

(3.1) Setup. I denne paragraf betegner R betegner en lokal noethersk ring med maksimalidealet $\mathfrak{m}$ og M betegner en endeligt frembragt R-modul.

(3.2) Definition. Modulen M over den lokale ring R kaldes en *Cohen–Macaulay modul*, hvis $\operatorname{depth} M = \dim M$ eller hvis $M = 0$.

For $M = 0$ er $\operatorname{depth} M = \infty$ og $\dim M = -\infty$, og altså specielt $\operatorname{depth} M \neq \dim M$. Hvis $M \neq 0$, så følger det af den sidste påstand i Sætning (2.10), anvendt med $\mathfrak{p} := \mathfrak{m}$, at der gælder uligheden,

$$\operatorname{depth} M \leqslant \dim M,$$

og betingelsen for at M er Cohen–Macaulay er således, at lighed gælder i denne ulighed.

(3.3) Hovedsætning. *Antag, at R er lokal med maksimalideal $\mathfrak{m}$. Lad M være en Cohen–Macaulay modul. Da gælder:*

(1) *For ethvert associeret primideal $\mathfrak{q}$ for M gælder ligningen* $\dim R/\mathfrak{q} = \dim M$. *Specielt har M ingen indlejrede primidealer.*

(2) *Hvis $\mathbf{f} = (f_1, \dots, f_r)$ er en M-regulær følge i $\mathfrak{m}$, så er $M/\mathbf{f}M$ en Cohen–Macaulay-modul, og*

$$\dim M/\mathbf{f}M = \dim M - r.$$

(3) *Er omvendt $\mathbf{f} = (f_1, \dots, f_r)$ en følge af r elementer i maksimalidealet $\mathfrak{m}$ således at* $\dim M/\mathbf{f}M = \dim M - r$, *så er følgen M-regulær.*

Bevis. (1): Lad $\mathfrak{q}$ være et associeret primideal for M (specielt kan M altså ikke være nulmodulen). Da gælder ulighederne,

$$\dim M = \operatorname{depth} M \leqslant \operatorname{ht} \mathfrak{m}/\mathfrak{q} = \dim R/\mathfrak{q} \leqslant \dim M.$$

Den første (lighed) følger af forudsætningen om M, den anden (ulighed) er Dybde-uligheden (2.14) anvendt med $\mathfrak{p} = \mathfrak{m}$, den tredie (lighed) følger af at $R/\mathfrak{q}$ er lokal, og den sidste ulighed følger af at $\mathfrak{q}$ er associeret for M og derfor i støtten for M.

Af disse uligheder fremgår ligningen i (1). Den anden påstand i (1) er øjensynlig en konsekvens af den første.

(2): Antag, at $\mathbf{f} = (f_1, \dots, f_r)$ er en M-regulær følge i $\mathfrak{m}$. Hvis $M = 0$, er påstanden triviel. Antag, at $M \neq 0$. Da er $\operatorname{depth} M/\mathbf{f}M = \operatorname{depth} M - r$ ifølge Korollar (2.9). Når f_1 i $\mathfrak{m}$ er M-regulær, gælder trivielt, at $\dim M/f_1M \leqslant \dim M - 1$. Gentagen anvendelse heraf giver uligheden $\dim M/\mathbf{f}M \leqslant \dim M - r$. Altså gælder ulighederne,

$$\operatorname{depth} M/\mathbf{f}M = \operatorname{depth} M - r = \dim M - r \geqslant \dim M/\mathbf{f}M.$$

For moduler forskellige fra 0 gælder altid, at dybden højst er dimensionen. I ulighederne ovenfor gælder derfor lighed. Heraf følger begge påstande i (2).

(3): Igen er påstanden triviel, hvis $M = 0$, så vi antager $M \neq 0$. Hvis f tilhører maksimalidealet $\mathfrak{m}$, så gælder som bekendt ulighederne,

$$\dim M - 1 \leqslant \dim M/fM \leqslant \dim M, \tag{*}$$

og uligheden til venstre er en lighed hvis og kun hvis f ikke tilhører et af de minimale primidealer $\mathfrak{q}$ for M for hvilke $\dim R/\mathfrak{q} = \dim M$.

Påstanden i (3) vises ved induktion efter r. Lad $(f_1, \dots, f_r)$ være en følge i $\mathfrak{m}$ således at ligningen $\dim M/(f_1, \dots, f_r)M = \dim M - r$ er opfyldt. Det fremgår af ulighederne (*), at denne ligning medfører begge ligningerne,

$$\dim M/f_1M = \dim M - 1, \qquad \dim M'/(f_2, \dots, f_r)M' = \dim M' - (r - 1),$$

hvor $M' = M/f_1M$. Af den første ligning følger, at f_1 ikke tilhører de primidealer $\mathfrak{q}$ i støtten for M for hvilket $\dim R/\mathfrak{q} = \dim M$. Af (1) følger derfor, at f_1 ikke kan tilhøre et associeret primideal for M. Altså er f_1 regulær på M. Af (2) følger så, at $M' = M/f_1M$ er en Cohen–Macaulay modul. Den anden ligning medfører derfor (induktivt), at $(f_2, \dots, f_r)$ er en M'-regulær følge. Altså er $(f_1, \dots, f_r)$ en M-regulær følge.

Hermed er de tre påstande bevist. $\square$

(3.4) Definition. Den lokale ring R kaldes en *Cohen–Macaulay ring*, hvis R som R-modul er en Cohen–Macaulay modul, dvs hvis $\operatorname{depth} R = \dim R$. Det er klart for en kvotient $R/\mathfrak{a}$, hvor $\mathfrak{a}$ er et ægte ideal (dvs $\mathfrak{a} \subseteq \mathfrak{m}$), at kvotienten er Cohen–Macaulay som ring, hvis og kun hvis den er Cohen–Macaulay som R-modul.

(3.5) Eksempel. En lokal ring af dimension 0 (fx et legeme) er altid Cohen–Macaulay. En lokal ring af dimension 1 er Cohen–Macaulay, hvis den er et integritetsområde. Fx er en diskret valuationsring en Cohen–Macaulay ring.

Betragt polynomiumsringen $k[X_1, \dots, X_n]$, hvor k er et legeme. Lad R være den lokale ring, der fremkommer ved at lokalisere polynomiumsringen i maksimalidealet $\mathfrak{M} = (X_1, \dots, X_n)$. Følgen $(X_1, \dots, X_n)$ er øjensynlig en regulær følge i polynomiumsringen, og dermed også en regulær følge i maksimalidealet $\mathfrak{m}$ i R. Altså er $\operatorname{depth} R \geqslant n$. På den anden side er det velkendt, at $\dim R = n$. Altså er R en lokal Cohen–Macaulay ring.

(3.6) Sætning. *Lad $M \neq 0$ være en Cohen–Macaulay modul over den lokale ring R. For en følge $\mathbf{f} = (f_1, \dots, f_r)$ af r elementer i maksimalidealet $\mathfrak{m}$ er følgende betingelser ækvivalente:*

(i) *Følgen $\mathbf{f}$ er en M-regulær følge.*
(ii) *Følgen $\mathbf{f}$ er en M-højdefølge.*
(iii) $\operatorname{ht}_M(\mathbf{f}R) = r$.
(iv) $\dim M/\mathbf{f}M = \dim M - r$.

Bevis. Implikationen (i)⇒(ii) følger af Sætning (2.10). Implikationen (ii)⇒(iii) følger af et korollar til Krull's Idealsætning.

(iii)⇒(iv): Betragt et primideal $\mathfrak{p}$ i støtten for $M/\mathbf{f}M$. Da gælder ulighederne,

$$\dim M \geqslant \operatorname{ht} \mathfrak{m}/\mathfrak{p} + \dim M_{\mathfrak{p}} \geqslant \operatorname{ht} \mathfrak{m}/\mathfrak{p} + r,$$

idet den første ulighed følger af definitionen på Krull-dimension og den anden følger af antagelsen i (iii). Ulighederne medfører, at der for ethvert sådant primideal $\mathfrak{p}$ gælder $\operatorname{ht} \mathfrak{m}/\mathfrak{p} \leqslant \dim M - r$. Heraf ses, at $\dim M/\mathbf{f}M \leqslant \dim M - r$. Som bekendt gælder den modsatte ulighed, da $M \neq 0$. Følgelig gælder ligheden i (iv).

Den afsluttende implikation (iv)⇒(i) følger af Hovedsætning (3.3)(3). □

(3.7) Bemærkning. Betingelserne (iii) og (iv) i Sætning (3.6) afhænger øjensynlig ikke af rækkefølgen af elementerne f_i. Det følger således når M er en Cohen–Macaulay modul over en lokal ring, at betingelserne (i) og (ii) er invariante under permutation af følgens elementer. Betingelsen (iv) er i øvrigt, når $M \neq 0$, ækvivalent med at $\mathbf{f}$ er en delfølge af et parametersystem for M.

I den efterfølgende paragraf skal vi se nærmere på Cohen–Macaulay ringe der ikke forudsættes at være lokale, og vi udleder en række egenskaber, der altså specielt gælder for lokale Cohen–Macaulay ringe.

4. Cohen–Macaulay ringe.

(4.1) Setup. I denne paragraf betegner R en noethersk ring, og M betegner en endeligt frembragt R-modul.

(4.2) Hovedsætning. *For en endeligt frembragt modul M over en noethersk ring R er følgende betingelser ækvivalente:*

(i) *For alle maksimalidealer $\mathfrak{m}$ i støtten for M er $M_\mathfrak{m}$ en Cohen-Macaulay modul over den lokale ring $R_\mathfrak{m}$.*
(ii) *For enhver følge $\mathbf{f} = (f_1, \dots, f_r)$ således at $\mathrm{ht}_M(\mathbf{f}R) = r$ og ethvert maksimalideal $\mathfrak{m} \supseteq R\mathbf{f}$ er følgen $\mathbf{f}$ en $M_\mathfrak{m}$-regulær følge.*
(iii) *For enhver følge $\mathbf{f} = (f_1, \dots, f_r)$ således at $\mathrm{ht}_M(\mathbf{f}R) = r$ og ethvert primideal $\mathfrak{p} \supseteq R\mathbf{f}$ er følgen $\mathbf{f}$ en $M_\mathfrak{p}$-regulær følge.*
(iv) *For enhver følge $\mathbf{f} = (f_1, \dots, f_r)$ således at $\mathrm{ht}_M(\mathbf{f}R) = r$ har kvotienten $M/\mathbf{f}M$ ikke indlejrede primidealer.*
(v) *Enhver M-højdefølge er en M-regulær følge.*
(vi) *For alle idealer $\mathfrak{a}$ er $\mathrm{depth}_\mathfrak{a} M = \mathrm{ht}_M(\mathfrak{a})$.*
(vii) *For alle primidealer $\mathfrak{p}$ i støtten for M er $\mathrm{depth}_\mathfrak{p} M = \dim M_\mathfrak{p}$.*
(viii) *For alle primidealer $\mathfrak{q}$ i støtten for M og alle primidealer $\mathfrak{p} \supseteq \mathfrak{q}$ gælder ligningen,*

$$\mathrm{depth}_\mathfrak{p} M - \mathrm{depth}_\mathfrak{q} M = \mathrm{ht}\, \mathfrak{p}/\mathfrak{q}. \tag{4.2.1}$$

(ix) *For alle primidealer $\mathfrak{p}$ i R er $M_\mathfrak{p}$ en Cohen-Macaulay modul over den lokale ring $R_\mathfrak{p}$.*

Bevis. Betragt en følge $\mathbf{f} = (f_1, \dots, f_r)$ med r elementer. Hvis $M/\mathbf{f}M = 0$, så er $\mathrm{ht}_M(\mathbf{f}R) = \infty$. Hvis $M/\mathbf{f}M \neq 0$, så gælder ifølge et korllar til Krull's Idealsætning, at $\mathrm{ht}_M(\mathbf{f}R) \leqslant r$. Forudsætningen $\mathrm{ht}_M(\mathbf{f}R) = r$, i betingelserne (ii), (iii) og (iv), er altså ækvivalent med følgende: $M/\mathbf{f}M \neq 0$ og for hvert primideal $\mathfrak{p}$, som omfatter $\mathbf{f}$ og tilhører støtten for M, er $\dim M_\mathfrak{p} \geqslant r$.

(i)⇒(ii): Hvis $\mathfrak{m}$ ikke tilhører støtten for M, er konklusionen i (ii) triviel. Antag derfor, at $\mathfrak{m} \in \mathrm{Supp}\, M$. I (ii) er antagelsen om $\mathbf{f}$, at der for hvert primideal $\mathfrak{p} \supseteq \mathbf{f}$ som tilhører støtten for M gælder uligheden $\dim M_\mathfrak{p} \geqslant r$. Dette kan specielt anvendes på primidealer $\mathfrak{p} \subseteq \mathfrak{m}$, og heraf ses, at $\mathrm{ht}_{M_\mathfrak{m}}(\mathbf{f}R_\mathfrak{m}) = r$. Ifølge forudsætningen (i) er $M_\mathfrak{m}$ en Cohen–Macaulay modul. Af Sætning (3.6), anvendt på billedet i $R_\mathfrak{m}$ af følgen $\mathbf{f}$, følger så, at $\mathbf{f}$ er en $M_\mathfrak{m}$-regulær følge.

(ii)⇒(iii): Vælg et maksimalideal $\mathfrak{m}$, der omfatter det i (iii) givne primideal $\mathfrak{p}$. Primidealet $\mathfrak{p}$ svarer så til et primideal i $R_\mathfrak{m}$, og ved lokalisering i dette primideal fremkommer $M_\mathfrak{p}$ af $M_\mathfrak{m}$. Ifølge forudsætningen (ii) er $\mathbf{f}$ en $M_\mathfrak{m}$ regulær følger, og den lokaliserede følge i $R_\mathfrak{p}$ er derfor $M_\mathfrak{p}$-regulær.

(iii)⇒(iv): Antag indirekte, at der findes et indlejret primideal $\mathfrak{q}$ for $M/\mathbf{f}M$. Primidealet $\mathfrak{q}$ er altså associeret til $M/\mathbf{f}M$ og der findes primidealer $\mathfrak{p}$ i støtten for $M/\mathbf{f}M$ således at $\mathfrak{p} \subset \mathfrak{q}$. Af den sidste egenskab følger, at $\dim M_\mathfrak{q} > \mathrm{ht}_M(\mathbf{f}R)$, dvs at $\mathrm{ht}_M\, \mathfrak{q} > \mathrm{ht}_M(\mathbf{f}R)$. Af denne sidste ulighed følger som bekendt, at der findes et element $f \in \mathfrak{q}$ for hvilket $\mathrm{ht}_M(\mathbf{f}, f) > \mathrm{ht}_M(\mathbf{f}R)$. I (iv) er det antaget, at $\mathrm{ht}_M(\mathbf{f}R) = r$. Altså er $\mathrm{ht}_M(\mathbf{f}, f) \geqslant r + 1$, og her gælder lighedstegn ifølge Krull's Idealsætning. Forudsætningen (iii) medfører derfor, at følgen $(\mathbf{f}, f)$ er $M_{\mathfrak{q}}$ regulær. På den anden side er $\mathfrak{q}$ associeret til $M/\mathbf{f}M$, og heraf følger som bekendt at maximalidealet $\mathfrak{q}R_{\mathfrak{q}}$ associeret til $M_{\mathfrak{q}}/\mathbf{f}M_{\mathfrak{q}}$. Følgen $\mathbf{f}$ i $\mathfrak{q}R_{\mathfrak{q}}$ kan derfor ikke udvides til en større regulær følge. Hermed er den ønskede modstrid opnået.

(iv)$\Rightarrow$(v): Betragt en M-højdefølge $(f_1, f_2, \dots)$. Det skal vises, for $i = 1, 2, \dots$, at f_i er regulær på $M/(f_1, \dots, f_{i-1})M$. Lad $\mathfrak{p}$ være et minimalt primideal for $M/(f_1, \dots, f_{i-1})M$. Af Krull's Hovedidealsætning følger, at $\dim M_{\mathfrak{p}} \leqslant i - 1$ (endda med lighed, da følgen er en højdefølge). Da følgen er en højdefølge, ses det, at $f_i \notin \mathfrak{p}$. Af forudsætningen (iv), anvendt med $r = i - 1$, sluttes derfor, at f_i er regulær på $M/(f_1, \dots, f_{i-1})$.

(v)$\Rightarrow$(vi): Lad $\mathfrak{a}$ være et ideal i R. I den ønskede ligning i (vi) er begge sider ∞, hvis $M/\mathfrak{a}M = 0$. Antag derfor, at $M/\mathfrak{a}M \neq 0$, og sæt $h := \operatorname{ht}_M \mathfrak{a}$. Det er da velkendt, at der i $\mathfrak{a}$ findes en M-højdefølge af længde h. Ifølge forudsætningen (v) er denne følge en M-regulær følge. Altså er $\operatorname{depth}_{\mathfrak{a}} M \geqslant h$. Den modsatte ulighed, og dermed den ønskede lighed, følger nu af Sætning (2.10).

(vi)$\Rightarrow$(vii): Dette følger umiddelbart, idet vi for primidealer $\mathfrak{p} \in \operatorname{Supp} M$ har $\operatorname{ht}_M \mathfrak{p} = \dim M_{\mathfrak{p}}$.

(vii)$\Rightarrow$(viii): Antag, at $\mathfrak{q} \in \operatorname{Supp} M$ og at $\mathfrak{p} \supseteq \mathfrak{q}$. Da gælder følgende uligheder:

$$\operatorname{depth}_{\mathfrak{q}} M + \operatorname{ht} \mathfrak{p}/\mathfrak{q} \leqslant \dim M_{\mathfrak{q}} + \operatorname{ht} \mathfrak{p}/\mathfrak{q} \leqslant \dim M_{\mathfrak{p}} = \operatorname{depth}_{\mathfrak{p}} M.$$

Den første følger nemlig af uligheden i Sætning (2.10) anvendt med $\mathfrak{a} = \mathfrak{q}$, den anden følger af definitionen på Krull-dimension, og den sidste (lighed) følger af forudsætningen (vii).

Ulighederne medfører, at højresiden i (4.2.1) er mindre end eller lig med venstresiden. For at vise den modsatte ulighed betragtes en maksimal M-regulær følge $(f_1, \dots, f_q)$ i $\mathfrak{q}$, hvor altså $q = \operatorname{depth}_{\mathfrak{q}} M$. Følgen er da også $M_{\mathfrak{q}}$-regulær, og følgens længde er ifølge forudsætningen (vii) lig med $\dim M_{\mathfrak{q}}$. Billedet af følgen i $R_{\mathfrak{q}}$ må derfor være en maksimal $M_{\mathfrak{q}}$-regulær følge i maksimalidealet $\mathfrak{q}R_{\mathfrak{q}}$. Maksimaliteten medfører, at maksimalidealet $\mathfrak{q}R_{\mathfrak{q}}$ er associeret primideal for $M_{\mathfrak{q}}/(f_1, \dots, f_q)M_{\mathfrak{q}}$. Heraf følger som bekendt, at $\mathfrak{q}$ er associeret primideal for modulen $M/(f_1, \dots, f_q)M$. Nu fås ulighederne,

$$\operatorname{depth}_{\mathfrak{p}} M = q + \operatorname{depth}_{\mathfrak{p}} M/(f_1, \dots, f_q) \leqslant q + \operatorname{ht} \mathfrak{p}/\mathfrak{q},$$

idet den første lighed fås af Korollar (2.9) og den anden ulighed af Dybde-uligheden (2.14). Heraf fremgår, at højresiden i (4.2.1) også er større end eller lig med venstresiden. Hermed er ligning (4.2.1) bevist.

(viii)$\Rightarrow$(ix): Lad $\mathfrak{p}$ være et primideal i R. Hvis $M_{\mathfrak{p}} = 0$, er påstanden klar. Antag altså, at $\mathfrak{p}$ tilhører støtten for M. Der findes da et primideal $\mathfrak{q} \subseteq \mathfrak{p}$ i støtten for M således at $\dim M_{\mathfrak{p}} = \operatorname{ht} \mathfrak{p}/\mathfrak{q}$. Forudsætningen (viii) medfører derfor, at

$$\dim M_{\mathfrak{p}} = \operatorname{ht} \mathfrak{p}/\mathfrak{q} = \operatorname{depth}_{\mathfrak{p}} M - \operatorname{depth}_{\mathfrak{q}} M \leqslant \operatorname{depth}_{\mathfrak{p}} M \leqslant \operatorname{depth} M_{\mathfrak{p}},$$

idet den sidste ulighed er triviel, jfr Bemærkning (2.11). Af Definition (3.2) fremgår nu, at $M_{\mathfrak{p}}$ er en Cohen–Macaulay modul.

(ix)$\Rightarrow$(i): Denne afsluttende implikation er triviel. $\square$

(4.3) Definition. Den endeligt frembragte R-modul M kaldes en *Cohen–Macaulay modul*, hvis de ækvivalente betingelser i Teorem (4.2) er opfyldt. Hvis ringen R, som modul over sig selv, er Cohen–Macaulay, kaldes ringen en *Cohen–Macaulay ring*.

For en lokal ring fremgår det af betingelsen (4.2)(i), at definitionen stemmer overens med Definition (3.2).

(4.4) Bemærkning. Et ideal $\mathfrak{a}$ i R siges at være 'unmixed', hvis alle associerede primidealer for $R/\mathfrak{a}$ har samme højde. Ækvivalent betyder det, at $R/\mathfrak{a}$ ikke har indlejrede primidealer og alle isolerede primidealer for $\mathfrak{a}$ har samme højde. For et ideal $R\mathbf{f}$ frembragt af en følge $\mathbf{f} = (f_1, \dots, f_r)$ med r elementer gælder ifølge Krull's Idealsætning, at ethvert isoleret primideal for idealet har højde højst r. Forudsættes at $\operatorname{ht}(R\mathbf{f}) = r$, så har altså ethvert isoleret primideal for $R\mathbf{f}$ højden r. Betingelsen (iv) udtrykker altså, at ethvert sådant ideal er 'unmixed', og den kaldes også 'unmixedness' betingelsen.

(4.5) Korollar. *Lad M være en Cohen–Macaulay modul. Da gælder:*

(0) *For alle primidealer $\mathfrak{p}$ i støtten for M er $M_\mathfrak{p}$ en Cohen-Macaulay modul over $R_\mathfrak{p}$ og* $\operatorname{depth}_\mathfrak{p} M = \operatorname{depth} M_\mathfrak{p} = \dim M_\mathfrak{p}$.

(1) *Modulen M har ingen indlejrede primidealer.*

(2) *Lad $(f_1, \dots, f_r)$ være en følge af elementer i R således at* $\operatorname{ht}_M(f_1, \dots, f_r) = r$ *(specielt kan følgen være en M-højdefølge, eller mere specielt en M-regulær følge). Da er $M/(f_1, \dots, f_r)M$ en Cohen–Macaulay modul.*

(3) *Modulen M er katernær, dvs at for enhver uforfinelig kæde af primidealer $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_h$ i støtten* $\operatorname{Supp} M$ *er* $h = \operatorname{ht} \mathfrak{p}_h/\mathfrak{p}_0$.

Bevis. Påstand (0) følger umiddelbart af at betingelserne (ix) og (vii) er opfyldt. Påstand (1) følger af betingelsen (iv), anvendt med $r = 0$.

(2): Sæt $\mathbf{f} := (f_1, \dots, f_r)$, og antag, at $\operatorname{ht}_M(\mathbf{f}R) = r$. Vi viser, at betingelsen (4.2)(i) er opfyldt for kvotienten $M/\mathbf{f}M$. Betragt hertil et maksimalideal $\mathfrak{m}$ i støtten for $M/\mathbf{f}M$. Det følger af betingelsen (4.2)(ii), at følgen $\mathbf{f}$ er $M_\mathfrak{m}$-regulær. Af Hovedsætning (3.3)(2) sluttes derfor, at kvotienten $M_\mathfrak{m}/\mathbf{f}M_\mathfrak{m}$ er Cohen–Macaulay over $R_\mathfrak{m}$. Denne sidste kvotient er lokaliseringen i $\mathfrak{m}$ af $M/\mathbf{f}M$. Altså er betingelsen (i) opfyldt for $M/\mathbf{f}M$.

(3): Denne påstand følger af ligningen (4.2.1). Antag nemlig, at følgen i (3) er uforfinelig. Da der ikke findes primidealer mellem $\mathfrak{p}_{i-1}$ og $\mathfrak{p}_i$, er $\operatorname{ht} \mathfrak{p}_i/\mathfrak{p}_{i-1} = 1$. Af (4.2.1) følger derfor, at $\operatorname{depth}_{\mathfrak{p}_i} M - \operatorname{depth}_{\mathfrak{p}_{i-1}} M = 1$. Ved addition af disse ligninger for $i = 1, \dots, h$ følger, at $\operatorname{depth}_{\mathfrak{p}_h} M - \operatorname{depth}_{\mathfrak{p}_0} M = h$, og fornyet anvendelse af (4.2.1) viser, at $\operatorname{ht} \mathfrak{p}_h/\mathfrak{p}_0 = h$. □

(4.6) Korollar. *Lad M være en Cohen–Macaulay modul, og antag yderligere, at M er co-equidimensional, dvs at for alle maksimalidealer $\mathfrak{m}$ i støtten for M er* $\dim M_\mathfrak{m} = \dim M$. *Da gælder:*

(1) *Modulen M er equidimensional, dvs opfylder, at for alle minimale primidealer $\mathfrak{q}$ for M er* $\dim R/\mathfrak{q} = \dim M$.

(2) *Lad* $\mathbf{f} = (f_1, \dots, f_r)$ *være en følge af r elementer i R således at* $\operatorname{ht}_M(\mathbf{f}R) = r$. *Da er $M/\mathbf{f}M$ (Cohen–Macaulay og) co-equidimensional, og* $\dim M/\mathbf{f}M = \dim M - r$.

(3) *For hvert ideal* $\mathfrak{a}$ *i* R *således at* $M/\mathfrak{a}M \neq 0$ *gælder ligningen,*

$$\operatorname{ht}_M \mathfrak{a} + \dim M/\mathfrak{a}M = \dim M.$$

Bevis. (1): Lad $\mathfrak{q}$ være et minimalt primideal for M, og betragt et maksimalideal $\mathfrak{m} \supseteq \mathfrak{q}$. Primidealet $\mathfrak{q}R_\mathfrak{m}$ er da minimalt primideal for modulen $M_\mathfrak{m}$. Da $M_\mathfrak{m}$ er en Cohen-Macaulay modul over $R_\mathfrak{m}$, følger det af Hovedsætning (3.3), at $\dim M_\mathfrak{m} = \operatorname{ht} \mathfrak{m}/\mathfrak{q}$. Altså er $\operatorname{ht} \mathfrak{m}/\mathfrak{q} = \dim M$. Heraf ses, at $\dim R/\mathfrak{q} = \dim M$.

(2): Kvotienten $M/\mathbf{f}M$ er Cohen–Macaulay ifølge Korollar (4.5)(2). Lad $\mathfrak{m}$ være et maksimalideal i støtten for $M/\mathbf{f}M$. Da betingelsen (4.2)(ii) gælder for M, er $\mathbf{f}$ en $M_\mathfrak{m}$-regulær følge. Da $M_\mathfrak{m}$ er Cohen–Macaulay ifølge (4.2)(i), følger det af Hovedsætning (3.3), at $\dim M_\mathfrak{m}/\mathbf{f}M_\mathfrak{m} = \dim M_\mathfrak{m} - r$. Da M er co-equidimensional, følger det at $M/\mathbf{f}M$ er co-equidimensional, af den i (2) angivne dimension.

(3): Højden $r := \operatorname{ht}_M(\mathfrak{a})$ er et infimum. Vælg blandt de minimale primidealer for $M/\mathfrak{a}M$ et primideal $\mathfrak{q}$ således at $\dim M_\mathfrak{q} = r$. Vælg videre en M-højdefølge $\mathbf{f} = (f_1, \dots, f_r)$ i $\mathfrak{a}$. Da $\operatorname{ht}_M(\mathbf{f}R) = r$ og $\dim M_\mathfrak{q} = r$, må primidealet $\mathfrak{q}$ være et minimalt primideal for $M/\mathbf{f}M$. Det følger af (2) og (1), at $M/\mathbf{f}M$ er equidimensional, så $\dim R/\mathfrak{q} = \dim M/\mathbf{f}M$, og videre følger det af (2), at $\dim M/\mathbf{f}M = \dim M - r$. Altså er $r + \dim R/\mathfrak{q} = \dim M$. Heraf følger, at $r + \dim M/\mathfrak{a}M \geqslant \dim M$, og da den modsatte ulighed er triviel, gælder den påståede lighed. □

(4.7) Bemærkning. Hvis ringen R er lokal, så er naturligvis enhver R-modul co-equidimensional. I dette tilfælde svarer påstandene (4.5)(1) og (4.6)(1) til påstand (1) i Hovedsætning (3.3), og påstand (4.6)(2) svarer til påstand (2) i Hovedsætning (3.3). Bemærk imidlertid, at påstand (3) i Hovedsætning (3.3) i almindelighed ikke gælder, når ringen ikke er lokal. Fx har vi i Bemærkning (1.5) betragtet polynomiumsringen $R = k[X, Y, Z]$ og den regulære følge (f_1, f_2, f_3) i maksimalidealet $\mathfrak{M} = (X, Y, Z)$. Som bekendt er R co-equidimensional af dimension 3, og vi viser herunder, at R er en Cohen–Macaulay ring. Det er klart, at $\dim R/(f_1, f_2, f_3) = 0$ (ifølge (4.6)(2), eller direkte: det er klart, at $(f_1, f_2, f_3) = \mathfrak{M}$). Men følgen (f_1, f_3, f_2) er ikke regulær.

(4.8) Sætning. *Antag, at* R *er en Cohen-Macaulay ring. Da er også polynomiumsringen* $R[X]$ *en Cohen-Macaulay ring.*

Bevis. Betragt et maksimalideal $\mathfrak{M}$ i $R[X]$, og lad $\mathfrak{p} := R \cap \mathfrak{M}$ være kontraktionen. Det skal vises, at den lokale ring $R[X]_\mathfrak{M}$ er en Cohen-Macaulay ring. Denne lokale ring fås ved lokalisering af $R_\mathfrak{p}[X]$ i primidealet svarende til $\mathfrak{M}$. Yderligere følger det af forudsætningen, at $R_\mathfrak{p}$ er en Cohen-Macaulay ring. Idet vi om fornødent erstatter R med $R_\mathfrak{p}$ kan vi derfor antage, at R er lokal og at kontraktionen $\mathfrak{p}$ er maksimalidealet $\mathfrak{m}$ i R. Sæt $h := \dim R$. Det er da velkendt, at $\mathfrak{M} \supset \mathfrak{m}[X]$ og at $\operatorname{ht} \mathfrak{M} = h + 1$. Yderligere er $\mathfrak{M}/\mathfrak{m}[X]$ et maksimalideal i polynomiumsringen $(R/\mathfrak{m})[X]$, og altså (da $R/\mathfrak{m}$ er et legeme) et hovedideal frembragt af et normeret polynomium. Specielt findes derfor i $\mathfrak{M}$ et normeret polynomium F.

Da R er Cohen-Macaulay, findes en R-regulær følge $\mathbf{f} = (f_1, \dots, f_h)$ i $\mathfrak{m}$. Det er klart, at et regulært element f i R, opfattet som (konstant) polynomium, er regulært i $R[X]$ og at

$R[X]/fR[X] = (R/fR)[X]$. Heraf ses, at følgen $\mathbf{f}$ er en $R[X]$-regulær følge, i idealet $\mathfrak{m}[X]$. Yderligere er det normerede polynomium F regulært på kvotienten $(R/\mathbf{f}R)[X]$. Følgen $(f_1, \dots, f_h, F)$ er altså en $R[X]$-regulær følge i $\mathfrak{M}$. Ved lokalisering fås en $R[X]_{\mathfrak{M}}$-regulær følge. Heraf ses, at depth $R[X]_{\mathfrak{M}} \geqslant h + 1$. Da $h + 1 = \operatorname{ht} \mathfrak{M} = \dim R[X]_{\mathfrak{M}}$, følger det, at $R[X]_{\mathfrak{M}}$ er en lokal Cohen-Macaulay ring. □

(4.9) Korollar. *Antag, at R er en Cohen-Macaulay ring. Da er også polynomiumsringen $R[X_1, \dots, X_n]$ en Cohen-Macaulay ring. Specielt er polynomiumsringen katernær.*

Bevis. Den første påstand følger af Sætningen ved induktion efter n. Den anden påstand er en konsekvens af den første, jfr Korollar (4.5)(4). □

(4.10) Lemma. *Lad R være et normalt integritetsområde, og lad $f \in R \setminus (0)$. Lad $\mathfrak{p}$ være et associeret primideal for R/fR. Da er maksimalidealet $\mathfrak{p}R_{\mathfrak{p}}$ i $R_{\mathfrak{p}}$ et hovedideal. Specielt er* $\operatorname{ht} \mathfrak{p} = 1$.

Bevis. Da R er normal, er det let at vise, at enhver lokalisering $S^{-1}R$, hvor $0 \notin S$, igen er normal. Efter lokalisering i $\mathfrak{p}$ kan vi derfor antage, at R er lokal og at $\mathfrak{p}$ er maksimalidealet i R. Ifølge antagelsen er $\mathfrak{p}$ associeret til R/fR. Specielt er $\mathfrak{p}$ altså indeholdt i annullatoren af en klasse forskellig fra 0 i R/fR. Der findes altså et element $a \in R$ så at $a \notin Rf$ og $\mathfrak{p}a \subseteq Rf$. Af den sidste inklusion fås inklusionen,

$$\mathfrak{p}(a/f) \subseteq R, \tag{1}$$

hvor venstresiden a priori er en undermodul i brøklegemet for R. Det påstås, at inklusionen er en lighed. Antag indirekte, at inklusionen er skarp. Da er venstresiden indeholdt i maksimalidealet $\mathfrak{p}$ i R, altså $\mathfrak{p}(a/f) \subseteq \mathfrak{p}$. Heraf fås successivt, at $\mathfrak{p}(a/f)^2 \subseteq \mathfrak{p}$, $\mathfrak{p}(a/f)^3 \subseteq \mathfrak{p}$ osv. Specielt er så $\mathfrak{p}(a/f)^n \subseteq R$ for alle n. Da $f \in \mathfrak{p}$, følger det, at $f(a/f)^n \subseteq R$ for alle n. For alle n er derfor $(a/f)^n$ indeholdt i R-modulen $R(1/f)$ frembragt af $1/f$. Følgelig er hele algebraen $R[a/f]$ indeholdt i $R(1/f)$. Da R er noethersk, sluttes videre, at $R[a/f]$ er endeligt frembragt som R-modul. Altså er a/f hel over R, og da R er antaget normal, må a være element i Rf. Dette er imidlertid i modstrid med antagelsen om a.

Vi har vist, at lighed gælder i inklusionen (1). Elementet 1 på højresiden tilhører altså venstresiden, så vi har $1 = p(a/f)$, hvor $p \in \mathfrak{p}$. Det følger nu let af inklusionen i (1), at $\mathfrak{p} = Rp$. Hermed er vist, at $\mathfrak{p}$ er et hovedideal, som ønsket. □

(4.11) Sætning. *En ring af dimension højst 0 er en Cohen–Macaulay ring. Et integritetsområde af dimension 1 er en Cohen–Macaulay ring. Et normalt integritetsområde af dimension 2 er en Cohen–Macaulay ring.*

Bevis. Betragt en (noethersk) ring R af dimension højst 2 og et primideal $\mathfrak{p}$ i R. Det skal vises, jfr betingelsen (4.2)(vii), under de respective forudsætninger i de tre udsagn, at ligningen $\operatorname{depth}_{\mathfrak{p}} R = \operatorname{ht} \mathfrak{p}$ er opfyldt.

Hvis $\operatorname{ht} \mathfrak{p} = 0$ er ligningen nødvendigvis opfyldt (og hermed er den første påstand bevist). Hvis $\operatorname{ht} \mathfrak{p} = 1$, forudsættes at R er et integritetsområde, og så er ligningen opfyldt, idet ethvert element $f \neq 0$ i $\mathfrak{p}$ er R-regulært.

Antag endelig, at $\operatorname{ht}\mathfrak{p} = 2$. I dette tilfælde forudsættes, at R er et normalt integritetsområde. Vælg et element $f \neq 0$ i $\mathfrak{p}$. Da er f et R-regulært element. Af Lemma (4.10) følger, at hvert associeret primideal for R/fR har højde 1. Specielt kan $\mathfrak{p}$ ikke være indeholdt i foreningsmængden af de endelig mange associerede primidealer for R/fR. Der findes derfor et element $g \in \mathfrak{p}$, således at g er regulær på R/fR. Følgelig er $\operatorname{depth}_{\mathfrak{p}} R \geqslant 2$, og dermed er $\operatorname{depth}_{\mathfrak{p}} R = \operatorname{ht}\mathfrak{p}$. □

(4.12) Bemærkning. Det følger af Lemma (4.10), jfr beviset for Sætning (4.11), at et (noethersk) normalt integritetsområde opfylder betingelsen (S_2), hvor betingelsen (S_k) for $k = 1, 2, \dots$ er *Serre's betingelse:*

$$(S_k) \qquad \operatorname{depth} R_{\mathfrak{p}} \geqslant \inf\{k,\ \operatorname{ht}\mathfrak{p}\} \quad \text{for alle primidealer } \mathfrak{p}.$$

Det er i øvrigt værd at bemærke, at Lemma (4.10) medfører følgende resultat:

Lad R være et normal integritetsområde. Da gælder i brøklegemet for R følgende lighed:

$$R = \bigcap_{\operatorname{ht}\mathfrak{p}=1} R_{\mathfrak{p}}. \tag{4.12.1}$$

Bevis:. For en given brøk $\alpha = a/f$ betragtes delmængden af R:

$$\mathfrak{a} := \{r \in R \mid r\alpha \in R\}.$$

Det er let at se, at $\mathfrak{a}$ er et ideal i R. Øjensynlig er $\mathfrak{a} = R$, hvis og kun hvis $\alpha \in R$. Det påstås for et primideal $\mathfrak{p}$, at $\mathfrak{a} \not\subseteq \mathfrak{p}$, hvis og kun hvis $\alpha \in R_{\mathfrak{p}}$. Er nemlig $\alpha \in R_{\mathfrak{p}}$, så har vi $\alpha = b/s$ hvor $s \notin \mathfrak{p}$; øjensynlig er $s \in \mathfrak{a}$, og følgelig er $\mathfrak{a} \not\subseteq \mathfrak{p}$. Og er omvendt $s \in \mathfrak{a} \setminus \mathfrak{p}$, så er $\alpha = (s\alpha)/s$ en brøk i $R_{\mathfrak{p}}$.

Nu bemærkes først, at venstresiden i (4.12.1) øjensynlig er indeholdt i højresiden. For at vise ligheden betragtes en brøk $\alpha = a/f$ som ikke tilhører R. Det skal vises, at der findes et primideal $\mathfrak{p}$ af højde 1 således at $\alpha \notin R_{\mathfrak{p}}$.

Det følger af definitionen på $\mathfrak{a}$, at for $r \in R$ gælder, at $ra \in Rf$ hvis og kun hvis $r \in \mathfrak{a}$. Heraf ses, at multiplikation med a definerer en injektiv homomorfi $R/\mathfrak{a} \hookrightarrow R/fR$. Da $\alpha \notin R$, er $R/\mathfrak{a} \neq 0$. Vælg nu et associeret primideal $\mathfrak{p}$ for $R/\mathfrak{a}$. Specielt er da $\mathfrak{p} \supseteq \mathfrak{a}$. Af inklusionen $R/\mathfrak{a} \subseteq R/fR$ følger, at $\mathfrak{p}$ også er associeret til R/fR. Af Lemma (4.10) følger, at $\operatorname{ht}\mathfrak{p} = 1$. Da $\mathfrak{a} \subseteq \mathfrak{p}$ følger det, at $\alpha \notin R_{\mathfrak{p}}$.

Altså har $\mathfrak{p}$ den ønskede egenskab. Hermed er ligheden i (4.12.1) bevist. □

5. Graduerede Cohen–Macaulay ringe.

(5.1) Setup. I denne paragraf er k et legeme og R betegner polynomiumsringen $R = k[X_1, \dots, X_n]$. Med $\mathfrak{N}$ betegnes maksimalidealet $(X_1, \dots, X_n)$ i R. Polynomiumsringen er gradueret: $R = \bigoplus R_n$, hvor R_n er vektorrummet af homogene polynomier af grad n. Maksimalidealet $\mathfrak{N}$ er homogent, idet $\mathfrak{N} = \bigoplus_{n \geqslant 1} R_n$. Øjensynlig er ethvert homogent, ægte ideal indeholdt i $\mathfrak{N}$. Videre betegner M en endeligt frembragt gradueret R-modul.

Det er velkendt, at R er en Cohen–Macaulay ring af dimension n, og yderligere, at R er bi-equidimensional, dvs for enhver maksimal kæde af primidealer i R,

$$(0) = \mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \cdots \subset \mathfrak{P}_h,$$

er $h = n$. Specielt er R en katernær ring.

(5.2) Lemma. (1) *Et ægte homogent ideal $\mathfrak{P}$ i R er et primideal, når blot betingelsen,*

$$fg \in \mathfrak{P} \implies f \in \mathfrak{P} \vee g \in \mathfrak{P},$$

er opfyldt for homogene elementer f, g i R.

(2) *Ethvert ideal, der er maksimalt blandt annullatorerne* $\operatorname{Ann}(x)$, *hvor $x \neq 0$ er et homogent element i M, er et (homogent) primideal i R.*

Bevis. (1): Antag, at betingelsen i (1) gælder for homogene elementer i R. Det skal vises, at den gælder for alle elementer i R. Betragt hertil to elementer f, g, så at $f \notin \mathfrak{P}$ og $g \notin \mathfrak{P}$. Elementet f er summen af sine homogene led f_i. Der findes derfor homogene led f_i som ikke tilhører $\mathfrak{P}$. Lad f_n være det homogene led af størst mulig grad således at $f_n \notin \mathfrak{P}$. Lad tilsvarende g_m være det homogene led i g af størst mulig grad således at $g_m \notin \mathfrak{P}$. Det følger da af antagelsen, at $f_n g_m \notin \mathfrak{P}$. Betragt det homogene led af grad $n + m$ i fg, altså summen af produkter,

$$\sum_{i+j=n+m} f_i g_j.$$

I denne sum forekommer produktet $f_n g_m$, som ikke tilhører $\mathfrak{P}$. For alle de øvrige produkter $f_i g_j$ er enten $i > n$ eller $j > m$, så valgene af n og m sikrer, at alle øvrige produkter tilhører $\mathfrak{P}$. Heraf følger, at summen ikke tilhører $\mathfrak{P}$. Leddet af grad $n + m$ i fg tilhører altså ikke $\mathfrak{P}$. Da $\mathfrak{P}$ er antaget homogent, følger det at $fg \notin \mathfrak{P}$.

(2): Det er klart, at en annullator $\operatorname{Ann}(x)$ af et homogent element i M er et homogent ideal i R. Påstanden i (2) fås nu – under brug af (1) – ved at kopiere beviset for det tilsvarende resultat i det ikke-graduerede tilfælde. □

(5.3) Sætning. *Lad M være en endeligt frembragt gradueret modul. Da er alle associerede primidealer (og specielt alle minimale primidealer) for M homogene. Specielt er alle associerede primidealer indeholdt i maksimalidealet $\mathfrak{N}$.*

Bevis. Da R er noethersk, følger det af Lemma (5.2), at hvis $M \neq 0$ så findes associerede primidealer for M, der er homogene. Altså har M en homogen undermodul M_1, der (ikke-gradueret) er isomorf med en kvotient $R/\mathfrak{P}$, hvor $\mathfrak{P}$ er et homogent primideal. Ved at gentage argumentet på M/M_1 og fortsætte, ses, da M er noethersk, at der findes en endelig filtration,

$$(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r = M,$$

med homogene undermoduler M_i, hvor de successive kvotienter M_i/M_{i-1} har formen $R/\mathfrak{P}_i$, hvor $\mathfrak{P}_i$ er et homogent primideal. Det er velkendt, at hvert associeret primideal for M må være et af $\mathfrak{P}_i$'erne. Hermed er Sætningen bevist. ∎

(5.4) Bemærkning. Som bekendt er $\dim M = 0$, hvis og kun hvis M har endelig længde, altså hvis og kun hvis alle minimale primidealer for M er maksimalidealer i R. Da de minimale primidealer ifølge Sætning (5.3) er homogene og dermed indeholdt i $\mathfrak{N}$, indtræffer dette netop når $\mathfrak{N}$ er det eneste primideal, der indeholder $\operatorname{Ann} M$, altså netop når $\operatorname{Ann} M$ indeholder en potens af $\mathfrak{N}$. Ækvivalent betyder dette, at hvert X_i er nilpotent på M (eller at $M_n = 0$ når $n \gg 0$).

(5.5) Korollar. *Lad M være en endeligt frembragt gradueret modul over polynomiumsringen $R = k[X_1, \dots, X_n]$. Da er $\dim M = \dim M_{\mathfrak{N}}$, hvor $\mathfrak{N}$ er det homogene maksimalideal i R. Yderligere gælder, at M er bi-equidimensional, når blot M er equidimensional (eller $M_{\mathfrak{N}}$ er equidimensional).*

Bevis. Hvis $M = 0$, er påstandene trivielle. Antag, at $M \neq 0$, og betragt en maksimal kæde i støtten for M,

$$\mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \cdots \subset \mathfrak{P}_h. \tag{*}$$

I kæden er $\mathfrak{P}_0$ et minimalt primideal for M og $\mathfrak{P}_h$ er et maksimalideal i R. Da R er bi-equidimensional, er $h = \dim R/\mathfrak{P}_0$. Blandt de minimale primidealer for M findes et primideal $\mathfrak{P}_0$ således at $\dim R/\mathfrak{P}_0 = \dim M$. Ifølge Sætning (5.3) er $\mathfrak{P}_0$ et homogent primideal, og dermed indeholdt i det homogene maksimalideal $\mathfrak{N}$. Der findes derfor en maksimal kæde (*), hvor $\mathfrak{P}_h = \mathfrak{N}$. Heraf fås, at $\dim M_{\mathfrak{N}} \geqslant h = \dim R/\mathfrak{P}_0 = \dim M$. Trivielt er $\dim M_{\mathfrak{N}} \leqslant \dim M$, og denne ulighed er altså en lighed.

Antag nu, at $M_{\mathfrak{N}}$ er equidimensional. Lad $\mathfrak{P}_0$ være et minimalt primideal for M. Da er $\mathfrak{P}_0$ homogent, og altså indeholdt i $\mathfrak{N}$, så antagelsen betyder, at der findes en kæde (*) med $\mathfrak{P}_h = \mathfrak{N}$ og $h = \dim M_{\mathfrak{N}}$. Ifølge det lige viste, er $h = \dim R/\mathfrak{P}_0$ og $\dim M_{\mathfrak{N}} = \dim M$. Altså er $\dim R/\mathfrak{P}_0 = \dim M$. Følgelig er M equidimensional. Ligningen $h = \dim R/\mathfrak{P}_0$ for enhver maksimal kæde (*) viser nu, at M er bi-equidimensional.

Hermed er Korollaret bevist. ∎

(5.6) Hovedsætning. *Lad M være en endeligt frembragt gradueret modul over polynomiumsringen $R = k[X_1, \dots, X_n]$. Antag, at M er en Cohen–Macaulay modul og $M \neq 0$. Da er M bi-equidimensional. Videre er for enhver følge $\mathbf{f} = (f_1, \dots, f_r)$ af homogene elementer af positiv grad følgende betingelser ækvivalente:*

(i) *Følgen $\mathbf{f}$ er M-regulær.*
(ii) $\operatorname{ht}_M(\mathbf{f}R) = r$.
(iii) $\dim M/\mathbf{f}M = \dim M - r$.

Bevis. Da M er en Cohen–Macaulay modul er også $M_{\mathfrak{N}}$ en Cohen–Macaulay modul over den lokale ring $R_{\mathfrak{N}}$. Af Hovedsætning (3.3) følger så, at $M_{\mathfrak{N}}$ er equidimensional. Af Korollar (5.5) følger derfor, at M er bi-equidimensional.

Betragt nu en følge $\mathbf{f} = (f_1, \dots, f_r)$ af homogene elementer af positiv grad. En M-regulær følge er en M-højdefølge ifølge Sætning (2.10), så specielt gælder (i)⇒(ii). Da M er bi-equidimensional er M specielt co-equidimensional, så (ii)⇒(iii) følger af Korollar (4.6)(2).

Endelig skal vi vise, at (iii)⇒(i). Dette vises ved induktion efter r. Vi bemærker først, at hvis $N \neq 0$ er endeligt frembragt gradueret R-modul, og f er et homogent element af positiv grad, så gælder ulighederne,

$$\dim N - 1 \leqslant \dim N/fN \leqslant \dim N.$$

De tilsvarende uligheder gælder nemlig for moduler over en lokal ring, og vi har vist i Korollar (5.5) at dimensionerne ikke ændres når N erstattes med $N_{\mathfrak{N}}$.

Af denne bemærkning følger, at ligningen forudsat i (iii) medfører begge ligningerne,

$$\dim M/f_1M = \dim M - 1, \qquad \dim M'/(f_2, \dots, f_r)M' = \dim M' - (r-1),$$

hvor $M' = M/f_1M$. Af den første ligning følger, at f_1 ikke tilhører de primidealer $\mathfrak{Q}$ i støtten for M for hvilket $\dim R/\mathfrak{Q} = \dim M$. Nu var M equidimensional, og ifølge Korollar (4.5)(1) har M ingen indlejrede primidealer. Altså kan f_1 ikke tilhøre et associeret primideal for M. Følgelig er f_1 regulær på M. Korollar (4.5)(2) medfører så, at $M' = M/f_1M$ er en Cohen–Macaulay modul. Den anden ligning ovenfor medfører derfor (induktivt), at $(f_2, \dots, f_r)$ er en M'-regulær følge. Altså er $(f_1, \dots, f_r)$ en M-regulær følge.

Hermed er ækvivalensen vist, og beviset afsluttet. ▯

(5.7) Definition. Udover polynomiumsringen $R = k[X_1, \dots, X_n]$ betragtes polynomiumsringen $R^h := k[X_0, \dots, X_n]$ i $n+1$ variable. Lad $f \in R$ være et polynomium forskelligt fra 0, og lad d være graden af f. Polynomiet f er en sum af sine homogene led, $f = \sum_{j \leqslant d} f_j$, og leddet f_d af højeste grad er forskelligt fra 0. Vi betegner det $f^{\max}$; det er et homogent polynomium af grad d. Ved det til f hørende *homogeniserede* polynomium forstås polynomiet

$$f^h := X_0^d f_0 + X_0^{d-1} f_1 + \dots + f_d.$$

Polynomiet f^h er et homogent polynomium af grad d i ringen R^h. Øjensynlig er

$$f^h(1, X_1, \dots, X_n) = f \quad \text{og} \quad f^h(0, X_1, \dots, X_n) = f^{\max}.$$

(5.8) Bezout's Sætning. *Lad $(f_1, \dots, f_n)$ være en følge af n ikke-konstante polynomier i $k[X_1, \dots, X_n]$, og betragt kvotienten $\Gamma := k[X_1, \dots, X_n]/(f_1, \dots, f_n)$. Antag om de homogene led $f_i^{\max}$, at kvotienten $k[X_1, \dots, X_n]/(f_1^{\max}, \dots, f_n^{\max})$ har dimension 0. Da er*

$$\dim_k \Gamma = (\deg f_1) \cdots (\deg f_n). \tag{5.8.1}$$

Bevis. Homomorfien $R^h \to R$, defineret ved $F \mapsto F(0, X_1, \dots, X_n)$, er surjektiv med kernen (X_0). Den afbilder f_i^h på $f_i^{\max}$, og inducerer derfor en isomorfi,

$$R^h/(f_1^h, \dots, f_n^h, X_0) \xrightarrow{\sim} R/(f_1^{\max}, \dots, f_n^{\max}).$$

Ifølge forudsætningen er højresiden af dimension 0. Af Hovedsætning (5.6) fremgår derfor, at $(f_1^h, \dots, f_n^h, X_0)$ er en regulær følge i R^h. Følgen $(f_1^h, \dots, f_n^h)$ er altså en regulær følge i R^h og i kvotienten $\Gamma^h := R^h/(f_1^h, \dots, f_n^h)$ er billedet x_0 af X_0 et regulært element. Bemærk, at kvotienten Γ^h er en gradueret ring og x_0 er homogen af grad 1.

Betragt nu homomorfien $R^h \to R$, defineret ved $F \mapsto F(1, X_1, \dots, X_n)$. Den er surjektiv med kernen $(X_0 - 1)$, og den afbilder f_i^h på f_i. Den inducerer derfor en en surjektiv homomorfi af $\varphi \colon \Gamma^h \to \Gamma$, med kernen $(x_0 - 1)$. Ved restriktion fås for hvert j en k-lineær homomorfi,

$$\varphi_j : \Gamma_j^h \to \Gamma.$$

Ligningen (5.8.1) er øjensynlig en konsekvens af følgende 3 påstande: (1) Billederne ved homomorfierne φ_j udgør en stigende følge af underrum i Γ og deres foreningsmængde er hele Γ. (2) Homomorfierne φ_j er injektive. (3) Når $j \gg 0$ er $\dim_k \Gamma_j^h$ konstant og lig med højresiden i (5.8.1).

Påstand (1) er triviel: elementet x_0 er homogent af grad 1 og $\varphi x_0 = 1$. For $\alpha \in \Gamma_j^h$ gælder altså ligningen $\varphi_j \alpha = \varphi_{j+1}(x_0\alpha)$, og den viser, at billedet af φ_j er indeholdt i billedet af φ_{j+1}. Da homomorfien $\varphi \colon \Gamma^h \to \Gamma$ er surjektiv, er Γ summen af disse billeder, og da billederne udgør en stigende følge, er Γ lig med foreningen af billederne.

Påstand (2) vises således: Antag, at der findes et element $\alpha \neq 0$ i kernen for φ_j. Elementet α er altså et homogent element af grad j i Γ^h og der findes en ligning,

$$\alpha = \gamma(x_0 - 1),$$

hvor γ tilhører Γ^h. Da $\alpha \neq 0$ er $\gamma \neq 0$. Lad γ_c og γ_d være de homogene led af laveste og højeste grad i γ. På ligningens højreside er det homogene led af laveste grad så $-\gamma_c$; da x_0 er regulær i Γ^h, er det homogene led af højeste grad lig med $\gamma_d x_0$. Disse to led på højresiden har graderne c og $d+1$. Da de to grader er forskellige, er dette i modstrid med at venstresiden α er homogen.

Påstand (3) vises således: Dimensionen $\dim_k \Gamma_j^h$ er, når $j \gg 0$, givet ved Hilbert-polynomiet af kvotienten $\Gamma^h = R^h/(f_1^h, \dots, f_n^h)$. Ringen R^h er polynomiumsringen i $n+1$ variable, og dens Hilbert-polynomium har derfor graden n og multipliciteten 1. Da følgen $(f_1^h, \dots, f_n^h)$ er en regulær følge i R^h, er det let at bestemme Hilbert-polynomiet for kvotienten. Det bliver konstanten givet ved højresiden i (5.8.1).

Hermed er de tre påstande, og dermed ligning (5.8.1), bevist. □

(5.10) Bemærkning. Kvotienten $\Gamma = R/(f_1, \dots, f_n)$ definerer som bekendt et skema X i $\mathbf{A}^n$. Under forudsætningen i Bezout's sætning er $\dim_k \Gamma$ specielt endelig, så X er et endeligt skema. Af bemærkning (5.4) fremgår en række betingelser, som er ækvivalente med forudsætningen om at $\dim R/(f_1^{\max}, \dots, f_n^{\max}) = 0$. Uden at vi her kan gå nærmere ind på det, skal det nævnes at denne forudsætning for Bezout's Sætning svarer til at skemaet X ikke har uendelige fjerne punkter.

Regulære ringe

1. Regulære lokale ringe.

(1.1) Setup. I denne paragraf betegner R en lokal noethersk ring med maksimalidealet $\mathfrak{m}$, og M betegner en endeligt frembragt R-modul.

(1.2) Definition. Vi minder om, at dimensionen af R er lig med det mindste antal elementer i $\mathfrak{m}$ som frembringer et $\mathfrak{m}$-primært ideal, dvs et ideal $\mathfrak{q}$ således at $R/\mathfrak{q}$ har endelig længde. Ifølge Nakayama's Lemma er det minimale antal frembringere for $\mathfrak{q}$ lig med dimensionen af $\mathfrak{q}/\mathfrak{m}\mathfrak{q}$ som vektorrum over restklasselegemet $k := R/\mathfrak{m}$. Specielt gælder altså uligheden,

$$\dim R \leqslant \operatorname{rk} \mathfrak{m}/\mathfrak{m}^2,$$

hvor højresiden er vektorrumsdimensionen.

Den lokale ring R siges at være en *regulær lokal ring*, hvis lighedstegn gælder i uligheden ovenfor, altså hvis der findes et sæt af $d = \dim R$ elementer, der frembringer maksimalidealet $\mathfrak{m}$. Et sådant sæt af elementer siges også at være et *regulært parametersystem* for R.

(1.3) Observation. En lokal ring R af dimension 0 er regulær, hvis og kun hvis den er et legeme. Da dimensionen d er 0, udtrykker regularitetsbetingelsen nemlig at maksimalidealet $\mathfrak{m}$ kan frembringes af ingen elementer, dvs at $\mathfrak{m} = (0)$, eller ækvivalent, at R er et legeme.

(1.4) Sætning. *En lokal ring R med maksimalideal $\mathfrak{m}$ og restklasselegeme $k := R/\mathfrak{m}$ er regulær, hvis og kun hvis den graduerede ring*

$$G_{\mathfrak{m}}(R) := R/\mathfrak{m} \oplus \mathfrak{m}/\mathfrak{m}^2 \oplus \mathfrak{m}^2/\mathfrak{m}^3 \oplus \cdots,$$

er gradueret isomorf med en polynomiumsring $k[X_1, \dots, X_d]$ (nødvendigvis i $d = \dim R$ variable).

Bevis. „Kun hvis“: Lad $(x_1, \dots, x_d)$ være et regulært parametersystem i R, hvor altså $d = \dim R$ og $\mathfrak{m} = (x_1, \dots, x_d)R$. Restklasserne af x_i modulo $\mathfrak{m}^2$ er homogene elementer af grad 1 i $G_{\mathfrak{m}}(R)$, og disse d restklasser definerer en homomorfi,

$$G := k[X_1, \dots, X_d] \to G_{\mathfrak{m}}(R).$$

Øjensynlig er denne homomorfi surjektiv. For at vise, at den er bijektiv, antages indirekte, at den ikke er injektiv. Kernen er da et homogent ideal $I = \bigoplus I_n$ forskelligt fra 0 i polynomiumsringen G. Lad $F \neq 0$ være et homogent polynomium i I. Polynomiet F kan ikke være konstant, så graden h af F er positiv (og specielt er altså $d > 0$). Da $F \in I_h$ er $G_{n-h}F \subseteq I_n$ for alle n. Nu fås for $n \geqslant h$ vurderingen,

$$0 \leqslant \operatorname{rk} \mathfrak{m}^n/\mathfrak{m}^{n+1} \leqslant \binom{n+d-1}{d-1} - \binom{n-h+d-1}{d-1}.$$

Vektorrummet $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ på venstresiden er nemlig isomorft med G_n/I_n (da homomorfien var surjektiv), og det er derfor isomorf med en kvotient af G_n/FG_{n-h}. Rangen på venstresiden er altså mindre end eller lig med lig med rangen af G_n/F_hG_{n-h}. Den sidste rang er differensen $\operatorname{rk} G_n - \operatorname{rk} G_{n-h}$ og dermed lig med differensen på højresiden.

Det er klart, at differensen på vurderingens højreside er polynomial af grad mindre end $d-1$. Dette er i modstrid med at venstresiden ifølge teorien om Samuel-polynomier er polynomial af grad lig med $\dim R - 1 = d - 1$. Hermed er „kun hvis" bevist.

„hvis": Antag, at $G_\mathfrak{m}$ er gradueret isomorf med en polynomiumsring G i r variable. Da er specielt vektorrummet $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ isomorft med vektorrummet G_i af homogene polynomier af grad i. Længden af $R/\mathfrak{m}^n$, der er summen af dimensionerne af $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ for $i = 0, \dots, n$, er derfor lig med dimensionen af vektorrummet af polynomier af grad mindre end n. Dette sidste vektorrum har som bekendt dimensionen $\binom{n+r-1}{r}$. Funktionen $n \mapsto \operatorname{long} R/\mathfrak{m}^n$ er altså lig med polynomiet $\binom{n+r-1}{r}$, og funktionens grad er således lig med r. På den anden side følger det af teorien for Samuel-polynomier, at funktionens grad er $\dim R$. Altså er $r = \dim R$. Da $\mathfrak{m}/\mathfrak{m}^2$ er isomorf med G_1, følger yderligere, at $\operatorname{rk} \mathfrak{m}/\mathfrak{m}^2 = \operatorname{rk} G_1 = \dim R$. Altså er R regulær. □

(1.5) Bemærkning. Ved *Samuel-polynomiet* for den lokale ring R forstås polynomiet $\chi = \chi_{\mathfrak{m},R}$, altså det polynomium, der er bestemt ved ligningen,

$$\chi(n) = \operatorname{long} R/\mathfrak{m}^n \quad \text{for } n \gg 0. \tag{1.5.1}$$

Som bekendt har χ graden $d = \dim R$, og χ har formen $e\binom{n}{d} + \cdots + e_0$. Koefficienten $e = e_\mathfrak{m}(R)$ kaldes *multipliciteten* af den lokale ring R.

Længden på højresiden i (1.5.1) fås ved at anvende summationsoperatoren Σ på funktionen $n \mapsto \operatorname{rk} \mathfrak{m}^n/\mathfrak{m}^{n+1}$. Hvis R er regulær, er denne sidste funktion bestemt ved isomorfien i Sætning (1.4). Det følger, jfr beviset for Sætning (1.4), at højresiden af (1.5.1) for $n \geqslant 0$ er lig lig med $\binom{n+d-1}{d}$. En regulær lokal ring af dimension d har altså funktionen $\binom{n+d-1}{d}$ som Samuelpolynomium, og den har specielt multipliciteten 1.

For de lokale ringe, man møder i klassisk algebraisk geometri, gælder omvendt, at hvis multipliciteten er lig med 1, så er ringen regulær. Men dette resultat gælder ikke for generelle (noetherske) lokale ringe.

(1.6) Korollar. *En regulær lokal ring er et integritetsområde.*

Bevis. Betragt den dalende følge af idealer,

$$R = \mathfrak{m}^0 \supseteq \mathfrak{m}^1 \supseteq \mathfrak{m}^2 \supseteq \cdots .$$

Ifølge Krull's Snitsætning er $\bigcap_n \mathfrak{m}^n = (0)$. For hvert element $a \neq 0$ i R findes derfor et størst muligt n, således at $a \in \mathfrak{m}^n$. Dette tal siges også at være a's *orden*. Idet n er ordenen af a, betegnes med a^* restklassen i $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ af a modulo $\mathfrak{m}^{n+1}$. Denne restklasse er et homogent element af grad n i den graduerede ring $G := G_\mathfrak{m}(R)$, og valget af n sikrer, at $a^* \neq 0$.

For at vise, at R er et integritetsområde, skal det vises, at nul-reglen gælder i R. Hertil betragtes to elementer $a \neq 0$ og $b \neq 0$ i R. Det skal vises, at $ab \neq 0$. Antag, at n og m er ordenerne af a og b. Produktet ab ligger da i $\mathfrak{m}^{n+m}$, og ifølge konstruktionen af G er produktet ab en repræsentant for produktet a^*b^* i den graduerede ring G. Ifølge Sætningen er G er polynomiumsring over et legeme. Specielt er G et integritetsområde. Da nul-reglen således gælder i G, er $a^*b^* \neq 0$. Produktet ab i $\mathfrak{m}^n$ repræsenterer derfor modulo $\mathfrak{m}^{n+1}$ en klasse som ikke er nul-klassen. Specielt er $ab \neq 0$. □

(1.7) Korollar. *Antag, at R er regulær lokal med maksimalideal $\mathfrak{m}$. Lad $(f_1, \dots, f_d)$ være et regulært parametersystem (hvor altså $d = \dim R$). Da er følgen $(f_1, \dots, f_d)$ en R-regulær følge. Yderligere gælder for $i = 1, \dots, d$, at idealet $(f_1, \dots, f_i)$ er et primideal, og at kvotientringen,*

$$\overline{R} := R/(f_1, \dots, f_i),$$

er en regulær lokal ring af dimension $d - i$. Er omvendt $\mathfrak{a} \subseteq \mathfrak{m}$ et ideal, således at kvotienten $\overline{R} = R/\mathfrak{a}$ er regulær, så er $\mathfrak{a}$ frembragt af $i = d - \dim \overline{R}$ elementer $(f_1, \dots, f_i)$, som kan suppleres til et regulært parametersystem.

Bevis. Betragt først et regulært parametersystem $(f_1, \dots, f_d)$. Frembringeren f_1 kan ikke undværes, så specielt er $f_1 \neq 0$. Da R er et integritesområde ifølge det foregående korollar, er f_1 regulær. Heraf følger, at kvotienten $\overline{R} := R/(f_1)$ er af dimension $d - 1$. Maksimalidealet $\overline{\mathfrak{m}}$ i $\overline{R}$ er øjensynlig frembragt af de $d - 1$ restklasser $\overline{f}_2, \dots, \overline{f}_d$. Følgelig er $\overline{R}$ regulær af dimension $d - 1$ og af korollar (1.6) følger, at (f_1) er et primideal. Det er herefter klart, at Korollarets to første påstande følger ved induktion efter d.

Antag omvendt, at $\overline{R} := R/\mathfrak{a}$ er regulær. Sæt $s := \dim \overline{R}$. Da kan maksimalidealet $\overline{\mathfrak{m}}$ i $\overline{R}$ frembringes af restklasserne $\overline{g}_j$ af s elementer $g_1, \dots, g_s$ i $\mathfrak{m}$. Øjensynlig har vi en eksakt følge af vektorrum over $R/\mathfrak{m}$:

$$0 \longrightarrow (\mathfrak{a} + \mathfrak{m}^2)/\mathfrak{m}^2 \longrightarrow \mathfrak{m}/\mathfrak{m}^2 \longrightarrow \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 \longrightarrow 0.$$

Vektorrummet i midten har dimension d og vektorrummet til højre har dimension s. De s restklasser af g_j modulo $\mathfrak{m}^2$ afbildes på en basis for vektorrummet på højresiden. Følgelig kan disse s restklasser suppleres med en basis for kernen til en basis for vektorrummet i midten. Der findes altså $i = d - s$ elementer $f_1, \dots, f_i$ i $\mathfrak{a}$, hvis restklasser modulo $\mathfrak{m}^2$ suppleret med restklasserne af g_j'erne udgør en basis for $\mathfrak{m}/\mathfrak{m}^2$. Følgen $(f_1, \dots, f_i, g_1, \dots, g_s)$ af $i + s$ elementer vil derfor frembringe $\mathfrak{m}$. Da $i + s = \dim R$, er denne følge endda et regulært parametersystem. Ifølge valget er $(f_1, \dots, f_i) \subseteq \mathfrak{a}$, så ringen $R/\mathfrak{a}$ er en kvotient af $R/(f_1, \dots, f_i)$. Ifølge det først viste er $R/(f_1, \dots, f_i)$ et integritetsområde, og af samme dimension $d - i = s$ som $R/\mathfrak{a}$. Heraf følger, at kvotienten $R/\mathfrak{a}$ må være lig med $R/(f_1, \dots, f_i)$, altså at $\mathfrak{a} = (f_1, \dots, f_i)$.

Hermed er også den anden halvdel af korollaret bevist. □

(1.8) Korollar. *En regulær lokal ring er en Cohen-Macaulay ring.*

Bevis. Påstanden følger umiddelbart af den første påstand i Korollar (1.7). ◻

(1.9) Lemma. *Lad A være et integritetsområde med brøklegemet K. Hvis en brøk α i K er hel over A, så findes et element $s \neq 0$ i A, således at $s\alpha^p \in A$ for alle p. Hvis A er noethersk, så gælder også „kun hvis".*

Bevis. Antag, at α er hel over A. Delalgebraen $M := A[\alpha]$ af K er da endeligt frembragt som A-modul. Hvis M er frembragt af endelig mange brøker, så vil en fælles nævner s for disse brøker øjensynlig opfylde, at $sM \subseteq A$. Da M indeholder alle potenser af α, gælder specielt, at $s\alpha^p \in A$ for alle p.

Antag omvendt, at $s\alpha^p \in A$ for alle p. Da er algebraen $A[\alpha]$ indeholdt i A-modulen $A(1/s)$. Den sidste modul er, som A-modul, isomorf med A. Hvis A er noethersk, sluttes derfor, at undermodulen $A[\alpha]$ er endeligt frembragt, og dermed at α er hel over A. ◻

(1.10) Sætning. *En regulær lokal ring R er normal.*

Bevis. Antag, at den lokale ring R er regulær. Ifølge Korollar (1.6) er R et integritetsområde. Ifølge Sætning (1.4) er den graduerede ring $G = G_{\mathfrak{m}}(R)$ isomorf med en polynomiumsring over et legeme. Specielt er G normal, da polynomiumsringen er faktoriel. Desuden er G noethersk ifølge Hilbert's Basissætning.

Vi viser, at normaliteten af G medfører, at R er normal. Betragt hertil en brøk a/s, som er hel over R. Det skal vises, at brøken tilhører R, altså at $a \in sR$. Det er nok at vise for alle n, at

$$a \in sR + \mathfrak{m}^n, \quad \text{altså at } a = sx + b \text{ hvor } x \in R,\ b \in \mathfrak{m}^n. \tag{1}$$

Da vil nemlig restklassen af a i $M := R/sR$ tilhøre $\mathfrak{m}^n M$ for alle n, og af Krull's Snitsætning følger så, at restklassen er nul, altså at $a \in sR$.

Relationen (1) vises ved induktion efter n. Den er trivielt opfyldt for $n = 0$. Antag, at (1) er vist for n. Det er nok at vise, at

$$b \in sR + \mathfrak{m}^{n+1}, \tag{2}$$

thi så er $b = ys + c$ med $c \in \mathfrak{m}^{n+1}$, og dermed $a = (x + y)s + c \in sR + \mathfrak{m}^{n+1}$.

Vi har antaget, at $b \in \mathfrak{m}^n$. Hvis $b \in \mathfrak{m}^{n+1}$, er (2) trivielt opfyldt. Vi antager derfor, at $b \notin \mathfrak{m}^{n+1}$. Idet vi anvender notationen fra beviset for Korollar (1.6) har b altså orden n. Nu er $b/s = a/s - x$, og da a/s er hel over R er også b/s hel over R. Af Lemma (1.9) anvendt med $A := R$ følger, at der findes $t \neq 0$ i R således at $tb^p \in s^pR$ for alle p. Af disse ligninger i R følger i G, at $t^*(b^*)^p \in (s^*)^pG$ for alle p. Da G er noethersk, fås af den anden halvdel af Lemma (1.9) anvendt med $A := G$, at b^*/s^* er hel over G. Da G er normal følger, at b^*/s^* tilhører G. Altså findes et element $y \neq 0$ i R således at $b^* = s^*y^*$. Elementet b havde orden n, så ligningen $b^* = s^*y^*$ i G viser, at b er kongruent med sy modulo $\mathfrak{m}^{n+1}$. Altså er (2) opfyldt.

Hermed er det ønskede bevist. ◻

(1.11) Korollar. *For en lokal noethersk ring R er følgende betingelser ækvivalente:*

(i) *R er en diskret valuationsring.*
(ii) *R er regulær af dimension* 1.
(iii) *R er et normalt integritetsområde af dimension* 1.

Bevis. (i)⇔(ii): Det er et velkendt resultat, at en diskret valuationsring er karakteriseret som en noethersk lokal ring, der er et integritetsområde og ikke et legeme, hvori maksimalidealet er et hovedideal. Da en regulær lokal ring er et integritetsområde ifølge Korollar (1.6), følger ækvivalensen af (i) og (ii).

(ii)⇒(iii) følger umiddelbart af Sætningen.

(iii)⇒(i): Antag, at R er et normalt integritetsområde af dimension 1. Da dimensionen er positiv, er $\mathfrak{m} \neq (0)$, og da dimensionen er lig med 1, er $\mathfrak{m}$ isoleret primideal for hovedidealet (f) frembragt af et vilkårligt element $f \neq 0$ i $\mathfrak{m}$. Specielt er $\mathfrak{m}$ associeret til $R/(f)$. Heraf følger, som det er velkendt fra kapitlet om dybde, at $\mathfrak{m}$ er et hovedideal. Følgelig er R regulær.

Hermed er ækvivalensen bevist. □

(1.12) Bemærkning. Antag, at den lokale ring R er regulær. Da gælder, at R er en faktoriel ring (Auslander–Buchsbaum's Sætning). Desuden gælder for hvert primideal $\mathfrak{p}$ i R, at den lokale ring $R_{\mathfrak{p}}$ er regulær. Begge disse resultater vises naturligt ved homologisk algebra. Vi skal senere skitsere dele af et bevis for det første resultat.

2. Regulære ringe.

(2.1) Definition. Som sædvanlig betegner R overalt i det følgende en noethersk ring. Ringen R siges at være en *lokalt regulær ring*, hvis der for alle primidealer $\mathfrak{p}$ i R gælder, at den lokale ring $R_{\mathfrak{p}}$ er regulær.

(2.2) Bemærkning. Det er et fundamentalt resultat, som vi ikke kan bevise her, at en lokal ring, der er regulær ifølge Definition (1.2), er lokalt regulær ifølge definition ovenfor.

Heraf ses, at det i definitionen ovenfor er nok at kræve, at den lokale ring $R_{\mathfrak{m}}$ er regulær for alle maksimalidealer i R. Desuden ses, at „lokalt" i Definition (2.1) egentligt er overflødigt. Vi kunne blot have sagt „regulær". Det skal imidlertid understreges, at en regulær ring i litteraturen ofte antages at have endelig Krull dimension.

(2.3) Sætning. *Lad R være en lokalt regulær ring. Da gælder:*

(1) *R er et endeligt produkt af lokalt regulære integritetsområder.*
(2) *R er en Cohen–Macaulay ring.*

Bevis. (1) Lad $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ være de minimale primidealer for R. Betragt den kanoniske homomorfi,

$$R \to R/\mathfrak{q}_1 \times \cdots \times R/\mathfrak{q}_r.$$

Lad $\mathfrak{p}$ være et primideal. De minimale primidealer for $R_{\mathfrak{p}}$ svarer da til de $\mathfrak{q}_i$, som er indeholdt i $\mathfrak{p}$. Da $R_{\mathfrak{p}}$ er et integritetsområde ifølge Korollar (1.6), følger det, at inklusionen $\mathfrak{q}_j \subseteq \mathfrak{p}$ er opfyldt for netop ét $\mathfrak{q}_j$ og at der for dette $\mathfrak{q}_j$ gælder, at $\mathfrak{q}_j R_{\mathfrak{p}} = (0)$. Heraf ses, at den kanoniske homomorfi efter lokalisering i $\mathfrak{p}$ bliver bijektiv. Da $\mathfrak{p}$ var et vilkårligt primideal, må den kanoniske homomorfi være bijektiv. Yderligere følger det, at integritetsområdet $R/\mathfrak{q}_j$ er en lokalt regulær ring, thi lokaliseres $R/\mathfrak{q}_j$ i et primideal $\mathfrak{p}/\mathfrak{q}_j$, svarende til $\mathfrak{p} \supseteq \mathfrak{q}_j$, fremkommer den regulære lokale ring $R_{\mathfrak{p}}$.

Påstanden (2) følger umiddelbart af Korollar (1.8). ∎

(2.3) Observation. En ring af dimension 0 er som bekendt et legeme, hvis og kun hvis den er et integritetsområde. Heraf ses, at de lokalt regulære ringe af dimension 0 netop er de ringe, der er et endeligt produkt af legemer.

(2.4) Sætning. *For et noethersk integritetsområde R af dimension 1 er følgende betingelser ækvivalente:*

(i) *R er en Dedekindring.*
(ii) *R lokalt regulær.*
(iii) *R er normal.*

Bevis. En Dedekindring kan som bekendt karakteriseres som et noethersk integritetsområde R, hvori der der for ethvert maksimalideal $\mathfrak{m}$ gælder, at den lokale ring $R_{\mathfrak{m}}$ er en valuationsring. Af Korollar (1.11) følger derfor at (i)⇔(ii).

For et integritetsområde R gælder, at R er normal, hvis og kun hvis $R_{\mathfrak{m}}$ er normal for alle maksimalidealer $\mathfrak{m}$. Af Korollar (1.11) følger derfor at (ii)⇔(iii). ∎

(2.5) Sætning. *Lad R være et noethersk integritetsområde af dimension 1. Lad K betegne brøklegemet for R, og lad legemet K' være en endelig udvidelse af K. Da er den hele afslutning af R i K' en Dedekindring.*

Bevis. Lad R' betegne den hele afslutning af R i K'. Da er R' hel over R. Af Cohen–Seidenberg's første Sætning følger derfor, at R' og R har samme dimension. Altså er R' et integritetsområde af dimension 1. Videre er R' normal, dvs helt afsluttet i sit brøklegeme. Brøklegemet for R' er nemlig indeholdt i legemet K' (da K'/K er antaget endelig, gælder faktisk at K' er brøklegemet for R'), så en brøk der er hel over R' er derfor også hel over R og dermed element i R'.

For at vise, at R' er en Dedekindring, skal det altså vises, jfr Sætning (2.4), at R' er noethersk. Denne påstand fremgår af det efterfølgende resultat. □

(2.6) Krull–Akizuki's Sætning. *Antag forudsætningerne i Sætning* (2.5). *Da vil enhver delring T af K', som omfatter R, være noethersk af dimension mindre end eller lig med* 1.

Bevis. Det er nok at vise, at der for hvert ideal $\mathfrak{a} \neq (0)$ i T gælder, at kvotienten $T/\mathfrak{a}$ har endelig længde som R-modul. Heraf følger nemlig først, at i enhver stigende følge af idealer i T,

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots,$$

hvor $\mathfrak{a}_1 \neq (0)$, er antallet af skarpe inklusioner begrænset opad af $\operatorname{long}_R(T/\mathfrak{a}_1)$. Altså er T noethersk. Videre følger det, at for hvert primideal $\mathfrak{p} \neq (0)$ i T er kvotienten $T/\mathfrak{p}$ af endelig længde som T-modul, og dermed et legeme. Altså er $\mathfrak{p}$ et maksimalideal. Følgelig har T dimension højst 1.

Det skal vises, at $T/\mathfrak{a}$ har endelig længde som R-modul. Indledende bemærker vi, at der findes et element $f \neq 0$ i $R \cap \mathfrak{a}$. Betragt nemlig et element $\alpha \neq 0$ i $\mathfrak{a}$. Da udvidelsen K'/K er endelig, er α algebraisk over R. Der findes altså en ikke-triviel relation $f_n\alpha^n + \cdots + f_1\alpha + f_0 = 0$, hvor $f_i \in R$. Da K' er et integritetsområde, kan vi i relationen antage, at $f_0 \neq 0$. Af $f_0 = -(\alpha^{n-1}f_n + \cdots + f_1)\alpha$ følger, at $f_0 \in \mathfrak{a}$. Altså er $f := f_0$ det søgte element i $R \cap \mathfrak{a}$.

For at vise at $T/\mathfrak{a}$ har endelig længde som R-modul, er det nok at vise, at der findes et tal l således at enhver endeligt frembragt R-undermodul af $T/\mathfrak{a}$ har en længde, der er mindre end eller lig med l. Vi viser, at en sådan øvre grænse opnås med tallet,

$$l := |K':K| \operatorname{long} R/fR.$$

Her er $|K':K|$ rangen af K' som vektorrum over K. Længden $\operatorname{long} R/fR$ er endelig, da R er et noethersk integritetsområde af dimension 1 og $f \neq 0$.

En endeligt frembragt R-undermodul af $T/\mathfrak{a}$ er billede af en endeligt frembragt R-undermodul $M \subseteq T$ ved den kanoniske homomorfi $T \to T/\mathfrak{a}$. Da $f \in \mathfrak{a}$, inducerer den kanoniske homomorfi en R-lineær homomorfi $M/fM \to T/\mathfrak{a}$. Enhver endeligt frembragt R-undermodul af $T/\mathfrak{a}$ er derfor homomorft billede af M/fM for en passende endeligt frembragt R-undermodul af T. Det er derfor nok at vise, at for enhver endeligt frembragt R-undermodul M af K' gælder uligheden,

$$\operatorname{long} M/fM \leqslant |K':K| \operatorname{long} R/fR.$$

Modulen M har, som delmængde af K-vektorrummet K' en endelig rang r, der er mindre end eller lig med rangen $|K'{:}K|$. Vi viser ligheden,

$$\operatorname{long} M/fM = r \ \operatorname{long} R/fR. \tag{1}$$

Betragt hertil i M en R-undermodul N frembragt af r elementer, der er lineært uafhængige over K. Disse frembringere er specielt lineært uafhængige over R, så $N = R^r$. Yderligere er hvert element x i M en K-linearkombinatione af disse frembringere. Idet $s \in R$ er en fælles nævner for koefficienterne i en sådan fremstilling, ses det at $sx \in N$. Kvotientmodulen $Q := M/N$ er derfor en torsionsmodul: hvert element i M/N annulleres af et element $s \neq 0$ i R. Da R har dimension 1, følger det, at kvotienten Q har endelig længde.

Betragt nu den eksakte følge,

$$0 \longrightarrow N \longrightarrow M \longrightarrow Q \longrightarrow 0,$$

og multiplikation med f i hver af de tre moduler. De to første moduler er indeholdt i K', og multiplikation med f er derfor injektiv. Lad ${}_fQ$ betegne kernen for multiplikation med f på Q. Da gælder følgende ligheder:

$$\operatorname{long} M/fM = \operatorname{long} N/fN + \operatorname{long} Q/fQ - \operatorname{long} {}_fQ = \operatorname{long} N/fN = r \ \operatorname{long} R/fR.$$

Den første lighed fås nemlig ved at betragte længderne af modulerne i den eksakte kerne-kokerne følge og udnytte, at den alternerende sum af længderne er lig med 0. Den anden lighed fås tilsvarende af den eksakte følge $0 \longrightarrow {}_fQ \to Q \xrightarrow{f} Q \longrightarrow Q/fQ \longrightarrow 0$, hvor alle modulerne har endelig længde. Endelig følger den tredie lighed af at $N = R^r$.

Af disse ligheder fremgår den ønskede ligning (1). Hermed er beviset fuldført. □

(2.7) Bemærkning. I teorien for Dedekindringe anvendes Sætning (2.5) oftest i tilfældet, hvor den givne ring R selv er en Dedekindring. For mange anvendelser er det nødvendigt at forudsætte, at den hele afslutning R' er endeligt frembragt som R-modul. Man kan vise, at dette er tilfældet, hvis udvidelsen K'/K er separabel, eller hvis R er endeligt frembragt som algebra over et legeme.

For $R = \mathbf{Z}$, hvor altså $K = \mathbf{Q}$, er legemet K' et såkaldt algebraisk tallegeme. Den hele afslutning R' består her af de hele algebraiske tal i K'.

(2.8) Sætning. *Antag, at R er lokalt regulær. Da er også polynomiumsringen $R[X]$ lokalt regulær.*

Bevis. Lad $\mathfrak{P}$ være et primideal i $R[X]$, og lad $\mathfrak{p} := R \cap \mathfrak{P}$ være kontraktionen. Det skal vises, at den lokale ring $R[X]_{\mathfrak{P}}$ er regulær. Denne lokale ring fås ved ved at lokalisere $R_{\mathfrak{p}}[X]$ i det til $\mathfrak{P}$ svarende primideal. Vi kan derfor antage, at R er en lokal ring og at $\mathfrak{p}$ er maksimalidealet i R. Lad h betegne højden af $\mathfrak{p}$, altså dimensionen af R. Da R er antaget lokalt regulær, er specielt R en regulær lokal ring, så der findes et regulært parametersystem, dvs h elementer $(x_1, \dots, x_h)$, der frembringer $\mathfrak{p}$. Der er nu to muligheder:

Enten er $\mathfrak{P} = \mathfrak{p}[X]$. I dette tilfælde er $\mathfrak{P}$ som bekendt af højde h. Yderligere er $\mathfrak{P}$ frembragt af de h elementer $(x_1, \dots, x_h)$. Den lokale ring $R[X]_{\mathfrak{P}}$ er derfor regulær.

Eller også er $\mathfrak{P} \supset \mathfrak{p}[X]$. I dette tilfælde er $\mathfrak{P}$ som bekendt af højde $h + 1$. Yderligere svarer $\mathfrak{P}$ til et ikke trivielt primideal i kvotienten $(R/\mathfrak{p})[X]$. Denne kvotientring er polynomiumsringen over et legeme, så det ikke trivielle primideal er et hovedideal. Vælges i $R[X]$ et polynomium f, hvis restklasse frembringer dette hovedideal, så er $\mathfrak{P}$ er frembragt af de $h + 1$ elementer $(x_1, \dots, x_h, f)$. Den lokale ring $R[X]_{\mathfrak{P}}$ er derfor regulær. $\square$

(2.9) Eksempel. Polynomiumsringen $k[X_1, \dots, X_n]$, hvor k er et legeme eller $k = \mathbf{Z}$, er lokalt regulær.

3. Jacobi's kriterium.

(3.1) Setup. I det følgende betragtes polynomiumsringen $R = k[X_1, \dots, X_n]$ i n variable over et legeme k. For et primideal $\mathfrak{p}$ i R betegnes med $\mathfrak{m}_\mathfrak{p}$ maksimalidealet i lokaliseringen $R_\mathfrak{p}$, og med $\boldsymbol{\kappa}(\mathfrak{p}) = R_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ betegnes restklasselegemet. For hver brøk f i $R_\mathfrak{p}$ betegnes med $f(\mathfrak{p})$ restklassen af f modulo $\mathfrak{m}_\mathfrak{p}$. Værdien $f(\mathfrak{p})$ er altså element i legemet $\boldsymbol{\kappa}(\mathfrak{p})$. Legemet $\boldsymbol{\kappa}(\mathfrak{p})$ er også brøklegemet for integritetsområdet $R/\mathfrak{p}$; hvis brøken f specielt er et polynomium, så er $f(\mathfrak{p})$ blot restklassen af f modulo $\mathfrak{p}$.

For $i = 1, \dots, n$ betegner ∂_i den partielle differentiation $f \mapsto \partial f/\partial X_i$. Afbildningerne ∂_i er k-lineære *derivationer* i R, dvs de opfylder ligningerne,

$$\partial_i(fg) = f\partial_i g + g\partial_i f,$$

og de kan derfor udvides til derivationer i brøkringen $R_\mathfrak{p}$.

(3.2) Definition. Den sammensatte afbildning $f \mapsto \partial_i f \mapsto \partial_i f(\mathfrak{p})$ inducerer ved restriktion en $R_\mathfrak{p}$-lineær afbildning $\mathfrak{m}_\mathfrak{p} \to \boldsymbol{\kappa}(\mathfrak{p})$. For $f \in R_\mathfrak{p}$ og $g \in \mathfrak{m}_\mathfrak{p}$ fås nemlig $\partial_i(fg)(\mathfrak{p}) = f(\mathfrak{p})\partial_i g(\mathfrak{p}) + g(\mathfrak{p})\partial_i f(\mathfrak{p}) = f(\mathfrak{p})\partial_i g(\mathfrak{p})$, idet $g(\mathfrak{p}) = 0$.

Da homomorfien $f \mapsto \partial_i f(\mathfrak{p})$ er en $R_\mathfrak{p}$-lineær afbildning $\mathfrak{m}_\mathfrak{p} \to \boldsymbol{\kappa}(\mathfrak{p})$, inducerer den en lineær afbildning af vektorrum over $\boldsymbol{\kappa}(\mathfrak{p})$,

$$\partial_i(\mathfrak{p})\colon \mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^2 \to \boldsymbol{\kappa}(\mathfrak{p}).$$

Med $\partial(\mathfrak{p})\colon \mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^2 \to \boldsymbol{\kappa}(\mathfrak{p})^n$ betegnes den $\boldsymbol{\kappa}(\mathfrak{p})$-lineære afbildning, hvis i'te koordinat er $\partial_i(\mathfrak{p})$.

Bemærk, at rangen af vektorrummet $\mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^2$ er lig med dimensionen af den lokale ring $R_\mathfrak{p}$, da $R_\mathfrak{p}$ er regulær ifølge Eksempel (2.9). Rangen er altså lig med højden af primidealet $\mathfrak{p}$. Af dimensionsformlen følger, at rangen også er lig med $n - \operatorname{tdeg}_k(R/\mathfrak{p})$.

(3.3) Lemma. *Homomorfien induceret af de partielle derivationer,*

$$\partial(\mathfrak{p})\colon \mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^2 \to \boldsymbol{\kappa}(\mathfrak{p})^n,$$

er injektiv, når blot en af følgende to betingelser er opfyldt:

(1) *Primidealet* $\mathfrak{p}$ *er et maksimalideal af formen*

$$\mathfrak{p} = (X_1 - p_1, \dots, X_n - p_n) \quad \textit{hvor } p_i \in k.$$

(2) *Legemet* k *er perfekt legeme, fx et legeme af karakteristik* 0, *eller et algebraisk afsluttet legeme, eller et endeligt legeme.*

Bevis. (1) Maksimalidealet af den angivne form er kernen for homomorfien $f \mapsto f(p)$, hvor $p = (p_1, \dots, p_n) \in k^n$. Kvotienten $R/\mathfrak{p}$ kan altså i dette tilfælde identificeres med k, og homomorfien $f \mapsto f(\mathfrak{p})$ kan identificeres med $f \mapsto f(p)$.

Polynomierne $X_i - p_i$ frembringer $\mathfrak{p}$ og dermed også $\mathfrak{m}_\mathfrak{p}$, og deres restklasser modulo $\mathfrak{m}_\mathfrak{p}^2$ er en k-basis for $\mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^2$. I denne basis er $\partial(p)$ øjensynlig givet ved enhedsmatricen. Specielt er $\partial(p)$ injektiv.

(2) Lad x_i betegne restklassen modulo $\mathfrak{p}$ af X_i. Da er $R/\mathfrak{p} = k[x_1, \dots, x_n]$, og afbildningen $g \mapsto g(\mathfrak{p})$ er blot indsættelse, $g \mapsto g(x_1, \dots, x_n)$, i polynomier. Kvotienten $k[x_1, \dots, x_n]$ er et integritetsområde og endeligt frembragt som algebra over k. Lad t betegne transcendensgraden over k.

Vi udtager blandt $x_1, \dots, x_n$ en transcendensbasis på følgende måde: Enten er x_i'erne algebraisk uafhængige over k, og så udgør de den søgte transcendensbasis. Eller også findes ikke-konstante polynomier g i R således at $g(x_1, \dots, x_n) = 0$. Vælg i dette tilfælde et sådant polynomium g af lavest mulig grad.

Antag først, at legemet k er af positiv karakteristik q. At legemet er perfekt betyder så, at afbildningen $a \mapsto a^q$ (der jo er en injektiv ringhomomorfi $k \to k$) er bijektiv. Med andre ord er hvert element i k en q'te potens. Det påstås, at mindst én af de variable X_i forekommer i g med en eksponent, der ikke er delelig med q. I modsat fald ville nemlig alle monomier $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ der forekommer i g være q'te potenser, og da koefficienterne i g også er q'te potenser, ville polynomiet g være en q'te potens, $g = h^q$. Af $0 = g(x_1, \dots, x_n) = h(x_1, \dots, x_n)^q$ ville der så følge $h(x_1, \dots, x_n) = 0$, i modstrid med at g var valgt af minimal grad. Efter omnummerering kan vi antage, at X_1 forekommer i g med en eksponent, der ikke er delelig med q. Det følger, at det afledede polynomium $\partial_1 g$ ikke er nulpolynomiet. Det afledede polynomium har lavere grad end g, så valget af g sikrer, at $\partial_1 g(x_1, \dots, x_n) \neq 0$.

Hvis karakteristikken af k er 0, er valget lettere. En af de variable forekommer i g, og efter omnummerering kan vi antage, at det er X_1. Det afledede polynomium $\partial_1 g$ er så ikke er nul-polynomiet, og følgelig er $\partial_1 g(x_1, \dots, x_n) \neq 0$.

Øjensynlig er x_1 algebraisk over $k[x_2, \dots, x_n]$. Nu fortsættes med elementerne $x_2, \dots, x_n$. Hvis disse elementer er algebraisk uafhængige, er de den søgte transcendensbasis. I modsat fald findes (eventuelt efter omnummerering af $x_2, \dots, x_n$) et polynomium g_2, som ikke afhænger af X_1, således at $g_2(x_1, x_2, \dots, x_n) = 0$ og $\partial_2 g_2(x_1, x_2, \dots, x_n) \neq 0$. Da g_2 ikke afhænger af X_1 er $\partial_1 g_2 = 0$.

Processen stopper efter endelig mange skridt (og omnummereringer) med et algebraisk uafhængigt sæt $x_{h+1}, \dots, x_n$ blandt x_i'erne og polynomier $g_1, \dots, g_h$ med $g_j(x_1, \dots, x_n) = 0$ og $\partial_j g_j(x_1, \dots, x_n) \neq 0$, og således at g_j ikke afhænger af de variable $X_1, \dots, X_{j-1}$. Elementerne $x_{h+1}, \dots, x_n$ udgør øjensynlig en transcendensbasis for $k[x_1, \dots, x_n]$ over k.

Da $g_j(x_1, \dots, x_n) = 0$, ligger følgen $(g) = (g_1, \dots, g_h)$ i primidealet $\mathfrak{p}$, og dermed også i $\mathfrak{m}_\mathfrak{p}$. Betragt $n \times h$ matricen, hvis j-te søjle er $\partial g_j(\mathfrak{p})$. De første h rækker udgør en (kvadratisk) $h \times h$ matrix. Heri stå på den j'te plads i diagonalen elementet $\partial_j g_j(\mathfrak{p})$ som er forskellig fra 0, og over dette element står $\partial_i g_j(\mathfrak{p})$ for $i < j$, som er lig med 0. Heraf ses, at matricen $\partial g(\mathfrak{p})$ har rang h.

Det følger, at afbildningen $\partial(\mathfrak{p}) \colon \mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^2 \to \kappa(\mathfrak{p})^n$ mindst har rangen h. På den anden side var $n - h$ lig med transcendensgraden af $R/\mathfrak{p}$, så h er lig med rangen af vektorrummet $\mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^2$, jfr (3.2). Altså er afbildningen $\partial(\mathfrak{p})$ injektiv.

Hermed er injektiviteten vist i begge tilfælde. □

(3.4) Bemærkning. Transcendensbasen konstrueret i beviset for Sætning (3.3) under forudsætning af at k er perfekt er en såkaldt *separerende transcendensbasis*. Af beviset fremgår for de fundne polynomier $g_1, \dots, g_h$, at restklasserne module $\mathfrak{m}_\mathfrak{p}^2$ er en basis for $\mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^2$. Polynomierne $g_1, \dots, g_h$ frembringer derfor maksimalidealet $\mathfrak{m}_\mathfrak{p}$. Da $h = \dim R_\mathfrak{p}$, udgør disse polynomier et regulært parametersystem for $R_\mathfrak{p}$.

Forudsætningen om at k er perfekt i (3.3)(2) er nødvendig for at homomorfien $\partial(\mathfrak{p})$ er injektiv for ethvert primideal $\mathfrak{p}$. Antag nemlig, at k ikke er perfekt, og lad a være et element i k, som ikke er en q'te potens (hvor q er karakteristikken af k). Polynomiet $X^q - a$ er da et irreducibelt polynomium, så idealet $\mathfrak{p} = (X^q - a)$ er et maksimalideal i $R := k[X]$. Det er klart, at homomorfien $\partial(\mathfrak{p})\colon \mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^2 \to \boldsymbol{\kappa}(\mathfrak{p})$ her er nul-homomorfien.

(3.5) Setup. I det følgende betragtes i R et sæt af s polynomier $\mathbf{f} = (f_1, \dots, f_s)$. Det antages, at $f_j \in \mathfrak{p}$. Med $\partial\mathbf{f}(\mathfrak{p})$ betegnes matricen, hvis j'te søjle er $\partial f_j(\mathfrak{p})$. Matricen kaldes *Jacobi-matricen*. Den er en $n \times s$ matrix med koefficienter i legemet $\boldsymbol{\kappa}(\mathfrak{p})$.

(3.6) Jacobi's kriterium. *Antag, at polynomierne $f_1, \dots, f_s$ tilhører primidealet $\mathfrak{p}$. Betragt kvotienten $\overline{R} := R/(f_1, \dots, f_s)$. Da gælder Jacobi's ulighed,*

$$\dim \overline{R}_\mathfrak{p} \leqslant \dim R_\mathfrak{p} - \operatorname{rk} \partial\mathbf{f}(\mathfrak{p}).$$

Hvis lighed gælder i uligheden, så er den lokale ring $\overline{R}_\mathfrak{p}$ regulær. Er den lineære afbildning $\partial(\mathfrak{p})\colon \mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^2 \to \boldsymbol{\kappa}(\mathfrak{p})^n$ injektiv, så gælder lighed, hvis og kun hvis $\overline{R}_\mathfrak{p}$ er regulær.

Bevis. Lad $\overline{\mathfrak{m}}_\mathfrak{p}$ betegne maksimalidealet i $\overline{R}_\mathfrak{p}$. Betragt følgende diagram af vektorrum over $\boldsymbol{\kappa}(\mathfrak{p})$:

$$\begin{tikzcd}
0 \arrow[r] & (\mathbf{f}, \mathfrak{m}_\mathfrak{p}^2)/\mathfrak{m}_\mathfrak{p}^2 \arrow[r] & \mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^2 \arrow[r] \arrow[d, "\partial(\mathfrak{p})"] & \overline{\mathfrak{m}}_\mathfrak{p}/\overline{\mathfrak{m}}_\mathfrak{p}^2 \arrow[r] & 0 \\
& \boldsymbol{\kappa}(\mathfrak{p})^s \arrow[u, "\mathbf{f}"] \arrow[r, "\partial\mathbf{f}(\mathfrak{p})"] & \boldsymbol{\kappa}(\mathfrak{p})^n. & &
\end{tikzcd}$$

Idealet $(\mathbf{f}, \mathfrak{m}_\mathfrak{p}^2)$ er idealet i $R_\mathfrak{p}$ frembragt af f_j'erne og $\mathfrak{m}_\mathfrak{p}^2$. Pilen øverst til højre er induceret af den surjektive homomorfi $\mathfrak{m}_\mathfrak{p} \to \overline{\mathfrak{m}}_\mathfrak{p}$. Det er klart, at diagrammets øverste række er eksakt. Den højre pil nedad er homomorfien fra Definition (3.2). Den venstre pil opad er bestemt ved at den j'te basisvektor i $\boldsymbol{\kappa}(\mathfrak{p})^s$ afbildes på ækvivalensklassen af f_j modulo $\mathfrak{m}_\mathfrak{p}^2$. Øjensynlig er denne pil er surjektiv. Det er klart, at diagrammet er kommutativt.

Lad V betegne $(\mathbf{f}, \mathfrak{m}_\mathfrak{p}^2)/\mathfrak{m}_\mathfrak{p}^2$. Af vektorrummene $\mathfrak{m}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^2$ og $\overline{\mathfrak{m}}_\mathfrak{p}/\overline{\mathfrak{m}}_\mathfrak{p}^2$ har det første som nævnt rang lig med $\dim R_\mathfrak{p}$, og for rangen af det andet gælder som bekendt uligheden $\dim \overline{R}_\mathfrak{p} \leqslant \operatorname{rk} \overline{\mathfrak{m}}_\mathfrak{p}/\overline{\mathfrak{m}}_\mathfrak{p}^2$. På den anden side er differensen mellem rangene af de to vektorrum lig med rangen af V. Vi har derfor vurderingen,

$$\dim \overline{R}_\mathfrak{p} \leqslant \operatorname{rk} \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 = \dim R_\mathfrak{p} - \operatorname{rk} V, \tag{1}$$

og som bekendt er uligheden en lighed, hvis og kun hvis $\overline{R}_\mathfrak{p}$ er regulær. På den anden side definerer homomorfien $\partial(\mathfrak{p})$ ved restriktion en $\boldsymbol{\kappa}(\mathfrak{p})$-lineær afbildning $V \to \boldsymbol{\kappa}(\mathfrak{p})^n$. Da homomorfien $\mathbf{f}$ er surjektiv, afbildes V ved $\partial(\mathfrak{p})$ netop på billedrummet for afbildningen $\partial\mathbf{f}(\mathfrak{p})$. Altså fås uligheden,

$$\operatorname{rk} V \geqslant \operatorname{rk} \partial\mathbf{f}(\mathfrak{p}), \tag{2}$$

med lighed, hvis $\partial(\mathfrak{p})$ er injektiv.

Kombination af (1) og (2) giver umiddelbart Jacobi's Kriterium. ▯

(3.7) Bemærkning. Resultatet i (3.6) kombineres naturligvis ofte med Lemma (3.3). Hvis k er et perfekt legeme, eller hvis $\mathfrak{p} = (X_1 - p_1, \dots, X_n - p_n)$, så er den lokale ring $\overline{R}_\mathfrak{p}$ altså er regulær, hvis og kun hvis lighed gælder i Jacobi's ulighed.

(3.8) Sætning. *Antag, under forudsætningerne i* (3.6), *at lighed gælder i Jacobi's ulighed, altså at* $\dim \overline{R}_\mathfrak{p} = \dim R_\mathfrak{p} - \operatorname{rk} \partial f(\mathfrak{p})$. *Der findes da blandt de isolerede primidealer for* $(f_1, \dots, f_s)$ *netop ét primideal* $\mathfrak{p}_0$, *således at* $\mathfrak{p}_0 \subseteq \mathfrak{p}$. *Højden af primidealet* $\mathfrak{p}_0$ *er lig med rangen af matricen* $\partial\mathbf{f}(\mathfrak{p})$.

Lad r *betegne rangen af matricen* $\partial\mathbf{f}(\mathfrak{p})$, *og antag fx at de første* r *søjler i matricen, svarende til de første* r *polynomier* $\mathbf{f}^* = (f_1, \dots, f_r)$, *er uafhængige over legemet* $\kappa(\mathfrak{p})$. *Da findes et polynomium* h *med* $h(\mathfrak{p}) \neq 0$, *således at følgende gælder:* (1) *De tre idealer* $(f_1, \dots, f_r) \subseteq (f_1, \dots, f_s) \subseteq \mathfrak{p}_0$ *har samme ekstension til brøkringen* $R[h^{-1}]$. (2) *For hvert primideal* $\mathfrak{q}$ *således at* $\mathfrak{q} \supseteq (\mathbf{f}^*)$ *og* $h(\mathfrak{q}) \neq 0$ *gælder, at* $\mathfrak{q} \supseteq (\mathbf{f})$ *og* $\dim \overline{R}_\mathfrak{q} = \dim R_\mathfrak{q} - \operatorname{rk} \partial\mathbf{f}(\mathfrak{q})$.

Bevis. Det følger af antagelsen, at den lokale ring $\overline{R}_\mathfrak{p} = R_\mathfrak{p}/(\mathbf{f})_\mathfrak{p}$ er regulær. Specielt er $R_\mathfrak{p}/(\mathbf{f})_\mathfrak{p}$ et integritetsområde. Heraf følger, at der blandt de isolerede primidealer for $(\mathbf{f})$ findes netop ét primideal $\mathfrak{p}_0$, der er indeholdt i $\mathfrak{p}$, nemlig kontraktionen til R af primidealet $(\mathbf{f})_\mathfrak{p}$ i $R_\mathfrak{p}$. Det er klart, at højden af $\mathfrak{p}/\mathfrak{p}_0$ er lig med $\dim \overline{R}_\mathfrak{p}$, og altså ifølge forudsætningen lig med $\dim R_\mathfrak{p} - r$. På den anden side er R en katernær ring, så højden af $\mathfrak{p}/\mathfrak{p}_0$ er differensen mellem højden af $\mathfrak{p}$ og højden af $\mathfrak{p}_0$. Højden af $\mathfrak{p}$ er lig med $\dim R_\mathfrak{p}$, så det følger, at højden af $\mathfrak{p}_0$ er lig med r. Hermed er Sætningens første påstand bevist.

Betragt de tre idealer er $(\mathbf{f}^*) \subseteq (\mathbf{f}) \subseteq \mathfrak{p}_0$. Ved lokalisering i $\mathfrak{p}$ fås inklusionerne,

$$(\mathbf{f}^*)_\mathfrak{p} \subseteq (\mathbf{f})_\mathfrak{p} \subseteq \mathfrak{p}_0 R_\mathfrak{p}.$$

Ifølge valget af $\mathfrak{p}_0$ er den sidste inklusion en lighed. Også den første inklusion er en lighed. Betragt nemlig Jacobi's ulighed for $(\mathbf{f}^*)$,

$$\dim R_\mathfrak{p}/(\mathbf{f}^*)_\mathfrak{p} \leqslant \dim R_\mathfrak{p} - \operatorname{rk} \partial\mathbf{f}^*(\mathfrak{p}).$$

Ifølge valget af $(\mathbf{f}^*)$ er rangen på højresiden lig med rangen r af $\partial\mathbf{f}(\mathfrak{p})$. Ifølge forudsætningen er højresiden derfor lig med $\dim R_\mathfrak{p}/(\mathbf{f})_\mathfrak{p}$, og da $R_\mathfrak{p}/(\mathbf{f})_\mathfrak{p}$ er en kvotient af $R_\mathfrak{p}/(\mathbf{f}^*)_\mathfrak{p}$, er højresiden altså mindre end eller lig med venstresiden. Heraf ses først, at lighed gælder i Jacobi's ulighed ovenfor, hvorfor $R_\mathfrak{p}/(\mathbf{f}^*)$ er regulær, og specielt et integritetsområde. Heraf følger videre, at $(\mathbf{f}^*)_\mathfrak{p} = (\mathbf{f})_\mathfrak{p}$, idet de to kvotientringe $R_\mathfrak{p}/(\mathbf{f}^*)_\mathfrak{p}$ og $R_\mathfrak{p}/(\mathbf{f})_\mathfrak{p}$ har samme dimension og den første er et integritetsområde.

De tre idealer $(\mathbf{f}^*) \subseteq (\mathbf{f}) \subseteq \mathfrak{p}_0$ bliver altså ens ved ekstension til $R_\mathfrak{p}$. Det følger(!), at de tre idealer bliver ens ved ekstension til en brøkring $R[h^{-1}]$, hvor h er et passende polynomium i komplementærmængden til $\mathfrak{p}$, dvs $h(\mathfrak{p}) \neq 0$.

Lad nu $\mathfrak{q} \supseteq (\mathbf{f}^*)$ være et primideal, således at $h(\mathfrak{q}) \neq 0$. Da h ikke tilhører $\mathfrak{q}$ er $\mathfrak{q}$ lig med kontraktionen af sin ekstension til $R[h^{-1}]$. Denne ekstension indeholder ekstensionen af $(\mathbf{f}^*)$, og den sidste ekstension er ifølge det viste lig med ekstensionen af $\mathfrak{p}_0$. Heraf følger, at $\mathfrak{q} \supseteq \mathfrak{p}_0$. Specielt er altså $\mathfrak{q} \supseteq (\mathbf{f})$. Med det ovenfor bestemte polynomium gælder altså Sætningens påstand (1) og den første påstand i (2).

Den anden påstand i (2) er ligheden $\dim R_\mathfrak{q} - \dim \overline{R}_\mathfrak{q} = \operatorname{rk} \partial\mathbf{f}(\mathfrak{q})$. Hertil bemærker vi først, at da h ikke tilhører primidealet $\mathfrak{q}$, er $R_\mathfrak{q}$ en lokalisering af $R[h^{-1}]$. Idealerne $(\mathbf{f})$ og $\mathfrak{p}_0$ har derfor samme ekstension til $R_\mathfrak{q}$. Heraf følger, at kvotienten $\overline{R}_\mathfrak{q} = R_\mathfrak{q}/(\mathbf{f})_\mathfrak{q}$ er lig med $R_\mathfrak{q}/\mathfrak{p}_0 R_\mathfrak{q}$. Dimensionen af $\overline{R}_\mathfrak{q}$ er derfor lig med højden af $\mathfrak{q}/\mathfrak{p}_0$. Da polynomiumsringen R er katernær, er $\operatorname{ht} \mathfrak{q}/\mathfrak{p}_0 = \dim R_\mathfrak{q} - \operatorname{ht} \mathfrak{p}_0$. Videre er $\operatorname{ht} p_0 = \operatorname{rk} \partial\mathbf{f}(\mathfrak{p})$ ifølge det først viste. Vi udleder derfor ligningen,

$$\dim R_\mathfrak{q} - \dim \overline{R}_\mathfrak{q} = \operatorname{rk} \partial\mathbf{f}(\mathfrak{p}).$$

Venstresiden i denne ligning er ifølge Jacobi's ulighed større end eller lig med $\operatorname{rk} \partial\mathbf{f}(\mathfrak{q})$, og det er Sætningens sidste påstand, at venstresiden i denne ligning er lig med $\operatorname{rk} \partial\mathbf{f}(\mathfrak{q})$. Ækvivalent gælder altså uligheden,

$$\operatorname{rk} \partial\mathbf{f}(\mathfrak{q}) \leqslant \operatorname{rk} \partial\mathbf{f}(\mathfrak{p}), \tag{*}$$

og det er påstanden at lighed gælder. For at vise denne lighed, må vi være mere omhyggelige med valget af polynomiet h. Da r er rangen af matricen $\partial\mathbf{f}(\mathfrak{p})$ findes i denne matrix en $r \times r$ underdeterminant, der er forskellig fra 0. I Jacobi-matricen $\partial\mathbf{f}$ findes altså en $r \times r$ underdeterminant h_1, således at $h_1(\mathfrak{p}) \neq 0$. Multiplicerer vi h med h_1 ændrer vi ikke de benyttede egenskaber ved h. Vi kan derfor antage, at h_1 er divisor i h. Da $h(\mathfrak{q}) \neq 0$, følger det så, at $h_1(\mathfrak{q}) \neq 0$. Matricen $\partial\mathbf{f}(\mathfrak{q})$ har altså en $r \times r$ underdeterminant forskellig fra 0, og dens rang er derfor mindst r. Heraf sluttes, at uligheden (*) må være en lighed, og hermed er Sætningens sidste påstand bevist. □

(3.9) Bemærkning. Som bekendt definerer det givne sæt $(\mathbf{f})$ af polynomier et skema V i $\mathbf{A}^n$, med koordinatringen $\Gamma(V) = \overline{R} = R/(\mathbf{f})$. Primidealerne i $\overline{R}$ svarer til integritetsskemaer indeholdt i X. Specielt svarer de minimale primidealer i $\overline{R}$, dvs de isolerede primidealer for $(\mathbf{f})$, til komponenterne af V, og maksimalidealerne i $\overline{R}$, dvs maksimalidealer i R som omfatter $(\mathbf{f})$, svarer til punkterne på V. Vilkårlige primidealer $\mathfrak{p} \supseteq (\mathbf{f})$ kaldes også „punkter“ på V.

I Sætning (3.8) definerer tilsvarende de første r polynomier $(\mathbf{f}^*)$ et skema $V^* \supseteq V$. Hvis h er et polynomium med $h(\mathfrak{p}) \neq 0$, så definerer betingelsen $h(\mathfrak{q}) \neq 0$ en såkaldt *åben omegn* af $\mathfrak{p}$. Forudsætningen om at lighed gælder i Jacobi's ulighed udtrykkes ved at sige, at V er *glat* i punktet $\mathfrak{p}$. Sætningens indhold kan udtrykkes geometrisk som følger:

Antag, at V er glat i punktet $\mathfrak{p}$. Da ligger $\mathfrak{p}$ på netop én komponent V_0 af V, og dimensionen af V_0 er lig med $n - \operatorname{rk} \partial\mathbf{f}(\mathfrak{p})$.

Desuden gælder i en åben omegn af $\mathfrak{p}$ er $V^* = V$, og heri er V et integritetsskema af dimension $n - r$, og glat i alle sine punkter.

(3.10) Bemærkning. Antag, at legemet k er perfekt. Af Lemma (3.3) og Jacobi's Kriterium følger så for et primideal $\mathfrak{p} \supseteq (\mathbf{f})$, at ligningen $\dim \overline{R}_\mathfrak{p} = \dim R_\mathfrak{p} - \operatorname{rk} \partial\mathbf{f}(\mathfrak{p})$ gælder, hvis og kun hvis den lokale ring $\overline{R}_\mathfrak{p}$ er regulær.

Antag specielt, at idealet $(\mathbf{f})$ selv er et primideal $\mathfrak{p}_0$. Da er $\overline{R} = R/\mathfrak{p}_0$ et integritetsområde, og den lokale ring $\overline{R}_{\mathfrak{p}_0}$ er brøklegemet herfor. Den lokale ring er derfor regulær, af dimension 0. Af Sætning (3.8) følger nu specielt, at der findes et polynomium h, som ikke tilhører $\mathfrak{p}_0$, således at der for alle primidealer $\mathfrak{q} \supseteq \mathfrak{p}_0$ med $h \notin \mathfrak{q}$ gælder, at den lokale ring $\overline{R}_{\mathfrak{q}}$ er regulær.

(3.11) Bemærkning. Betragt tilfældet hvor $k = \mathbb{R}$. For maksimalidealer af formen

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

svarende til punkter $p = (p_1, \ldots, p_n) \in \mathbb{R}^n$, jfr Sætning (3.3), gælder, at $\mathfrak{p} \supseteq (\mathbf{f})$, hvis og kun hvis $f_j(p) = 0$ for $j = 1, \ldots, s$. Sådanne primidealer svarer altså til punkter $p \in \mathbb{R}^n$, der tilfredsstiller ligningerne,

$$f_j(x) = 0 \text{ for } j = 1, \ldots, s. \tag{3.11.1}$$

Betragt nu et punkt $p \in \mathbb{R}^n$ i løsningsmængden til ligningerne (3.11.1). Lad r være rangen af Jacobi-matricen $\partial\mathbf{f}(p)$. Da gælder:

Sætning. *Den lokale ring $\overline{R}_{\mathfrak{p}}$ er regulær (nødvendigvis af dimension $n-r$), hvis og kun hvis løsningsmængden til ligningerne* (3.11.1) *i en omegn af p er en glat $\mathcal{C}^\infty$ mangfoldighed af dimension $n - r$.*

Bevis. Antag først, at den lokale ring $\overline{R}_{\mathfrak{p}}$ er regulær. Med betegnelserne fra Sætning (3.8) betragtes polynomiet h. Betingelsen $h(x) \neq 0$ for punkter x i $\mathbb{R}^n$ bestemmer da en åben delmængde U af $\mathbb{R}^n$. Af Sætning (3.8) følger, at de s ligninger (3.11.1) i den åbne delmængde U er ensbetydende med de r ligninger $f_j(x) = 0$ for $j = 1, \ldots, r$. Desuden har Jacobi-matricen $\partial\mathbf{f}^*$ for disse r ligninger i punktet p den maksimale rang r. Af sætningen om implicit givne funktioner følger derfor, at løsningsmængden i U til ligningerne i en omegn af p er en glat mangfoldighed af dimension $n - r$.

Antag omvendt, at løsningsmængden til ligningerne (3.11.1) i et givet punkt p er glat af dimension $n-r$. Det påstås, at den lokale ring $\overline{R}_{\mathfrak{p}}$ så er regulær (nødvendigvis af dimension $n - r$). Lad t være dimensionen af $\overline{R}_{\mathfrak{p}}$. Vælg først et polynomium h med $h(p) \neq 0$, så at brøkringen $S := \overline{R}[h^{-1}]$ har samme dimension t som $\overline{R}_{\mathfrak{p}}$. Ringen S er som $\mathbb{R}$-algebra frembragt af billederne x_i af X_i i S samt af $1/h(x_1, \ldots, x_n)$. Ifølge Noether's Normaliseringslemma findes i S et sæt af t algebraisk uafhængige elementer $y_1, \ldots, y_t$, således at S er endeligt frembragt som modul over delringen $S_0 := \mathbb{R}[y_1, \ldots, y_t]$. Elementerne y_j i S har formen

$$y_j = \frac{\varphi_j(x_1, \ldots, x_n)}{h(x_1, \ldots, x_n)^{d_j}},$$

hvor φ_j'erne er polynomier. Højresiderne i disse ligninger definer $\mathcal{C}^\infty$-funktioner på den åbne delmængde U af $\mathbb{R}^n$, der er bestem ved uligheden $h(x) \neq 0$. Højresiderne bestemmer altså en $\mathcal{C}^\infty$-afbildning

$$\varphi\colon U \to \mathbb{R}^t.$$

Lad Z betegne den del af løsningsmængden til (3.11.1), som ligger i U. Det er velkendt, hvordan restriktionen $\varphi\colon Z \to \mathbb{R}^t$ er bestemt ved inklusionen $S_0 \subseteq S$: Et punkt p i Z svarer til et maksimalideal i S, og kontraktionen af dette maksimalideal til S_0 er et maksimalideal svarende til billedpunktet $q = \varphi(p)$. Da S er endeligt frembragt som modul over S_0 følger det specielt, at afbildningen $\varphi\colon Z \to \mathbb{R}^t$ har endelig fibre.

Nu var løsningsmængden ifølge antagelsen glat af dimension $n - r$ i en omegn af p. Der findes altså en åben delmængde V af $\mathbb{R}^{n-r}$ og en $\mathcal{C}^\infty$-afbildning $\psi\colon V \to Z$, som afbilder V homeomorft (og specielt injektivt) på en åben omegn i Z af punktet p. Den sammensatte afbildning $\varphi\psi$ er så en $\mathcal{C}^\infty$-afbildning $V \to \mathbb{R}^t$, og den har endelig fibre. Heraf følger let, at $n - r \leqslant t$. I Jacobi's ulighed, $t \leqslant n - r$, gælder derfor lighed, og den lokale ring $\overline{R}_{\mathfrak{p}}$ er derfor regulær ifølge Kriteriet.

Hermed er også det omvendte eftervist. □

(3.12) Eksempel. Betragt for $n = 2$ polynomiumsringen $R = k[X, Y]$ og polynomiet $f = Y^2 - X^2(X + 1)$. Øjensynlig er f et irreducibelt polynomium, og idealet (f) er altså et primideal $\mathfrak{p}_0$. Kvotienten $\overline{R} = R/(f)$ er altså et integritetsområde, af dimension 1. Jacobimatricen ∂f er søjlen med koordinaterne $-(3X^2 + 2X)$ og $2Y$. Betragt et primideal $\mathfrak{p} \supseteq (f)$, og lad x og y betegne billederne af X og Y i $R/\mathfrak{p}$. Da er

$$y^2 = x^2(x + 1), \quad \text{og } \partial f(\mathfrak{p}) = \begin{pmatrix} -(3x^2 + 2x) \\ 2y \end{pmatrix}$$

Betragt først tilfældet, hvor $x = 0$. Her følger det af ligningen, at også $y = 0$. At $x = y = 0$ betyder imidlertid, at X og Y tilhører $\mathfrak{p}$, og så må $\mathfrak{p}$ være maksimalidealet (X, Y) i R. Dette $\mathfrak{p}$ svarer til punktet $(0, 0)$ i k^2, jfr Lemma (3.3)(1). Den lokale ring $\overline{R}_{\mathfrak{p}}$ har her dimension 1, og matricen $\partial f(\mathfrak{p})$ er øjensynlig 0, og altså af rang 0. Der gælder altså ikke lighed i Jacobi's ulighed. Altså er den den lokale ring $\overline{R}_{\mathfrak{p}}$ ikke regulær, jfr Bemærkning (3.10).

Betragt dernæst tilfældet $x \neq 0$. Her får søjlen $\partial f(\mathfrak{p})$ rangen 1. Hvis nemlig $2y \neq 0$, dvs hvis $y \neq 0$ og karakteristikken ikke er 2, er dette klart. Hvis $y = 0$, så følger det af ligningen (idet $x \neq 0$), at $x = -1$, og så er $3x^2 + 2x = 1 \neq 0$. Og endelig, hvis karakteristikken er 2, så er $3x^2 + 2x = x^2 \neq 0$. Af Jacobi's kriterium følger derfor, at $\overline{R}_{\mathfrak{p}}$ er regulær.

En tilsvarende undersøgelse kan udføres med polynomierne $f = Y^2 - X^3$ og $f = Y^2 - X(X - 1)(X + 1)$.

(3.13) Eksempel. Betragt for $n = 3$ og $R = \mathbb{R}[X, Y, Z]$ de to polynomier $(f_1, f_2) = (XY, XZ)$. Mængden L af punkter (x, y, z) i $\mathbb{R}^3$, der opfylder ligningerne $xy = xz = 0$, er øjensynlig foreningsmængden af x-aksen ($y = z = 0$) og yz-planen ($x = 0$). Jacobi-matricen er

$$\partial f = \begin{pmatrix} y & z \\ x & 0 \\ 0 & x \end{pmatrix}.$$

Punktet $o = (0, 0, 0)$ er øjensynlig singulært. [Det svarer til maksimalidealet $o = (X, Y, Z)$ i R. Idealet $(\mathbf{f})$ er øjensynlig fællesmængden af primidealerne (X) og (Y, Z), så disse primidealer svarer til de to minimale primidealer i $\overline{R}$. Da begge disse primidealer er indeholdt i o, er $\overline{R}_o$ ikke engang et integritetsområde.]

Betragt et punkt $\mathfrak{p} \neq o$ på x-aksen. Heri har Jacobi-matricen rangen 2 (da $x \neq 0$), og L er glat af dimension 1 nær $\mathfrak{p}$. Altså er $\overline{R}_\mathfrak{p}$ regulær af dimension 1.

Betragt dernæst et punkt $\mathfrak{p} \neq o$ i yz-planen. Heri har Jacobi-matricen rangen 1 (da enten $y \neq 0$ eller $z \neq 0$), og L er glat af dimension 2 nær $\mathfrak{p}$. Altså er $\overline{R}_\mathfrak{p}$ regulær af dimension 2. Bemærk, at punktet $\mathfrak{p}$ her i en vis forstand er singulært for Jacobi-matricen. I $\mathfrak{p}$ er rangen lig med 1, men i en omegn af $\mathfrak{p}$ er rangen lig med 2 næsten overalt. Det er således ikke kun ved at se på Jacobi-matricen, at man kan indse, at L nær $\mathfrak{p}$ er glat af dimension 2.

Lidt om algebraisk geometri

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

1. Affine mangfoldigheder.

(1.1) Definition. Ved indsættelse af et punkt $p = (p_1, \dots, p_n)$ i et polynomium F fremkommer værdien $F(p) = F(p_1, \dots, p_n)$. 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 delmængde $\mathfrak{F}$ af $k[X_1, \dots, X_n]$, 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 $R = k[X_1, \dots, X_n]$. Lad nemlig $\mathfrak{F}$ være en mængde af polynomier. Da udgør de polynomier, der kan skrives på formen $G_1 F_1 + \dots + G_l F_l$, 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 $F_1, \dots, F_r$, og så følger det, at $\mathcal{V}(\mathfrak{I}) = \mathcal{V}(F_1, \dots, F_r)$.

(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 $k[X_1, \dots, X_n]$ 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 $k[X_1, \dots, X_n]$, 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 $k[X_1, \dots, X_n] \to k$ 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 $k[X_1, \dots, X_n]$. Det er velkendt, og let at vise, at idealet netop er maksimalidealet,

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

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

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 $k[X_1, \dots, X_n]$ 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 $R = k[X_1, \dots, X_n]$ 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 $k[X_1, \dots, X_n]$. 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,

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

hvor F_i'erne er polynomier i de variable $X_1, \dots, X_{n-1}$. Ved indsættelse af et vilkårligt $(n-1)$-sæt $p' = (p_1, \dots, p_{n-1})$ 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 $p' = (p_1, \dots, p_{n-1})$ 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* $k[X_1, \dots, X_n]$ *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* $k[X_1, \dots, X_n]$. *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 $k[X_1, \dots, X_n]$. Da ringen $k[X_1, \dots, X_n]$ 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 ringhomomorfi $k[X_1, \dots, X_n] \to \Gamma(V)$. 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,

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

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,

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

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 $k[X_1, \dots, X_n]$.*
(iii) *Koordinatringen $\Gamma(V)$ er et integritetsområde.*

Bevis. Da $k[X_1, \dots, X_n]/\mathcal{I}(V) \xrightarrow{\sim} \Gamma(V)$, 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,

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

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 $i = 1, \dots, n$, 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 $g_1, \dots, g_n$ 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 $k[X_1, \dots, X_n]$, som opfylder ligningen,*

$$F(g_1, \dots, g_n) = 0. \tag{$*$}$$

(3) *Lad V være en mangfoldighed i k^n bestemt ved delmængden $\mathfrak{F}$ af $k[X_1, \dots, X_n]$. 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 $k[X_1, \dots, X_n]$. 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 $F(G_1, \dots, G_n)$. 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,

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

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 $i = 1, \dots, n$. Dette sæt af billeder kan ikke foreskrives vilkårligt; af isomorfien (1.11.1) ses, at et foreskrevet sæt $g_1, \dots, g_n$ af billeder definerer en homomorfi af k-algebraer, hvis og kun hvis følgende betingelse er opfyldt:

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

På den anden side svarer sæt af n polynomiumsfunktioner $g_1, \dots, g_n$ 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. $\square$

(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 $k[X_1, \dots, X_n] \to \Gamma(V)$. Af Sætning (2.3)(2) følger, at homomorfien $k[X_1, \dots, X_n] \to \Gamma(W)$ 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 $w_1, \dots, w_m$ er koordinatfunktionerne på W, så er $\Gamma(W) = k[w_1, \dots, w_m]$, og værdierne er altså polynomier i w_j'erne. Ligningerne har altså formen,

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

hvor G_i'erne er polynomier i m variable. Men det skal understreges, at disse ligninger ikke kan foreskrives vilkårligt. Betingelsen er, at højresiderne $g_i = G_i(w_1, \dots, w_m)$ opfylder, at $F(g_1, \dots, g_n) = 0$ 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 $(w_1, \dots, w_m)$ afbildes på det punkt i V, hvis v-koordinater er bestemt ved ligningerne,

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

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 $k[X_1,\dots,X_n]$ er netop idealerne af formen $\mathfrak{M}_p = (X_1-p_1,\dots,X_n-p_n)$ for $p\in k^n$.*

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

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

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

Bevis. (1) Lad $\mathfrak{M}$ være et maksimalideal i $k[X_1,\dots,X_n]$. Betragt kvotientringen $A := k[X_1,\dots,X_n]/\mathfrak{M}$. 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 $i=1,\dots,n$ 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 $k[X_1,\dots,X_n]$, 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 $R := k[X_1,\dots,X_n]/\mathfrak{I}$, 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 $k[X_1,\dots,X_n]$, som indeholder $\mathfrak{I}$ og ikke indeholder F. Altså er

$$\mathfrak{I}\subseteq\mathfrak{P} \quad\text{og}\quad F\notin\mathfrak{P}. \tag{$*$}$$

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 $i = 1, \dots, n$ elementer $p_i \in k$ således at X_i og p_i har samme billede ved den sammensatte homomorfi,

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

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 $k[X_1, \dots, X_n]$, dvs de idealer, der er lig med deres eget radikal. Ved den bijektive forbindelse fra* (1.7) *svarer primidealerne i $k[X_1, \dots, X_n]$ 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 $k[X_1, \dots, X_n]$ 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 $m_j \geqslant 1$). 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 $k[X_1, \dots, X_n]$ 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. $\square$

(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: $\Gamma(V) = k[X_1, \dots, X_n]/\mathcal{I}(V)$, 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 $k[X_1, \dots, X_n]$, 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 ekstension 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 ekstensionen hele ringen $\mathcal{O}_{V,p}$. I modsat fald, dvs hvis alle funktioner i $\mathfrak{I}$ forsvinder i punktet p, så er ekstensionen 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 $k[X_1, \dots, X_n]$.

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 $k[X_1, \dots, X_n]$. 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 $k[X_1, \dots, X_n]$. 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,

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

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

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

De rationale punkter er karakteriseret ved at homomorfien $k \to \kappa(p)$ 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 $k[X_1, \dots, X_n]$.

Igen vil vi på trods af ordlyden aldrig opfatte et skema som værende en kvotientring af $k[X_1, \dots, X_n]$. 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 $k[X_1, \dots, X_n]$. Den kvotient af $k[X_1, \dots, X_n]$, 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 $k[X_1, \dots, X_n]/\mathfrak{I}$. 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,

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

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 $k[X_1, \dots, X_n]$, 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 $k[X_1, \dots, X_n]$, 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 $\Gamma(X) = k[X_1, \dots, X_n]/\mathcal{I}(X)$; 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 $k[X_1, \dots, X_n]$. Da gælder formlen,*

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

Bevis. (1) Ifølge definitionen svarer et punkt i $\mathbf{A}^n$ til et maksimalideal $\mathfrak{M}$ i polynomiumsringen $k[X_1, \dots, X_n]$ og restklasselegemet er kvotienten $k[X_1, \dots, X_n]/\mathfrak{M}$. 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 $k[X_1, \dots, X_n]$. 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 $k[X_1, \dots, X_n]$, altså at kvotienten $\kappa := k[X_1, \dots, X_n]/\mathfrak{M}$ 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 κ, er også κ endeligdimensional over k. Altså er κ hel over legemet k og et integritetsområde. Heraf følger som bekendt, at κ 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 $k[X_1, \dots, X_n]$, 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 $k[X_1, \dots, X_n]$. 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,

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

så kvotienten $\Gamma(X)/\mathfrak{M}$ er isomorf med billedet ved denne homomorfi. Billedet er en delalgebra af $\kappa(q)$. Da $\kappa(q)$ 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 $\kappa(\varphi q)$ for billedpunktet er et dellegeme af $\kappa(q)$. Specielt er graden af billedpunktet φq en divisor i graden af q. Mere præcist: Som vektorrum over $\kappa(\varphi q)$ er legemet $\kappa(q)$ 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 ekstensionen $\mathfrak{I}B$ 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 $\operatorname{long}\Gamma(X) \leqslant \dim_k \Gamma(X)$. 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*

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

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

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

Multipliciteten $m := \operatorname{mult}_p(X)$ 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 $\operatorname{mult}_p(X)$, 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 $k[y_1, \dots, y_d]$ frembragt af et sæt af d algebraisk uafhængige elementer $y_1, \dots, y_d$. Delalgebraen er altså isomorf med polynomiumsringen $k[Y_1, \dots, Y_d]$, og inklusionen af delalgebraen svarer til en injektiv homomorfi $k[Y_1, \dots, Y_d] \to \Gamma(X)$. „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 $\kappa(p) = A/\mathfrak{m}$. Yderligere er restklasselegemet $\kappa(p)$ 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 ekstensionen $\mathfrak{m}B$ 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 $k[X_1, \dots, X_n]$, at for enhver kæde af primidealer (5.9.1) er $d \leqslant n$, og at der eksisterer en kæde med $d = n$. Eksistensen indses ved at betragte kæden defineret ved $\mathfrak{p}_i = (X_1, \dots, X_i)$.

Uligheden vises således: Kvotienten $A_i := k[X_1, \dots, X_n]/\mathfrak{p}_{i-1}$ 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 $k[X_1, \dots, X_n]$ 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 $\dim Y \geqslant \dim X$ og $\dim X \geqslant \dim Y$ 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 $\dim Y \geqslant d$. Da (5.8.1) var en vilkårlig kæde, sluttes at $\dim Y \geqslant \dim X$.

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 $\dim X \geqslant \dim Y$.

(3) Ifølge Noether's Normaliseringslemma findes i $\Gamma(X)$ et sæt af d algebraisk uafhængige elementer $y_1, \dots, y_d$ således at $\Gamma(X)$ er endeligt frembragt som modul over delalgebraen $k[y_1, \dots, y_d]$. Antallet d er som bekendt transcendensgraden $\operatorname{tdeg}_k \Gamma(X)$. Inklusionen af $k[y_1, \dots, y_d]$ 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. $\square$

(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. $\square$

(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 $i = 1, \dots, t$ og ikke for $i = t+1, \dots, r$. 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 $\operatorname{mult}_p(C)$. 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*

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

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 $i \geqslant h$. 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,

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

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 $i \geqslant h$, 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 $\kappa(p)$, jfr (4.4). Ifølge Hilbert's Nulpunktssætning (4.5) er restklasselegemet $\kappa(p)$ 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 $i_p(C.D) = \operatorname{mult}_p(C \cap D)$, 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 $S_i X_i$ tilhører idealet (F, G). For $i = 1, 2$ findes derfor polynomier B_{i1} og B_{i2} så at

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

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

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

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 $s_1 s_2 \neq 0$, 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

$$i_p(C.D) \geqslant \operatorname{mult}_p(C) \cdot \operatorname{mult}_p(D),$$

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 $i_o(C.D) = \operatorname{mult}_o(C) \cdot \operatorname{mult}_o(D)$ gælder, hvis og kun hvis de homogene led af laveste orden i F og G er primiske.

(7.7) Multiplicitetssætningen. *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 $0 \leqslant i_p(F.G) \leqslant \infty$. 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,

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

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 $F = X_2^d H$, 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 $d \geqslant e$. 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,*

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

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 $\operatorname{mult}_p(C \cap D)$. 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 $\Gamma_{\leqslant h}$ 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:*

$$\begin{aligned}
(F, G) \cap \Gamma_{\leqslant h} &= \Gamma_{\leqslant h-c} F + \Gamma_{\leqslant h-d} G \text{ for alle } h, \text{ og} && (7.12.1)\\
&= \Gamma_{\leqslant h-c} F \oplus \Gamma_{\leqslant h-d} G \text{ for } h < c+d, && (7.12.2)\\
\Gamma_{c+d-1} &= \Gamma_{d-1} F_c \oplus \Gamma_{c-1} G_d, && (7.12.3)\\
\Gamma_h &= \Gamma_{h-c} F_c + \Gamma_{h-d} G_d \text{ for } h \geqslant c+d-1, && (7.12.4)\\
\Gamma &= (F, G) + \Gamma_{\leqslant h} \text{ for } h \geqslant c+d-2. && (7.12.5)
\end{aligned}$$

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

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

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 $a \leqslant h - c$. 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 $0 = A_aF_c + B_bG_d$ (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 $i + j = h \geqslant c + d - 1$, tilhører højresiden. Et sådan monomium kan øjensynlig skrives som et produkt $M = M_1M_2$ 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 $l \leqslant h$ er polynomiet selv af grad højst h. Hvis $l > h$, så er specielt $l \geqslant c+d-1$. 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 $\Gamma = (F, G) + \Gamma_{\leqslant h}$. Isomorfien i Noether's første Isomorfisætning er altså en isomorfi,

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

På højresiden er tælleren og nævneren endeligdimensionale over k. Tællerens dimension er lig med antallet af monomier $X_1^i X_2^j$ med $i + j \leqslant h$, 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 $i_p(\mathfrak{c}) \leqslant i_p(\mathfrak{c}')$, 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,

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

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,

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

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,

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

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

$$H = AF + BG, \tag{$*$}$$

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. $\square$

(8.3) Korollar (Pascal's Sætning). *Betragt en sekskant indskrevet i et keglesnit D, dvs en følge af 6 (forskellige) rationale punkter $p_1, \dots, p_6$ 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 $i = 1, \dots, 6$ (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 Bezout'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 Noether's 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. $\square$

(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

$$C.L = p + q + r. \tag{$*$}$$

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 $i + j \geqslant n$. 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 $n \leqslant 0$ 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,

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

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,

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

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,

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

(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 $n \geqslant c + d - 1$. 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:* $\dim_k \Gamma_{<n}/(F, G)_{<n} \leqslant cd$.
(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,

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

idet den første ligning er observeret i (9.1) (her bruges, at $n \geqslant c + d - 1$), 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 $a+c \geqslant n$), 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 $n \geqslant c+d-1$. 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,*

$$\dim_k \Gamma/(F,G) \leqslant (\deg F)(\deg G),$$

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 $n \geqslant c+d-1$. 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,

$$\dim \Gamma_{<n}/(F,G)_{<n} \;\leqslant\; \dim \Gamma/(F,G) \;\leqslant\; cd\,, \tag{9.5.1}$$

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 $n \geqslant c+d-1$, 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 $n \geqslant f+g-1$. 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:* $\dim_k \Gamma/(\mathfrak{M}^n, F, G) \geqslant fg$.

(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

$$\begin{aligned}
\dim\Gamma/(\mathfrak{M}^n, F, G)^n &\geqslant \dim\Gamma^n - \dim\Gamma^{n-f} - \dim\Gamma^{n-g} + \dim\Gamma^{n-f-g}\\
&= \binom{n+1}{2} - \binom{n-f+1}{2} - \binom{n-g+1}{2} + \binom{n-f-g+1}{2}\\
&= fg,
\end{aligned}$$

idet den første ligning er observeret i (9.1) (her bruges, at $n \geqslant f+g-1$), 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,

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{M}^{n-f} \oplus \mathfrak{M}^{n-g} \arrow[r] \arrow[d, "\mu"'] & \Gamma \oplus \Gamma \arrow[r] \arrow[d, "\nu"'] & \Gamma^{n-f} \oplus \Gamma^{n-g} \arrow[r] \arrow[d, "\beta^n"] & 0\\
0 \arrow[r] & \mathfrak{M}^n \cap (F, G) \arrow[r] & (F, G) \arrow[r] & \Gamma^n, &
\end{tikzcd}$$

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,

$$0 \longrightarrow \operatorname{Ker}\mu \longrightarrow \operatorname{Ker}\nu \longrightarrow \operatorname{Ker}\beta^n \longrightarrow \operatorname{Coker}\mu \longrightarrow 0.$$

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,

$$0 \longrightarrow \operatorname{Im}\alpha^n \to \operatorname{Ker}\beta^n \to \operatorname{Coker}\mu \longrightarrow 0.$$

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. $\square$

(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,*

$$\dim_k \mathcal{O}/(F,G)\mathcal{O} \geqslant (\operatorname{mult}_o F)(\operatorname{mult}_o G),$$

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 $n \geqslant f+g-1$ gælder derfor ulighederne,

$$\dim \mathcal{O}/(F,G) = \dim \overline{\mathcal{O}} \geqslant \dim \overline{\mathcal{O}}/\mathfrak{m}^n = \dim \Gamma/(\mathfrak{M}^n, F, G) \geqslant fg, \tag{9.7.1}$$

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 $n \geqslant f + g - 1$, 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 $n \geqslant f+g-1$. 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. ∎

Associative algebraer

1. Simple og semisimple moduler og ringe.

(1.1) Setup. I dette kapitel betegner Λ en fast, ikke nødvendigvis kommutativ ring (med 1-element). Ved *radikalet* af Λ, betegnet $\mathfrak{r}(\Lambda)$, vil vi her forstå Jacobson-radikalet defineret som fællesmængden af alle maksimale venstre-idealer. Det er et ideal (to-sidet), og må naturligvis ikke forveksles med „nil-radikalet" af en kommutativ ring, bestående af de nilpotente elementer. Hvis A er kommutativ, ligger hvert nilpotent element øjensynlig i $\mathfrak{r}(A)$.

Moduler vil altid være venstre-moduler over Λ, med mindre andet udtrykkeligt er forudsat. Med Λ_s betegnes Λ som (venstre-)modul over sig selv. En modul S er som bekendt *simpel*, hvis $S \neq 0$ og S kun har trivielle undermoduler, eller, ækvivalent, hvis S er isomorf med en kvotient $\Lambda_s/\mathfrak{m}$, hvor $\mathfrak{m}$ er et maksimalt venstreideal i Λ.

(1.2) Semisimpel modul. Lad N være en undermodul i Λ-modulen M. Ved et *komplement* til N i M forstås en undermodul $K \subseteq M$ med $N \oplus K = M$, dvs således, at den kanoniske homomorfi $(n, k) \mapsto n + k$ er en isomorfi $N \oplus K \xrightarrow{\sim} M$.

En undermodul N i M, som har et komplement, kaldes en *direkte sumand* i M. Hvis N er direkte sumand i M er alle komplementer isomorfe, nemlig isomorfe med M/N.

Modulen M kaldes *semisimpel*, hvis enhver undermodul $N \subseteq M$ er direkte sumand i M.

(1.3) Observation. *Undermoduler og kvotientmoduler i en semisimpel modul M er igen semisimple.*

Bevis. Betragt nemlig først en undermodul $N \subseteq M$. Lad $N_0 \subseteq N$ være en undermodul i N. Så har N_0 et komplement i M, altså $N_0 \oplus K = M$, og så er det let at indse, at $K \cap N$ er et komplement i N til undermodulen N_0.

Den anden påstand følger af den første, thi for en kvotientmodul M/N har N et komplement K i M, og så er M/N isomorf med undermodulen K af M. ▯

(1.4) Lemma. *En semisimpel modul M er sum af simple undermoduler.*

Bevis. Nul-modulen er sum af den tomme mængde af undermoduler, så vi kan antage $M \neq 0$. Vi viser først, at M så har en simpel undermodul.

Med $m \neq 0$ i M er Λm nemlig så en cyklisk undermodul, isomorf med $\Lambda_a/\mathfrak{a}$, hvor $\mathfrak{a}$ er et ægte venstreideal i Λ. Af Zorns Lemma følger som bekendt, at det eksisterer et maksimalt venstreideal $\mathfrak{m} \supseteq \mathfrak{a}$. Den simple modul $S := \Lambda_s/\mathfrak{m}$ er så en kvotient af $\Lambda_s/\mathfrak{a} = \Lambda m$. Da M er semisimpel, er Λm semisimpel, og så er den simple kvotient S isomorf med en undermodul af Λm, og denne undermodul er så en simpel undermodul af M.

Lad nu M_0 være summen af alle simple undermoduler af M. Hvis $M_0 \subset M$, har M_0 er komplement $K \neq 0$. Ifølge det viste har K så en simpel undermodul, men det er i modstrid med at alle simple undermoduler af M er indehold i M_0. Altså er $M_0 = M$. $\square$

(1.5) Udskiftningssætningen. *Antag, at Λ-modulen M er sum af simple undermoduler S_i, $i \in I$. Lad $N \subseteq M$ være en undermodul. Da findes en delmængde $J \subseteq I$ således, at M er direkte sum af undermodulerne N og S_j for $j \in J$.*

Bevis,(for I endelig, ellers bruges Zorns Lemma). Lad J være maksimal blandt de delmængder $I' \subseteq I$, som opfylder at undermodulerne N og S_j for $j \in I'$ er uafhængige. Specielt er undermodulerne N og S_j for $j \in J$ uafhængige, og deres sum (der jo så er direkte),

$$M_0 := N \oplus \bigoplus\nolimits_{j \in J} S_j$$

er en undermodul af M. Vi skal vise, at $M_0 = M$. Antag, indirekte, at $M_0 \subset M$. Så findes $i \in I$ med $S_i \not\subseteq M_0$. Da S_i er simpel, følger det at $S_i \cap M_0 = 0$, og så er M_0 og S_i uafhængige. Da $J \subset J \cup \{i\}$, er det i modstrid med maksimaliteten af J. $\square$

(1.6) Sætning. *For en Λ-modul M er følgende betingelser ækvivalente:*

(i) *M er semisimpel.*
(ii) *M er sum af simple undermoduler.*
(iii) *M er direkte sum af simple undermoduler.*

Bevis. Implikationen (i) $\Rightarrow$ (ii) er Lemma (1.4), (iii) $\Rightarrow$ (i) er trivielt, og at (ii) medfører (i) og (iii) følger af Udskiftningssætningen. $\square$

(1.7). Der gælder en entydighedssætning om fremstillingen af en semisimpel modul som direkte sum af simple undermoduler. Vi begrænser os til følgende resultat:

Sætning. *Antag, at $M = \sum_{i \in I} S_i$ er sum af simple undermoduler S_i* (og altså semisimpel). *Da er enhver simpel undermodul af M isomorf med en af undermodulerne S_i. Yderligere gælder, at M har endelig længde, hvis og kun hvis M er endeligt frembragt. Er dette tilfældet gælder:*

M har en entydig fremstilling $M = S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}$, hvor undermodulerne S_j er simple og parvis ikke-isomorfe.

Bevis. Lad $S \subseteq M$ være en simpel undermodul. Da M er semisimpel er S isomorf med en kvotientmodul af M, så der findes en surjektiv homomorfi $M \to S$. Restriktion til S_i giver for hvert i en homomorfi $S_i \to S$. Mindst en af disse homomorfier må være forskellig fra nul-homomorfien, og den må så være en isomorfi $S_i \xrightarrow{\sim} S$.

Antag, at nu at M endeligt frembragt. Da M er semisimpel, kan vi antage at summen er direkte, $M = \bigoplus_{j \in J} S_j$. De endeligt mange frembringere har da kun koordinater forskellige fra 0 for endeligt mange indices j, og vi slutter, at J består af disse endeligt mange indices, altså at J er en endelig mængde, $M = S_1 \oplus \cdots \oplus S_p$. Heraf følger som bekendt, at M har endelig længde, og at undermodulerne S_i, med multiplicitet, er entydigt bestemte. $\square$

(1.8) Skævlegemer. Lad D være et skævlegeme. Det betyder som bekendt, at $D \neq 0$ og at hvert element $\lambda \neq 0$ i D har en invers. Det er nok at kræve, at hvert $\lambda \neq 0$ har en venstre-invers, og ækvivalent betyder det, at D har præcis to venstre-idealer, nemlig de to trivielle idealer. Med andre ord: *Ringen Λ er et skævlegeme, præcis når Λ som venstremodul over sig selv er simpel.*

Lad V være en D-modul (et D-*vektorrum*). For $v \neq 0$ er $Dv \simeq D_s$ en simpel undermodul, så trivielt er V altså sum af simple undermoduler. Altså er V en semisimpel D-modul, og derfor en direkte sum af simple undermoduler. Med andre ord: *Der findes en basis for V.*

Betragt et øjeblik for en vilkårlig ring Λ matrixringen $\mathrm{Mat}_n(\Lambda)$ og Λ-modulen Λ^n af søjler som $\mathrm{Mat}_n(\Lambda)$-moduler. Produktet αx for $\alpha \in \mathrm{Mat}_n(\Lambda)$ og $x \in \Lambda^n$ er blot produktet af matricen α med søjlen x.

For hver matrix $\alpha \in \mathrm{Mat}_n(\Lambda)$ er $x \mapsto \alpha x$ en *højre*-Λ-lineær afbildning $\Lambda^n \to \Lambda^n$. Det er let at se, at disse afbildninger er samtlige højre-Λ-lineære afbildninger $\Lambda^n \to \Lambda^n$, og mere præcist, at der etableres en ringisomorfi $\mathrm{Mat}_n(\Lambda) \xrightarrow{\sim} \mathrm{End}_\Lambda(\Lambda^n_d)$.

For skævlegemet D gælder der specielt det følgende resultat.

Lemma. *Modulen $S := D^n$ af søjler er simpel som modul over matrixringen $\Lambda := \mathrm{Mat}_n(D)$.*

Bevis. Det skal vises for hvert $x \neq 0$ i S, at $\Lambda x = S$, altså at der for hvert $x \neq 0$ i S og hvert $y \in S$ findes $\alpha \in \Lambda$ med $y = \alpha x$, altså at der findes en højre-D-lineær afbildning $\alpha\colon D^n \to D^n$ med $\alpha(x) = y$. Det følger af, at D^n er semisimpel som D-modul. Vektoren $x \neq 0$ kan derfor suppleres til en basis for D^n, og en højre-D-lineær afbildning α fra D^n kan bestemmes ved at foreskrive værdierne på denne basis. Specielt kan $\alpha(x) = y$ opnås. □

(1.8) Semisimple ringe. Ringen Λ kaldes *semisimpel*, hvis Λ er semisimpel som modul over sig selv, altså hvis Λ_s er en semisimpel Λ-modul. Som vi om lidt skal se, medfører dette, at også højre-modulen Λ_d er semisimpel. Der er således ingen grund til at skelne mellem (venstre-)semisimpel og højre-semisimpel.

For en semisimpel ring Λ er Λ_s endeligt frembragt og semisimpel, så der findes en entydig fremstilling,

$$\Lambda_s = S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}, \tag{1.8.1}$$

hvor undermodulerne S_i er parvis ikke-isomorfe. Specielt har Λ_s endelig længde. En cyklisk Λ-modul er en kvotient af Λ_s, og dermed semisimpel og isomorf med en direkte sum af nogle af modulerne S_i. Specielt er enhver simpel modul isomorf med en af modulerne S_i, og enhver Λ-modul er semisimpel.

Det er let at se, at et produkt $\Lambda = \Lambda_1 \times \cdots \times \Lambda_r$ af semisimple ringe igen er en semisimpel ring.

Et skævlegeme D er naturligvis en semisimpel ring af længde $\operatorname{long} D_s = 1$. Videre gælder:

Observation. *Matrixringen* $\mathrm{Mat}_n(D)$ *er en semisimpel ring af længden* $\operatorname{long}\mathrm{Mat}_n(D) = n$, *og modulen $S = D^n$ af søjler er den eneste simple* $\mathrm{Mat}_n(D)$*-modul.*

Bevis. Vi har nemlig set, at $S = D^n$ er simpel som modul over $\Lambda = \mathrm{Mat}_n(D)$. Lad $e_1, \dots, e_n$ være den kanoniske (højre-)D-basis for $S = D^n$. Afbildningen $\mathrm{Mat}_n(D) \to S^n$, bestemt

ved
$$\alpha \mapsto (\alpha e_1, \dots \alpha e_n),$$
knytter til matricen α sættet af matricens n søjler. Den er klart bijektiv, og trivielt en $\mathrm{Mat}_n(D)$-lineær afbildning. Altså er $\Lambda_s \xrightarrow{\sim} S^n$, hvoraf påstandene fremgår. ∎

(1.9) Første struktursætning. *For en ring Λ er følgende betingelser ækvivalente:*

(i) Λ_s *er semisimpel.*

(ii) *Enhver Λ-modul er semisimpel.*

(iii) Λ *er et endeligt produkt,*
$$\Lambda = \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_r}(D_r),$$
af matrixringe over skævlegemer D_i.

(iv) Λ_s *har endelig længde, og Λ er uden radikal, dvs $\mathfrak{r}(\Lambda) = 0$.*

Bevis. Implikationen (ii) $\Rightarrow$ (i) er triviel. Antag omvendt, at Λ_s er semisimpel. Det følger, at enhver kvotient af Λ_s, altså enhver cyklisk modul, er semisimpel og dermed en sum af simple undermoduler; da enhver Λ-modul er sum af cykliske undermoduler, følger det, at enhver Λ-modul er sum af simple undermoduler, og dermed semisimpel.

(i) $\Rightarrow$ (iii): Betragt fremstillingen (1.8.1). For $i \neq j$ er S_i og S_j ikke isomorfe, og derfor er $\mathrm{Hom}_\Lambda(S_i, S_j) = 0$. Heraf følger:
$$\Lambda^{\mathrm{op}} = \mathrm{End}_\Lambda(\Lambda_s) = \prod_i \mathrm{End}_\Lambda(S_i^n) = \prod_i \mathrm{Mat}_{n_i}(\mathrm{End}_\Lambda(S_i))$$
Videre gælder ifølge Schur's lemma, at endomorfiringen $D_i := \mathrm{End}_\Lambda(S_i)$ er et skævlegeme. Fremstillingen har altså formen
$$\Lambda^{\mathrm{op}} = \prod_i \mathrm{Mat}_{n_i}(D_i),$$
og heraf fås den ønskede fremstilling, blot med skævlegemerne D_i^{op}.

(i) $\Rightarrow$ (iv): Antag, at Λ er semisimpel. Af sætningen i (1.7) fremgår, at Λ_s har endelig længde. Specielt er radikalet $\mathfrak{r} = \mathfrak{r}(\Lambda)$ et endeligt frembragt venstre-ideal. Lad nu venstre-idealet $\mathfrak{a}$ være et komplement til $\mathfrak{r}$; specielt er så $\mathfrak{r} \cap \mathfrak{a} = (0)$. Vi har $\mathfrak{r}\mathfrak{a} \subseteq \mathfrak{a}$, og yderligere er $\mathfrak{r}\mathfrak{a} \subseteq \mathfrak{r}$, da $\mathfrak{r}$ er tosidet. Altså er $\mathfrak{r}\mathfrak{a} = (0)$. Nu følger det, at
$$\mathfrak{r} = \mathfrak{r}\Lambda = \mathfrak{r}(\mathfrak{r} + \mathfrak{a}) = \mathfrak{r}^2,$$
og Nakayama giver $\mathfrak{r} = (0)$.

[Alternativ: $\mathfrak{r}(\text{simpel}) = 0 \Rightarrow \mathfrak{r}(\text{semisimpel}) = 0 \Rightarrow \mathfrak{r}(\Lambda_s) = 0$ (når Λ_s er semisimpel.

(iv) $\Rightarrow$ (i): Da Λ_s har endelig længde, findes specielt kun endelig mange maksimale venstre-idealer $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ i Λ. Fællesmængden af idealerne $\mathfrak{m}_i$ er radikalet $\mathfrak{r} = (0)$. Det betyder, at den naturlige afbildning er injektiv:
$$\Lambda_s \hookrightarrow \Lambda_s/\mathfrak{m}_1 \oplus \cdots \oplus \Lambda_s/\mathfrak{m}_r.$$
Kvotienten $\Lambda_s/\mathfrak{m}_i$ er en simpel modul. Højresiden er derfor semisimpel. Altså er også undermodulen Λ_s semisimpel. ∎

(1.10) Simple typer. Lad Λ være en semisimpel ring, og vælge en fremstilling $\Lambda_s \simeq S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}$, hvor modulerne S_λ for $\lambda = 1, \dots, r$ er simple, og parvis ikke-isomorfe. Enhver simpel Λ-modul S er da isomorf med netop en af modulerne S_λ; modulen S siges at *være simpel af type* λ; der er altså r simple typer. Er M en Λ-modul, siges undermodulen

$$M(\lambda) = \sum\{S \mid S \subseteq M \text{ er simpel af type } \lambda\}$$

at være M's *isotypiske komponent af type* λ. Modulen M er den direkte sum af sine r isotypiske komponenter,

$$M = \bigoplus_\lambda M(\lambda),$$

thi da M er semisimpel, er $M = \sum M(\lambda)$, og summen er direkte: Ellers fandtes et λ således, at $M(\lambda) \cap \sum_{\mu\neq\lambda} M(\mu) \neq 0$; denne fællesmængde ville så indeholde en simpel undermodul S, men det er i modstrid med at enhver simpel undermodul af $M(\lambda)$ har type λ og enhver simpel undermodul af $\sum_{\mu\neq\lambda} M(\mu)$ må have type forskellig fra λ.

Det er klart, at $M(\lambda)$ er invariant under enhver Λ-endomorfi af M.

Andvendt på $M = \Lambda_s$ fås fremstillingen $\Lambda_s = \bigoplus \Lambda_s(\lambda)$. Komponenten $\mathfrak{a}_\lambda = \Lambda_s(\lambda)$ er en undermodul i Λ_s, altså et venstreideal i Λ. De er faktisk idealer, altså også højreidealer, idet der mere præcist gælder det efterfølgende resultat.

Sætning. *Komponenterne $\mathfrak{a}_\lambda$ for $\lambda = 1, \dots, r$ er idealer i Λ, og hvert ideal i Λ er en direkte sum af nogle af komponenterne $\mathfrak{a}_\lambda$.*

Bevis. Vi udnytter, at idealerne i Λ netop er de venstre-idealer, der er invariante under alle endomorfier af Λ_s.

Heraf følger klart, at hver komponent $\mathfrak{a}_\lambda$, og dermed også en sum af komponenter, er et ideal i Λ.

Lad omvendt $\mathfrak{b}$ være et ideal i Λ. Som venstreideal har vi fremstillingen $\mathfrak{b} = \bigoplus \mathfrak{b}(\lambda)$, og øjensynlig er $\mathfrak{b}(\lambda) \subseteq \mathfrak{a}_\lambda$. Det skal vises, at hvis $\mathfrak{b}(\lambda) \neq 0$, så er $\mathfrak{b}(\lambda) = \mathfrak{a}_\lambda$, eller, ækvivalent: Hvis $S, T \subseteq \Lambda_s$ er simple undermoduler af samme type λ, og $S \subseteq \mathfrak{b}$, så er $T \subseteq \mathfrak{b}$. Hertil bemærkes, at da S og T har samme type, findes en Λ-isomorfi $f\colon S \to T$. Da S er direkte sumand i Λ_s, kan f udvides til en Λ-lineær endomorfi $\tilde{f}\colon \Lambda_s \to \Lambda_s$, fx ved at sætte $\tilde{f} = 0$ på et komplement til S. Da $\mathfrak{b}$ er invariant under $\tilde{f}$ og $S \subseteq \mathfrak{b}$, følger det, at $T = \tilde{f}(S) \subseteq \mathfrak{b}$, som ønsket. □

(1.11) Simple ringe. Ringen Λ kaldes *simpel*, hvis Λ er semisimpel og har netop to idealer (som så må være (0), og Λ, og $\Lambda \neq 0$).

Sætning. *For en ring Λ er følgende betingelser ækvivalente:*

(i) *Λ er simpel.*
(ii) *Λ er semisimpel, og der findes netop en simpel type.*
(iii) *Der findes en isomorfi $\Lambda_s \simeq S^n$, hvor S er en simpel Λ-modul.*
(iv) *$\Lambda = \mathrm{Mat}_n(D)$ er (isomorf med) en matrixring over et skævlegeme.*
(v) *Λ_s har endelig længde, og der findes præcis to idealer i Λ.*

Bevis. Ækvivalensen følger umiddelbart af de foregående resultater. ∎

Det skal understreges, at man i litteraturen også kan møde egenskaben i (v), uden forudsætning om endelig længde, som definitionen på en simpel ring.

Bemærk, at de semisimple kommutative ringe netop er produkter af legemer, de simple er legemerne.

2. Associative algebraer.

I det følgende betegner R en *kommutativ* ring, men i almindelighed forudsættes ringe *ikke* at være kommutative.

(2.1) Modul med produkt. Lad A være en R-modul. Ved et *bilineært produkt* i A forstås en R-bilineær afbildning $A \times A \to A$. Et produkt er altså en komposition i A, betegnet $(a, b) \mapsto ab$, med bilinearitetskravene (for $a, b, c \in A$ og $r \in R$):

$$(a+b)c = ac + bc, \quad a(b+c) = ab + ac, \quad (ra)b = a(rb) = r(ab).$$

De to første ligninger udsiger, at den distributive lov er opfyldt.

Pålægges produktet eventuelt yderligere krav, fremkommer forskellige typer algebraer. Vi vil her alene omtale associative algebraer.

(2.2) Associative algebraer. Ved en *associativ R-algebra*, også kaldet en *associativ algebra over R*, forstås en R-modul A med et bilineært produkt, som er associativt og har et neutralt element (kaldet algebraens et-element). Udførligt burde det hedde en associativ algebra med et-element. I det følgende nøjes vi med ordet *algebra*.

I en R-algebra A er produktet specielt distributivt med hensyn til additionen i R-modulen A, så de ekstra krav sikrer, at A, med modulens addition og det givne produkt som multiplikation, er en ring. En R-algebra kan alternativt opfattes som en ring A, hvor der også er givet en multiplikation med skalarer fra R, som med ringens addition gør A til en R-modul, og således at multiplikation med skalar er *kompatibel* med ringens multiplikation i den forstand, at $r(ab) = (ra)b = a(rb)$.

Af kompatibiliteten fremgår specielt, at

$$(r1_A)a = a(r1_A) = ra.$$

Specielt kommuterer elementet $r1_A$ (for $r \in A$) med alle elementer i ringen A. Elementet ligger altså i *centret* $\mathrm{Cent}(A)$ for ringen A. Det er let at se, at afbildningen $r \mapsto r1_A$ er en ringhomomorfi,

$$\varphi\colon R \to \mathrm{Cent}(A) \hookrightarrow A. \tag{2.2.1}$$

Omvendt, hvis A er en given ring, og der er givet en ringhomomorfi (2.2.1), så organises A som R-algebra, idet modul-addition i A er ringens addition, og multiplikation med skalar er bestemt ved $ra := \varphi(r)a$. Det er faktisk i mange henseender enklest at opfatte en R-algebra A som et par (A, φ) bestående af en ring A og en ringhomomorfi $\varphi\colon R \to \mathrm{Cent}(A)$, kaldet *algebraens strukturhomomorfi*.

Bemærk, at idealer og venstre-idealer i ringen A automatisk er undermoduler i R-modulen A. Begreber som *R-delalgebra* og *R-kvotientalgebra*, og *R-algebrahomomorfi* og *billedalgebra* har oplagte definitioner.

(2.3) Eksempler. (1) Enhver given ring A kan opfattes som $\mathbb{Z}$-algebra med den kanoniske homomorfi $\mathbb{Z} \to A$ som strukturhomomorfi.

(2) Enhver ring A kan opfattes som algebra over enhver delring $R \subseteq \mathrm{Cent}(A)$.

(3) En *kommutativ R-algebra S* er blot en homomorfi $\varphi\colon R \to S$ mellem kommutative ringe. Specielt, for et givet ideal $\mathfrak{a} \subseteq R$ er $R/\mathfrak{a}$ en R-algebra.

(4) Matrixringen $\mathrm{Mat}_n(R)$ er en R-algebra, med strukturhomomorfien $r \mapsto r1_n$, hvor $r1_n$ er *skalar-matricen* med r i diagonalen.

(5) Endomorfiringen $\mathrm{End}_R(M)$ af en R-modul M er en R-algebra, med strukturhomomorfien $r \mapsto r1_M$, hvor $r1_M$ (eller r_M) betegner multiplikationen $x \mapsto rx$ med skalaren r.

(6) Polynomiumsringen $R[T]$ er en R-algebra, idet strukturhomomorfien er den naturlige inklusion $R \hookrightarrow R[T]$.

Observation. *Lad a være et element i en R-algebra A. Da findes netop en R-algebrahomomorfi $\psi\colon R[T] \to A$ således, at $\psi(T) = a$, nemlig afbildningen $p(T) \mapsto p(a)$. Billedalgebraen er den mindste delalgebra af A, som indeholder a; den er kommutativ* (og den betegnes $R[a]$).

(7) Polynomiumsringen $R[T_1, \dots, R_n]$ i n variable er en algebra over R, idet strukturhomomorfien er den naturlige inklusion $R \hookrightarrow R[T_1, \dots, T_n]$.

Observation. *Lad $a_1, \dots, a_n$ være et sæt af n kommuterende elementer i en R-algebra A. Da findes netop en R-algebrahomomorfi $\psi\colon R[T_1, \dots, T_n] \to A$ således, at $\psi(T_i) = a_i$ for $i = 1, \dots, n$, nemlig afbildningen $p(T_1, \dots, T_n) \mapsto p(a_1, \dots, a_n)$. Billedalgebraen er den mindste delalgebra, som indeholder $a_1, \dots, a_n$; den er kommutativ* (og betegnes $R[a_1, \dots, a_n]$).

(8) Gruppenalgebraen $R[G]$ (eller blot RG) for en given (multiplikativ) gruppe G defineres således: Som R-modul er det den direkte sum $R^{\oplus G}$, der kan opfattes som en fri R-modul med basiselementer e_s svarende til elementerne $s \in G$. Multiplikation defineres bilineært ved for basiselementer e_s og e_t at sætte

$$e_s \cdot e_t := e_{st}.$$

Elementerne i $R[G]$ er så summer $\sum_{s \in G} r_s e_s$, hvor $r_s \neq 0$ kun for endelig mange $s \in G$. Homomorfien $R \to R[G]$ er inklusionen $r \mapsto re_1$, hvor 1 er neutralelementet i gruppen G. Af definitionen følger, at $s \mapsto e_s$ er en multiplikativ homomorfi $G \hookrightarrow R[G]$. Gruppealgebraen $R[G]$ „indeholder“ altså G; når kompositionen i G (som her) er multiplikativt skrevet, fører det ikke til misforståelse blot at skrive s for elementet e_s i gruppealgebraen.

Definitionen af RG forudsætter i øvrigt kun at G er et *monoid*, dvs en mængde med en komposition, der er associativ og har et neutralt element.

Observation. *Lad $\alpha\colon G \to A$ være en multiplikativ homomorfi af G ind i en R-algebra A. Da findes netop en R-algebrahomomorfi $\psi\colon R[G] \to A$ således, at $\psi|G = \alpha$, nemlig afbildningen $\sum_s r_s s \mapsto \sum_s r_s \alpha(s)$.*

Når G er en gruppe, følger ligningen $\alpha(1) = 1$, hvor 1 står for det neutrale element i G og for et-elementet i A, af multiplikativiteten; hvis G blot er et monoid, må denne ligning forudsættes.

(9) Til hver mængde U hører et „frit monoid" $\mathcal{M}(U)$ frembragt af U. Monoidet $\mathcal{M}(U)$ består af alle endelige ord, inklusive det tomme ord, dannet med U som mængden af bogstaver. Produkt i $\mathcal{M}(U)$ er sammenkædning/sammenføjning af ord. Den tilhørende monoid-algebra $R[\mathcal{M}(U)]$ kan betegnes $R\langle U\rangle$. Hvis U endelig, $U = \{u_1, \dots, u_n\}$, bruges betegnelsen $R\langle u_1, \dots, u_n\rangle$.

(10) Et produkt af $A = A_1 \times \cdots \times A_n$ af R-algebraer A_i, med koordinatvise kompositioner, er igen en R-algebra.

(2.4) Moduler over en algebra. Lad A være en R-algebra. Ved en A-modul forstås blot en (venstre-)modul over ringen A. En A-modul M kan specielt opfattes som R-modul, idet multiplikation med skalarer fra R defineres via strukturhomomorfien $R \to A$. Den sidste homomorfi afbilder ind i centret $\mathrm{Cent}(A)$. Heraf følger, for $a \in A$, at multiplikation i M med skalaren a, betegnet a_M og givet ved $a_M(x) = ax$, er en R-lineær afbildning. Vi har altså $a_M \in \mathrm{End}_R(M)$. Det er let at se, at $a \mapsto a_M$ er en R-algebrahomomorfi,

$$A \to \mathrm{End}_R(M),$$

og det er af og til bekvemt at opfatte en A-modul M som et par (M, φ) bestående af en R-modul M og en R-algebrahomomorfi $\varphi\colon A \to \mathrm{End}_R(M)$.

(2.5) Eksempler. (1) En $R[T]$-modul M *er* (det samme som) en R-modul M med en given endomorfi $\alpha \in \mathrm{End}_R(M)$.

(2) En $R[T_1, \dots, R_n]$-modul M *er* en R-modul M med et givet sæt $(\alpha_1, \dots, \alpha_n)$ af kommuterende endomorfier $\alpha_i \in \mathrm{End}_R(M)$.

(3) En $R[G]$-modul M *er* en R-modul M med en given multiplikativ afbildning $G \to \mathrm{End}_R(M)$ (hvis G er en gruppe, er det automatisk en gruppehomomorfi $G \to \mathrm{Aut}_R(M)$). En $R[G]$-modul M kaldes også en R-lineær *repræsentation af* G (i M). For $M = R^n$ er $\mathrm{End}_R(R^n) = \mathrm{Mat}_n(R)$ (og $\mathrm{Aut}_R(M) = \mathrm{GL}_n(R)$), og repræsentationer i R^n kaldes også *matrixrepræsentationer*.

Specielt ses, når G er det frie monoid frembragt af $\{u_1, \dots, u_n\}$, at en $R\langle u_1, \dots, u_n\rangle$-modul *er* en R-modul M med et givet sæt $(\alpha_1, \dots, \alpha_n)$ af (ikke nødvendigvis kommuterende) endomorfier $\alpha_i \in \mathrm{End}_R(M)$.

(4) En modul M over et produkt $A = A_1 \times \cdots A_n$ er essentielt en familie $(M_1, \dots, M_n)$, hvor M_i er en A_i-modul. Mere præcist: For en given familie $(M_1, \dots, M_n)$ organiseres $M = M_1 \times \cdots \times M_n$ som A-modul, med koordinatvis multiplikation med skalarer fra A. Og enhver A-modul M har denne form: Idet $e_i \in A$ er skalaren med 1 på den i'te plads og 0 på de øvrige pladser, genfindes M_i ud fra M som $M_i = e_i M$.

Bemærk specielt, at A-undermoduler i $M_1 \times \cdots \times M_n$ har formen $N_1 \times \cdots \times N_r$, hvor N_i er en A_i-undermodul af M_i.

(2.5) Forskellige typer af algebraer. Lad A være en R-algebra. Specielt er A så en R-modul, men samtidig er A en ring, og dermed også en venstre- og højre-modul over sig selv. I forbindelse med modul-begreber kan det altså være vigtigt at præcisere, fra hvilke ringe skalarerne kommer.

Algebraen A kaldes *semisimpel*, eller *simpel*, hvis ringen A har egenskaben. Algebraen kaldes *venstre-noethersk*, *venstre-artinsk*, eller siges at have endelig *venstre-længde*, hvis ringen A har egenskaben som modul over sig selv. Venstre-idealer i ringen A er specielt undermoduler i R-modulen A, så hvis en af endelighedsbetingelserne er opfyldt for R-modulen A, er de også opfyldt for algebraen A.

Algebraen A kaldes en *divionsalgebra*, hvis ringen A et skævlegeme.

Algebraen A kaldes *endeligt frembragt* over R (eller mere præcist: endeligt frembragt som *som R-algebra*), hvis der findes endelig mange elementer $a_1, \dots, a_n \in A$ således, at A er den mindste delalgebra, der indeholder disse elementer; ækvivalent betyder det, at A er isomorf med en kvotient af $R\langle u_1, \dots, u_n\rangle$. Det må selvfølgelig ikke forveksles med, at A kan være *endeligt frembragt som R-modul*.

Trivielt gælder, at hvis en R-algebra A som R-modul er noethersk, artinsk, eller af endelig længde, så er A som modul over sig selv (både venstre- og højre-) noethersk, artinsk, af endelig længde.

(2.6) Tensorprodukt af algebraer. Lad A og B være R-algebraer. Opfattes A og B som R-moduler, kan vi danne tensorproduktet $A \otimes_R B$, der igen er en R-modul. Det er let (men omstændeligt) at se, at forskriften,

$$(a \otimes b)(a' \otimes b') := aa' \otimes bb',$$

bestemmer et veldefineret produkt i $A \otimes_R B$, og at $A \otimes_R B$ hermed er en R-algebra, kaldet *tensorproduktet* af A og B.

Øjensynlig er $A \otimes_R R = A$ og $R \otimes_R B = B$. De to afbildninger $a \mapsto a \otimes 1$ og $b \mapsto 1 \otimes b$ er homomorfier af R-algebraer,

$$\iota_A \colon A \to A \otimes_R B, \qquad \iota_B \colon B \to A \otimes B.$$

Er C endnu en R-algebra, siges to homomorfier $\alpha \colon A \to C$ og $\beta \colon B \to C$ at *kommutere*, hvis der for alle $a \in A$ og $b \in B$ gælder $\alpha(a)\beta(b) = \beta(b)\alpha(a)$. Øjensynlig kommuterer homomorfierne ι_A og ι_B.

Observation. *Lad $\alpha \colon A \to C$ og $\beta \colon B \to C$ være kommuterende R-algebrahomomorfier. Da findes netop en R-algebrahomomorfi $\psi \colon A \otimes_R B \to C$ således, at $\psi(a \otimes 1) = \alpha(a)$ og $\psi(1 \otimes b) = \beta(b)$.*

(2.7) Eksempler. (0) Lad $R \to S$ være en homomorfi mellem kommutative ringe. For en R-algebra A bliver $S \otimes_R A$ en S-algebra med strukturhomomorfien $\iota_S \colon S \to S \otimes_R A$. Den siges at fremgå af R-algebraen A ved at *udvide skalarringen fra R til S*.

(1) For en vilkårlig R-algebra A gælder:

$$A \otimes_R R[T] = A[T], \qquad \text{specielt: } R[X] \otimes_R R[Y] = R[X, Y].$$

(2) For en vilkårlig R-algebra A gælder:

$$A \otimes_R \mathrm{Mat}_n(R) = \mathrm{Mat}_n(A), \qquad \text{specielt: } \mathrm{Mat}_p(R) \otimes_R \mathrm{Mat}_n(R) = \mathrm{Mat}_n(\mathrm{Mat}_p(R))$$

$= \mathrm{Mat}_{np}(R)$; den sidste isomorfi fås ved at opfatte en $(np \times np)$-matrix som en blokmatrix bestående af n^2 blokke af $(p \times p)$-matricer.

(3) En $A \otimes_R B$-modul *er* en R-modul, som også er både en A-modul og en B-modul, som begge udvider multiplikation med skalarer fra R, og således, at multiplikation med skalarer a fra A kommuterer med multiplikation med skalarer b fra B, altså

$$a(bx) = b(ax), \quad a \in A, \quad b \in B, \quad x \in M.$$

At multiplikation med skalaren $a \in A$ kommuterer med multiplikation med skalarer fra B kan udtrykkes ved at endomorfien a_M er B-lineær, altså ved at homomorfien $a \mapsto a_M$ afbilder ind i delringen $\mathrm{End}_B(M)$. En modul M over $A \otimes_R B$ kan altså alternativt opfattes som en B-modul M med en given R-algebrahomomorfi,

$$A \to \mathrm{End}_B(M).$$

(4) En B^{op}-modul er det samme som en højre B-modul. I en $A \otimes_R B^{\mathrm{op}}$-modul er det derfor naturligt at skrive skalarer fra A til venstre og skalarer fra B til højre for modul-elementet. Kommutationsreglen i (3) får så form af en „kompatibilitet":

$$a(xb) = (ax)b, \quad a \in A, \quad b \in B, \quad x \in M.$$

En $A \otimes_R B^{\mathrm{op}}$-modul kaldes også en A-B-*bimodul*.

Bemærk specielt, at en A-A-bimodul er det samme som en $A \otimes_R A^{\mathrm{op}}$-modul: En R-modul, som er en venstre A-modul og også en højre-A-modul (som begge udvider multiplikation med skalarer fra R), og som opfylder kompatibilitetskravet ovenfor for $a, b \in A$. Ud over ringen $A \otimes_R A^{\mathrm{op}}$ som modul over sig selv, er A det oplagte eksempel på en A-A-bimodul. Undermodulerne, altså A-A-biundermodulerne i A, er netop idealerne (to-sidede) i A.

(5) Det er let for et endeligt produkt $A = A_1 \times \cdots \times A_n$ og en algebra B at bestemme en isomorfi,

$$(A_1 \times \cdots \times A_n) \otimes_R B = (A_1 \otimes_R B) \times \cdots \times (A_n \otimes_R B).$$

3. Divisionsalgebraer.

(3.1) Setup. I hele dette afsnit betegner k et givet (kommutativt) legeme. Algebraer forudsættes, når intet andet er nævnt, at være *endeligdimensionale* algebraer over k. Specielt er algebraerne af endelig længde, og specielt både noetherske og artinske.

Struktursætning. *For en endeligdimensional k-algebra A er følgende betingelser ækvivalente:*

(i) *A er semisimpel.*
(ii) *$A = \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_r}(D_r)$ er et produkt af matrixringe over endeligdimensionale divisionsalgebraer $D_1, \dots, D_r$.*
(iii) *A er uden radikal.*

Videre er følgende betingelser ækvivalente:

(i) *A er simpel.*
(ii) *$A = \mathrm{Mat}_n(D)$ er en matrixring over en endeligdimensional divisionsalgebra D.*
(iii) *A har netop to idealer.*

(3.2) Hovedsætning om gruppealgebra. *Lad k være et legeme, og lad G være en endelig gruppe. Gruppealgebraen kG har da dimension $\dim kG = |G|$. Yderligere gælder, hvis karakteristikken Char(k) ikke går op i ordenen $|G|$ (fx i karakteristik 0), at gruppealgebraen kG er semisimpel.*

Bevis. Lad $A = kG$ være gruppealgebraen. Det skal vises, at A-modulen $M := A_s$ er semisimpel, altså at der til hver A-undermodul $N \subseteq M$ findes en komplementær A-undermodul. Nu var M en A-modul, og specielt er M et vektorrum over k og N et underrum. Derfor findes i M et komplementært underrum V til N, hvor altså $M = N \oplus V$. Lad $\pi : M \to N$ være den tilhørende k-lineære projektion, bestemt ved $\pi(n + v) = n$. Af forudsætningen om karakteristikken følger, at ordenen $|G|$ har en invers i k. Vi kan derfor definere afbildningen $p : M \to N$ ved

$$p(x) = \frac{1}{|G|} \sum_{s \in G} s^{-1}\pi(sx).$$

Hvis $x \in N$, så er $sx \in N$ (da N var en A-undermodul), og da π var projektionen på N følger det at $\pi(sx) = sx$, og dermed er $s^{-1}\pi(sx) = x$; hvert led i summen ovenfor er altså lig med x, så vi får ligningen $p(x) = x$. Derfor er $p : M \to N$ en projektion. Yderligere er det let at se, at p er A-lineær. Derfor er kernen for p en A-undermodul, komplementær til N. □

(3.3) Eksempel. Et interessant spørgsmål er, hvornår man ud fra simpelhed, eller semisimpelhed om A og B kan slutte noget om tensorproduktet $A \otimes_k B$.

Betragt fx for et primtal p legemet $k = \mathbb{F}_p(t)$ (brøklegemet for polynomiumsringen $\mathbb{F}_p[t]$ over det endelige legeme med p elementer). Polynomiet $X^p - t$ er et irreducibelt polynomium. Adjungeres en rod α i dette polynomium til k, fremkommer et legeme $K = k(\alpha)$ af dimension p over k. Specielt er K en simpel algebra. Men tensorproduktet $K \otimes_k K$ er ikke engang en semisimpel algebra. Vi har nemlig

$$\big(\alpha \otimes 1 - 1 \otimes \alpha\big)^p = \alpha^p \otimes 1 - 1 \otimes \alpha^p = t \otimes 1 - 1 \otimes t = 0;$$

det sidste lighedstegn følger af at $t \in k$. Venstresiden $\alpha \otimes 1 - 1 \otimes \alpha$ er altså et ikke-trivielt nilpotent element i $K \otimes_k K$. Det følger, da $K \otimes_k K$ er kommutativ, at radikalet af $K \otimes_k K$ er ikke trivielt.

Vi undersøger spørgsmålet nærmere i det følgende.

(3.4) Central algebra. Hvis k-algebraen A ikke er nul-algebraen, er homomorfien $k \to A$ injektiv, og vi kan identificere k med billedet i A; der gælder altså

$$k \subseteq \mathrm{Cent}(A) \subseteq A.$$

Hvis algebraerne A og B ikke er nul, er homomorfierne $A \to A \otimes_k B$ og $B \to A \otimes_k B$ injektive; vi vil ofte identificere A og B med delalgebraer af $A \otimes_k B$. Med denne identifikation, altså $a = a \otimes 1$ og $b = 1 \otimes b$ for $a \in A,\ b \in B$, er

$$a \otimes b = (a \otimes 1)(1 \otimes b) = ab.$$

Algebraen A over k kaldes *central*, hvis $k = \mathrm{Cent}(A)$. Lad mere generelt M være en A-A-bimodul, altså en $A \otimes_k A^{\mathrm{op}}$-modul. Ved *centret for* M forstås delmængden, øjensynlig et k-underrum af M:

$$\mathrm{Cent}(M) := \{m \in M \mid am = ma \text{ for alle } a \in A\}.$$

Bimodulen M kaldes *central*, hvis den naturlige homomorfi $A \otimes_k \mathrm{Cent}(M) \to M$ er en isomorfi:

$$A \otimes_k \mathrm{Cent}(M) \xrightarrow{\sim} M. \tag{3.4.1}$$

(3.5) Observation. *Antag, at algebraen A er endeligdimensional og central over k. For en A-A-bimodul M er følgende betingelser ækvivalente:*

(i) *M er central.*
(ii) *Der findes en A-A-isomorfi $M \simeq A \otimes_k V$ med et vektorrum V over k.*
(iii) *Der findes en A-A-isomorfi $M \simeq A^{\oplus J}$ med en indexmængde J.*

Bevis. (i)$\Rightarrow$(ii) følger af definitionen, med $V := \mathrm{Cent}(M)$. Et valg af basis for et vektorrum V giver en isomorfi $V \simeq k^{\oplus J}$; derfor gælder (ii)$\Rightarrow$(iii). Det er let at bestemme centret for en direkte sum, så af (iii) fås $\mathrm{Cent}(M) \simeq k^{\oplus J}$, og dernæst isomorfien (3.4.1), dvs (i). ∎

(3.6) Observation. *En endeligdimensional k-algebra A er simpel, hvis og kun hvis A er simpel som modul over $A \otimes_k A^{\mathrm{op}}$.*

Bevis. Da A er antaget endeligdimensional over k, har A specielt endelig venstrelængde. Derfor er A en simpel ring, hvis og kun hvis A har præcis to idealer. Idealerne i A svarer til venstre-undermoduler i $A \otimes_k A^{\mathrm{op}}$-modulen A. Heraf følger påstanden umiddelbart. ∎

(3.7) Lemma. *Antag, at A er endeligdimensional, simpel og central over k. Lad M være en central A-A-modul. Da er enhver under-A-A-modul N af M ligeledes central, og altså lig med $A \otimes_k \mathrm{Cent}(N)$.*

Bevis. Med $A^{\mathrm{e}} := A \otimes_k A^{\mathrm{op}}$ er M en A^{e}-modul. Af forudsætningen følger, at A er en simpel A^{e}-modul, og af Observation (3.5) fås en A^{e}-isomorfi $M \simeq A^{\oplus J}$. Altså er M en semisimpel A^{e}-modul, og enhver simpel A^{e}-undermodul af M er isomorf med A. Heraf følger videre, at under-A^{e}-modulen N er isomorf med en direkte sum $N = A^{\oplus I}$, og nu følger det igen af Observation (3.5) at N er central, $N = A \otimes_k \mathrm{Cent}(N)$. □

(3.8) Hovedsætning. *Antag, at A og B er endeligdimensionale, simple algebraer, og at A er central over k. Da er $A \otimes_k B$ simpel, med centrum (som ring) lig med centret af ringen B.*

Bevis. Sæt $C := A \otimes_k B$. Da har C endelig dimension over k, og specielt endelig længde. For at vise, at C er simpel, er det altså nok at vise, at ethvert ideal $\mathfrak{c} \subseteq C$ er trivielt.

Anvend det foregående med $M := C$ som A^{e}-modul via faktoren A. Da er M central ifølge Observation (3.5), med $B = \mathrm{Cent}_A(C)$, hvor index A indikerer, at det er centret som A^{e}-modul. Idealet $\mathfrak{c}$ er specielt en A^{e}-undermodul, og derfor central ifølge Lemma (3.6), altså $\mathfrak{c} = A \otimes_k U$, hvor $U = \mathrm{Cent}_A(\mathfrak{c})$ er et k-underrum af B. Da $\mathfrak{c}$ var et ideal i C, er U invariant under venstre- og højre-multiplikation med elementer fra B. Det betyder, at U er et ideal i B. Da B er simpel, er der kun mulighederne $U = 0$ eller $U = B$, og altså kun mulighederne $\mathfrak{c} = 0$ eller $\mathfrak{c} = C$, som påstået.

Centret i ringen C består øjensynlig af de elementer i $\mathrm{Cent}_A(C) = B$, som kommuterer med multiplikation fra højre og venstre med elementer fra B. Centret er altså centret i B. □

(3.9) Korollar. *Antag, at A og B er endeligdimensionale, simple og centrale over k. Da er $C := A \otimes_k B$ simpel og central over k, og dermed isomorf med en matrixring $\mathrm{Mat}_n(D)$, hvor D er en central divisionsalgebra. Lad S være den simple C-modul, opfattet som en B-modul med en k-algebrahomomorfi $A \to \mathrm{End}_B(S)$, betegnet $a \mapsto a_S$, jfr. (3.6)(3). Da er D^{op} isomorf med A's kommutant i $\mathrm{End}_B(S)$, bestående af de B-endomorfier, der kommuterer med endomorfierne a_S for $a \in A$. Videre gælder ligningerne,*

$$\dim_k A \ \dim_k B = n^2 \dim_k D, \qquad \dim_k A \ \mathrm{long}_B B = n \,\mathrm{long}_B S.$$

(3.10) Korollar. *Lad D være en endeligdimensional, central divisionsalgebra over k. Da findes en isomorfi*

$$D \otimes_k D^{\mathrm{op}} \simeq \mathrm{Mat}_n(k).$$

Bevis. Sæt $C := D^{\mathrm{op}} \otimes_k D$. Da er D en simpel C-modul, idet C-undermodulerne i D er de tosidede idealer i D, og altså trivielle. Ifølge (3.9), anvendt med $A = D^{\mathrm{op}}$ og $B = D$, er $C = \mathrm{Mat}_n(E)$ simpel og central, og E^{op} er D^{op}'s kommutant i $\mathrm{End}_D(D)$. Denne kommutant er øjensynlig centret i D, altså lig med k. Altså er $E = k$, og $C = \mathrm{Mat}_n(k)$, som ønsket. □

(3.11) Skolem–Noether's sætning. *Lad $\varphi, \varphi' \colon A \to \mathrm{Mat}_n(D)$ være to k-algebrahomomorfier fra en endeligdimensional, simpel k-algebra A til en matrixring over en endeligdimensional, central divisionsalgebra D. Da er φ og φ' konjugerede i den forstand, at der findes en invertibel matrix $Q \in \mathrm{Mat}_n(D)$ således at*

$$\varphi'(a) = Q\varphi(a)Q^{-1} \quad \text{for alle } a \in A. \tag{3.11.1}$$

Bevis. Sæt $E := D^{\mathrm{op}}$. Den direkte sum D^n er en højre-D-modul, altså en E-modul, og de E-lineære afbildninger $D^n \to D^n$ er netop afbildningerne $x \mapsto Px$ med en matrix $P \in \mathrm{Mat}_n(D)$. Forbindelsen er en isomorfi af algebraer $\mathrm{End}_E(D^n) = \mathrm{Mat}_n(D)$, og den givne homomorfi φ er kan opfattes som en homomorfi af algebraer,

$$\varphi \colon A \to \mathrm{End}_E(D^n).$$

Herved organiseres D^n som en modul, betegnet M, over $A \otimes_k E$, jfr (3.6)(3), Tilsvarende betegnes med M' den $A \otimes_k E$-modul, der fås via homomorfien φ'.

Ifølge Hovedsætning (3.8) er $A \otimes_k E$ simpel. Altså er M og M' isomorfe med en direkte sum af eksemplarer af den simple $A \otimes_k E$-modul. Da M og M' er isomorfe som E-moduler (begge har dimension n), følger det, at M og M' er isomorfe som $A \otimes_k E$-moduler. Isomorfien $M \to M'$ er specielt E-lineær, og dermed af formen $x \mapsto Qx$ med $Q \in \mathrm{Mat}_n(D)$. At isomorfien også er A-lineær, betyder at

$$Q(\varphi(a)x) = \varphi'(a)(Qx),$$

for alle $a \in A$ og $x \in D^n$. Og den ligning, for alle $x = Q^{-1}y$, er ensbetydende med (3.11.1). □

(3.12) Bemærkning. I Skolem–Noether's sætning er homomorfierne, fra en simpel ring, nødvendigvis injektive, så billederne er to isomorfe simple delalgebraer af $\mathrm{Mat}_n(D)$. Sætningen formuleres ofte sådan: *Lad A og A' være simple delalgebraer af $\mathrm{Mat}_n(D)$, hvor D er en endeligdimensional, central divisionsalgebra over k. Enhver isomorfi $\psi \colon A \xrightarrow{\sim} A'$ kan da realiseres ved en indre automorfi i den forstand, at der findes en invertibel matrix $Q \in \mathrm{Mat}_n(D)$ således, at $\psi(a) = QaQ^{-1}$ for alle $a \in A$.*

(3.13) Korollar. *Lad D være en endeligdimensional, central divisionsalgebra over k, og lad $L \subseteq D$ være en maksimal kommutativ delalgebra af D. Da er L et legeme, og der findes en isomorfi af L-algebraer,*

$$L \otimes_k D \simeq \mathrm{Mat}_t(L), \quad \text{og } t = \dim_l L = \dim_L D.$$

Specielt er $\dim_k D = t^2$ et kvadrat.

Bevis. Vi kan opfatte D som (venstre) D-modul og som højre L-modul, altså som modul over $L^{\mathrm{op}} \otimes_k D = L \otimes_k D$. Da er D simpel som $L \otimes_k D$-modul, alene fordi D kun har trivielle venstreidealer. Anvend (3.9) med $A = L$ og $B = D$. Det følger, at $L \otimes_k D = \mathrm{Mat}_t(E)$, hvor E^{op} er isomorf med L's kommutant i $\mathrm{End}_D(D)$, og $n = \dim_k L$. Denne kommutant består øjensynlig af de elementer α i D, som kommuterer med alle elementer i L. For et sådant element α er $L[\alpha]$ øjensynlig igen en kommutativ delalgebra, og maksimaliteten af L sikrer derfor, at $\alpha \in L$. Altså er kommutanten lig med L, hvoraf $E = L$. Af $L \otimes_k D = \mathrm{Mat}_t(L)$ følger, at $\dim_k D = t^2$, og så følger det videre, at $\dim_D L = t$. □

(3.14) Frobenius' sætning. *På isomorfi nær findes kun tre endeligdimensionale divisionsalgebraer over $\mathbb{R}$, nemlig $\mathbb{R}$, $\mathbb{C}$ og $\mathbb{H}$.*

Bevis. Lad D være en divisionsalgebra over $\mathbb{R}$, lad k være centrum i D, og lad $L \supseteq k$ være en maksimal kommutativ delalgebra af D. Så er

$$\mathbb{R} \subseteq k \subseteq L \subseteq D.$$

Sæt $t = \dim_k L$, og altså også $t = \dim_L D$. Det er en simpel følge af algebraens fundamentalsætning, at en kommutativ divisionsalgebra over R, altså et legeme af endelig dimension over R, må være enten $\mathbb{R}$ eller $\mathbb{C}$. Hvis $\mathbb{R} \subset k$, må vi altså have $k = L = \mathbb{C}$, og dermed $t = 1$ og $D = \mathbb{C}$.

Antag derfor, at $\mathbb{R} = k$. Hvis $k = L$ får vi igen $t = 1$, altså $D = \mathbb{R}$.

Antag derfor yderligere, at $\mathbb{R} = k \subset L$. Heraf følger, at $L \simeq \mathbb{C}$, hvoraf $t = 2$ og $\dim_{\mathbb{C}}(D) = 2$. Lad $i \in L$ være den imaginære enhed (svarende til valg af en isomorfi $L \simeq \mathbb{C}$). Kompleks konjugering i L er en automorfi af L, og den er en indre automorfi ifølge Skolem–Noether's sætning. Der findes altså et element $j \in D$ således, at

$$jij^{-1} = -i. \tag{*}$$

Da $j \notin L$ er $1, j$ en L-basis for D, og $1, i, j, ij$ er følgelig en $\mathbb{R}$-basis for D.

Af (*) følger, at j^2 kommuterer med i, og derfor kommuterer j med de 4 elementer i $\mathbb{R}$-basen. Altså ligger j^2 i centret, dvs $j^2 \in \mathbb{R}$. Her gælder endda, at $j^2 < 0$, thi ellers var $j^2 = a^2$ med $a \in \mathbb{R}$, og $(j - a)(j + a) = 0$ medfører, at $j = \pm a \in \mathbb{R}$, en modstrid. Vi har altså $j^2 = -b^2$ med $b > 0$; erstattes j med j/b gælder (*) stadig, og nu kan det antages, at $j^2 = -1$. Ialt har vi så relationerne,

$$i^2 = -1, \quad j^2 = -1, \quad ij + ji = 0,$$

(den sidste ifølge (*)), og disse relationer bestemmer $\mathbb{H}$. $\square$

(3.15) Wedderburn's sætning. *Alle endelige skævlegemer er kommutative.*

Bevis. Lad D være et endeligt skævlegeme, lad k være centrum i D, og lad L være en vilkårlig maksimal kommutativ delring. Vi har

$$k \subseteq L \subseteq D.$$

Sæt $q := |k|$ og $t = \dim_k L$ ($= \sqrt{\dim_k D}$, uafhængigt af L). Legemet L har altså q^t elementer, og derfor er L spaltningslegeme for polynomiumet $X^{q^t} - X$ over k. Heraf følger videre, at alle maksimale kommutative delalgebraer $L \subseteq$ er k-isomorfe, fx isomorfe med en fast valgt L_0.

Ifølge Skolem–Noethers sætning er en isomorfi $L_0 \simeq L$ nødvendigvis indre, dvs af formen $a \mapsto yay^{-1}$ med $y \in D^*$, og L er altså konjugeret til L_0, dvs $L = yL_0y^{-1}$.

Ethvert element i D, og specielt ethvert element i D^*, er indeholdt i en kommutativ delalgebra L. Altså er

$$D^* = \bigcup_{y \neq 0} y L_0^* y^{-1}.$$

En sådan ligning, $G = \bigcup yHy^{-1}$, for en undergruppe H af en endelig gruppe G, kan imidlertid kun være opfyldt, hvis $H = G$. Antallet af konjugerede yHy^{-1} er jo $|G{:}N|$, hvor N er nomalisatoren af H, og hver konjugeret gruppe yHy^{-1} indeholder $|H|$ elementer. Elementantallet i foreningsmængden er altså $\leqslant |G:N| \cdot |H|$ og specielt $\leqslant |G|$. To forskellige undergrupper yHy^{-1} er ikke disjunkte. Hvis elementantallet er $= |G|$, er der altså kun én undergruppe yHy^{-1}, og $|H| = |G|$ medfører $H = G$.

Følgelig er $D^* = L_0^*$, og specielt er D kommutativ. □

(3.16) Separabel algebra. *For en endeligdimensional k-algebra A er følgende betingelser ækvivalente:*

(i) $A \otimes_k A^{\mathrm{op}}$ *er en semisimpel ring.*
(ii) *Den A-A-lineære multiplikationsafbildning $\mu\colon A \otimes_k A \to A$ har en A-A-lineær højreinvers.*
(iii) *Der findes et element $\sigma \in A \otimes_k A$ således, at $\mu(\sigma) = 1$ og $(a \otimes 1)\sigma = \sigma(1 \otimes a)$ for alle $a \in A$.*
(iv) *For enhver semisimpel k-algebra B er $B \otimes_k A$ semisimpel.*
(v) *For enhver endelig udvidelse $k \subseteq K$ af legemer er $K \otimes_k A$ semisimpel.*
(vi) *A er et produkt af matrixringe over endeligdimensionale divisionsalgebraer D_i,*

$$A = \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_r}(D_r),$$

hvor centret i D_i for $i = 1, \dots, r$ er en endelig separabel udvidelse af k.

(3.17) Eksempel.

(1) Gruppealgebraen $k[G]$ for en endelig gruppe G, hvis orden $|G|$ er invertibel i k, er separabel, med $\sigma = |G|^{-1} \sum (s^{-1} \otimes s)$.

(2) (Bruges/kan bruges i beviset for (3.16)) En separabel legemsudvidelse K/k er separabel som algebra over k. Hvis $K = k(\theta)$ og p er det minimale polynomium for θ, er $p'(\theta) \neq 0$. Vi har $k(\theta) = k[X]/(p)$, og kan identificere $K \otimes_k K$ med $K[X]/(p)$. Lad ξ være klassen af X i $K[X]/(p)$. Multiplicationen $\mu\colon K[X]/(p) \to K$ er bestemt ved $\xi \mapsto \theta$. I $K[X]$ har vi $p = (X - \theta)\beta$, hvor $\beta \in K[X]$. og heraf følger $(\xi - \theta)\beta(\xi) = 0$ og $\beta(\theta) = p'(\theta) \neq 0$. Nu virker $\sigma := \beta(\xi)/\beta(\theta)$.

Index for Kommutativ Algebra og Kommutativ Algebra II.