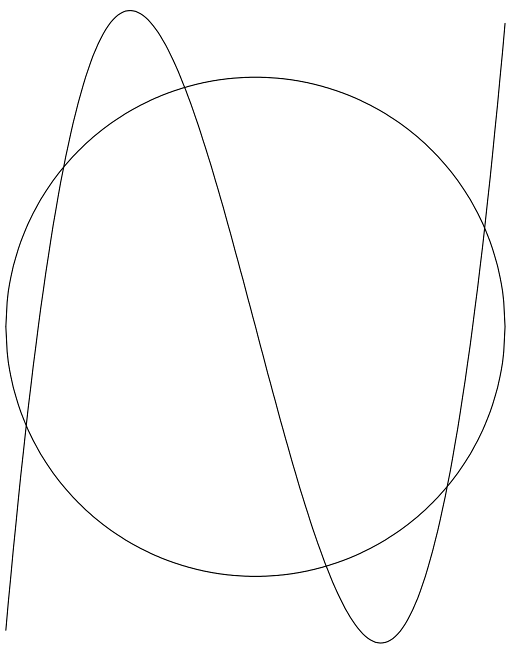
Matematik 3AG Forår 2003

Algebraisk Geometri

KURVER OG MODULER

Hans–Bjørn Foxby



$$0 \to (A/hA)_{\mathfrak{m}_P} \to (A/ghA)_{\mathfrak{m}_P} \to (A/gA)_{\mathfrak{m}_P} \to 0$$

INDHOLD & STIKORD

INDHOLD

Noterne består således af to *kapitler:* **PAK: Projektive Algebraiske Kurver** og **ROM: Ringe Og Moduler**, der er inddelt i *afsnit:* PAK 0, PAK 1, PAK 2, ... og ROM 1, ROM 2, ... , hvoraf PAK 0 er en indledning, der senere bliver overflødig. Den n'te side i afsnit i PAK m (henholdsvis ROM m) betegnes PAK $m.n$ (henholdsvis ROM $m.n$). Dele af teksten på en side kan mærkes med $(*)$, hvor $*$ er et tal, bogstav eller andet symbol, og henvisning til $(*)$ på side PAK $m.n$ (henholdsvis ROM $m.n$) sker ved PAK $m.n(*)$ (henholdsvis ROM $m.n(*)$), idet "overflødige" dele af henvisningen udelades, så alle henvisninger er så "lokale" som muligt: På side PAK 1.2 henviser

ROM 4.5(a) til ROM 4.5(a)
4.5(a) til PAK 4.5(a)
5(a) til PAK 1.5(a)
(a) til PAK 1.2(a)

Nogle stikord

Nogle symboler

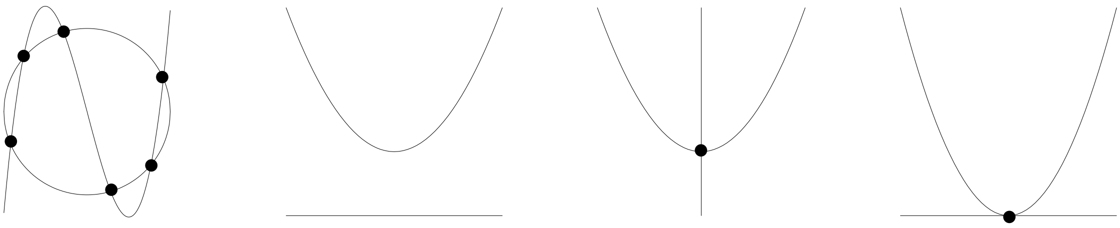
0. Indledning

Dette er en kort beskrivelse af et af hovedresultaterne i Matematik 3AG.

Lad C være en plan algebraisk kurve af grad m, det vil sige, at der findes et polynomium i to variable $p(x,y) = \sum_{i=0}^{m} \sum_{j=0}^{i} a_{i-j,j} x^{i-j} y^j$ af grad m (dvs. der findes j, så $a_{m-j,j} \neq 0$)[1], så C er nulpunktmængden for p, hvilket vil sige, at C består af netop de punkter (x,y) i planen, som opfylder $p(x,y) = 0$. Kort taler man om kurven $C : p(x,y) = 0$, hvor ligningen eventuelt omformes til et mere velkendt udseende. F.eks. er enhedscirklen en andengradskurve, nemlig $C : x^2 + y^2 = 1$ (svarende til polynomiet $f(x,y) = 1 - x^2 - y^2$ i to variable). Et andet eksempel er, at grafen for polynomiet $h(x) = 4x^3 - 3x$ (i én variabel) er trediegradskurven $D : y = 4x^3 - 3x$ (svarende til polynomiet $g(x,y) = 3x + y - 4x^3$ i to variable). I dette eksempel med to kurver af grader 2 og 3 er der 6 skæringspunkter, sml. figur (1) nedenfor. Det er ikke noget tilfælde:

Bezout's sætning. *Hvis C og D er plane algebraiske kurver af grader henholdsvis m og n og uden fælles komponent, da skærer C og D hinanden i netop mn punkter.*

(1) (2) (3) (4)



Kurverne skal være uden fælles komponenter, for at fællesmængden er endelig. F.eks. er foreningmænden $C \cup D$ en kurve med ligning $(1 - x^2 - y^2)(3x + y - 4x^3) = 0$, og den har to komponenter C og D, så fællesmængden med f.eks. kurven D er ikke endelig.

Tilsyneladende er Bezout's sætning ikke opfyldt i figurerne (2) – (4). Parabelen $E : y = x^2$ er med i alle tre figurer, den har grad 2. De andre kurver er førstegradskurver, nemlig linierne: $F : y = -1$, $G : x = 0$ og $H : y = 0$. I hvert af de tre tilfælde burde de to kurver altså have 2 skæringspunkter, men det er *tilsyneladende* ikke tilfældet i noget af dem. Det vil vise sig, at de 2 skæringspunkter er der alligevel, når man:

(a) *kigger ordentlig efter;*
(b) *ikke er snævertsynet;*
(c) *tæller korrekt.*

At "kigge ordentlig efter" betyder, at man f.eks. i (2) (selvfølgelig) også skal betragte de komplekse skæringspunkter; der er netop 2 skæringspunkter, som der skal være, nemlig $(-i, -1)$ og $(i, -1)$. (I formuleringen af Bezout's sætning kunne man have præciseret, at kurverne er *komplekse* kurver.)

For "ikke at være snævertsynet" skal man f.eks. i (3) ud over skæringspunktet $(0,0)$ også betragte skæringspunktet i "retningen" $(0,1)$ (dvs. i lodret retning) i det "uendelig fjerne", og herved er der netop 2 skæringspunkter. Dette med "retningen" i det "uendelig fjerne" bliver præciseret om lidt ved at indføre den *projektive plan* (og i formuleringen kunne man have nævnt, at kurverne er *projektive plane* kurver).

[1] Hvis man skriver $p(x,y) = \sum_{h,j} a_{hj} x^h y^j$, da er $m = \sup\{\, n \mid \exists\, h,j \in \mathbb{Z} \colon a_{hj} \neq 0 \wedge h + j = n \,\}$.

Også i 1(4) er der 2 skæringspunkter; skæringspunktet $(0,0)$ skal blot tælles dobbelt svarende til, at 0 er dobbeltrod i polynomiet $h(x) = x^2$. Det gælder altså om at "tælle korrekt", dvs. benytte de *snitmultipliciteter*, der bliver indført senere (og dette kunne have været nævnt i formuleringen).

Den projektive plan. I denne forbindelse kaldes planen $\mathbb{C}^2$ den *affine (komplekse) plan* og betegnes $\mathbb{A}^2_{\mathbb{C}}$. For "ikke at være snævertsynet" skal man udvide $\mathbb{A}^2_{\mathbb{C}}$ med alle mulige "retninger" (x_0, y_0), hvor $(x_0, y_0) \in \mathbb{C}^2 \setminus \{(0,0)\}$.

Mere præcist er den *projektive (komplekse) plan* mængden af linier i $\mathbb{C}^3$ gennem $(0,0,0)$, og den betegnes $\mathbb{P}^2_{\mathbb{C}}$. Da en linie gennem $(0,0,0)$ er bestemt ved en retningsvektor, kan ethvert element i $\mathbb{P}^2_{\mathbb{C}}$ repræsenteres ved et talsæt $(x_0, y_0, z_0) \in \mathbb{C}^3 \setminus \{(0,0,0)\}$, og $(x_0 : y_0 : z_0)$ betegner linien gennem $(0,0,0)$ med retningsvektor (x_0, y_0, z_0). Da to retningsvektorer bestemmer samme linie, netop når de er proportionale, gælder der, at $(x_1 : y_1 : z_1) = (x_2 : y_2 : z_2)$, netop hvis der findes $c \in \mathbb{C}$, så $(x_1, y_1, z_1) = c(x_2, y_2, z_2)$. Elementerne $(x_0 : y_0 : z_0)$ i $\mathbb{P}^2_{\mathbb{C}}$ kaldes *punkter*.

Den affine plan $\mathbb{A}^2_{\mathbb{C}}$ identificeres med en delmængde af $\mathbb{P}^2_{\mathbb{C}}$ ved at identificere $(x_0, y_0) \in \mathbb{A}^2_{\mathbb{C}}$ med $(x_0 : y_0 : 1) \in \mathbb{P}^2_{\mathbb{C}}$. De øvrige punkter i $\mathbb{P}^2_{\mathbb{C}}$, *punkterne i uendelig*, har formen $(x_0 : y_0 : 0)$, hvor $(x_0, y_0) \in \mathbb{C}^2 \setminus \{(0,0)\}$; disse punkter er "retningerne i det uendeligt fjerne".

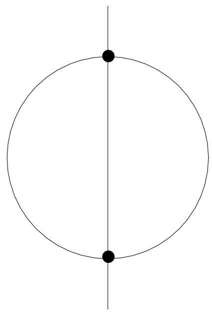
De kurver, der hidtil er nævnt, f.eks. kurverne $C : x^2 + y^2 = 1$ og $D : y = 4x^3 - 3x$, kaldes fra nu af *affine kurver*. De tilsvarende *projektive kurver* får man ved at *homogenisere:* $\bar{C} : x^2 + y^2 = z^2$ og $\bar{D} : yz^2 = 4x^3 - 3xz^2$. (Man ganger hvert led med potenser af z, så de alle får samme grad, hhv. 2 og 3.) En generel affin m'te gradskurve $C : p(x,y) = 0$ med $p(x,y) = \sum_{i=0}^m \sum_{j=0}^i a_{i-j,j} x^{i-j} y^j$ homogeniseres til $\bar{C} : \bar{p}(x,y,z) = 0$, hvor $\bar{p}(x,y,z) = \sum_{i=0}^m (\sum_{j=0}^i a_{i-j,j} x^{i-j} y^j) z^{m-i}$, der er et *homogent* polynomium af grad m (alle led har samme grad).

For et ikke-trivielt homogent polynomium $\bar{p}$ i tre variable og et punkt $(x_0 : y_0 : z_0) \in \mathbb{P}^2_{\mathbb{C}}$ med repræsentant (x_0, y_0, z_0) kan man ikke tale om værdien af $\bar{p}(x_0 : y_0 : z_0)$, fordi den afhænger af valg af repræsentanten. Men man kan godt tale om, at $\bar{p}(x_0 : y_0 : z_0)$ er nul; det er nemlig uafhængigt af valg af repræsentant. (Her kræves lidt eftertanke!) I figur 1(3) optræder $E : y - x^2 = 0$ og $G : x = 0$, der homogeniserer til hhv. $\bar{E} : yz - x^2 = 0$ og $\bar{G} : x = 0$. Punktet $(0 : 1 : 0)$ fra den projektive plan tilhører begge disse kurver (svarende til at kurverne går gennem "retningen" $(0,1)$ i det "uendelig fjerne").

Når $\bar{C}$ er en projektiv kurve givet ved $\bar{p}(x,y,z) = 0$, da fås den tilsvarende affine kurve ved ligningen $\bar{p}(x,y,1) = 0$; altså ved at sætte z lig 1. Den affine del af kurven $x^2 + y^2 - z^2 = 0$ har ligningen $x^2 + y^2 - 1 = 0$, som fremstiller enhedscirklen.

Koordinatskift. En isomorfi $\varphi : \mathbb{C}^3 \to \mathbb{C}^3$ inducerer en *vel*defineret afbildning $\varphi' : \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ ved at lade $\varphi'(x : y : z) \in \mathbb{P}^2_{\mathbb{C}}$ være repræsenteret af $\varphi(x,y,z)$. (Der er lidt at overveje her: $\varphi(x,y,z) \neq (0,0,0)$, og hvis $(x_1 : y_1 : z_1) = (x_2 : y_2 : z_2)$, dvs. (x_1, y_1, z_1) og (x_2, y_2, z_2) er proportionale, da er $\varphi(x_1, y_1, z_1)$ og $\varphi'(x_2, y_2, z_2)$ også proportionale, dvs. de repræsenterer samme punkt i $\mathbb{P}^2_{\mathbb{C}}$.) Man siger, at φ' er et *projektivt koordinatskift*. Hvis yderligere $\bar{p}$ er et homogent polynomium af grad m i tre variable, da er $\bar{p} \circ (\varphi')^{-1}$ ligeledes et homogent polynomium af grad m. Hvis C er den projektive kurve bestemt ved $\bar{p}$, da er billedet $\varphi'(C)$ af C ved φ' igen en projektiv kurve af grad m, nemlig bestemt ved polynomiet $\bar{p} \circ (\varphi')^{-1}$.

(1)



Projektive koordinatskift er fordelagtige, når man skal "kigge ordentlig efter" og "ikke være snævertsynet". Betragt f.eks. kurverne $E : y = x^2$ og $G : x = 0$ fra figur 1(3). Ved koordinatskiftet $\varphi'(x : y : z) = (x : \frac{1}{2}(-y+z) : \frac{1}{2}(y+z))$ går $\bar{E}$ og $\bar{G}$ over i kurverne henholdsvis $\varphi'(\bar{E}) : x^2+y^2-z^2 = 0$ og $\varphi'(\bar{G}) : x = 0$ (da $(\varphi')^{-1}(x : y : z) = (x : -y+z : y+z)$). De affine dele af disse kurver er vist på figur (1) ovenfor. Nu kan man "se" det "uendelig fjerne"skæringspunkt!

Koordinatskiftet $\psi'(x : y : z) = (-\frac{i}{2}(y+z) : x : \frac{i}{2}(y-z))$ fører kurverne $E : y = x^2$ og $F : y = -1$ fra figur 1(2) over i kurver med ligningerne hhv. $x^2 + y^2 - z^2 = 0$ og $x = 0$; altså de samme kurver som ovenfor, sml. figur (1) ovenfor. Nu er de 2 "imaginære" skæringspunkter blevet "synlige"!

Kurverne fra 1(2) og 1(3) kan altså koordinatskiftes over i samme kurver. Det er iøvrigt ikke noget tilfælde! Det vil fremgå af næste afsnit, at kurverne i figur 1(4) ikke kan koordinatskiftes over i kurver med 2 forskellige skæringspunkter, og dermed kan kurverne fra 1(4) ikke koordinatskiftes over i kurverne fra (1) ovenfor.

Snitmultipliciteter. Først omtales snitmultipliciteten $\mathrm{m}_{(0,0)}(C, D)$ i punktet $(0, 0)$ for affine kurver C og D. Polynomiumsringen $\mathbb{C}[x, y]$ er et vektorrum over $\mathbb{C}$, og (x, y) er et maximalideal i denne ring. Når man lokaliserer[2] $\mathbb{C}[x, y]$ i maximalidealet (x, y), får man en ring R, som også er et vektorrum over $\mathbb{C}$. Lad C og D være givet ved polynomierne p og q, og lad $(p, q)R$ være idealet i R frembragt af p og q. Hvis C og D ikke har fælles komponent, da kan man bevise, at restklasseringen $R/(p, q)R$ har endelig dimension som vektorrum over $\mathbb{C}$. Snitmultipliciteten defineres ved $\mathrm{m}_{(0,0)}(C, D) = \dim_{\mathbb{C}} R/(p, q)R$.

For vilkårlige projektive plane kurver $\bar{C}$ og $\bar{D}$ og et punkt $P \in \mathbb{P}^2_{\mathbb{C}}$ vælges et koordinatskift φ', så $\varphi'(P) = (0 : 0 : 1)$. (Dette er altid muligt!) Det viser sig, at $\mathrm{m}_{(0,0)}(\varphi'(\bar{C}), \varphi'(\bar{D}))$ ikke afhænger af valget af φ', og snitmultipliciteten i P for $\bar{C}$ og $\bar{D}$ defineres ved $\mathrm{m}_P(\bar{C}, \bar{D}) = \mathrm{m}_{(0,0)}(\varphi'(\bar{C}), \varphi'(\bar{D}))$. Hvis $P \notin \bar{C} \cap \bar{D}$, da er $\mathrm{m}_P(\bar{C}, \bar{D}) = 0$, og derfor har det mening at betragte summen $\sum_{P \in \mathbb{P}^2_{\mathbb{C}}} \mathrm{m}_P(\bar{C}, \bar{D})$.

Nu er vi forberedt til en præcis formulering af sætningen.

Bezout's sætning. *Hvis $\bar{C}$ og $\bar{D}$ er projektive komplekse plane kurver af grader henholdsvis m og n og uden fælles komponent, da gælder:*

$$\sum_{P \in \mathbb{P}^2_{\mathbb{C}}} \mathrm{m}_P(\bar{C}, \bar{D}) = mn\,.$$

Beviset kræver indgående forståelse af snitmultipliciteterne $\mathrm{m}_P(\bar{C}, \bar{D})$, og dermed de ringteoretiske konstruktioner, der fører frem til ringen og vektorrummet $R/(p, q)R$, og som derfor beskrives i dette kursus.

[2]Lokalisering er en proces, der beskrives i kurset.

1. Linier i den projektive plan

(1) **Grundlegemet.** I dette kursus benyttes de komplekse tals legeme $\mathbb{C}$. Det er nemlig straks vigtigt at kunne dividere med tal forskellige fra 0, sml. allerede (s) nedenfor. Endvidere udnyttes, at $\mathbb{C}$ er *algebraisk afsluttet* (dvs. ethvert ikke-konstant polynomium i én variabel har en rod), således at f.eks. kurverne i 0.1(2) har skæringspunkter. Endelig bliver der til tider brugt, at $\mathbb{C}$ har *karakteristik* 0 (dvs. de hele tals ring $\mathbb{Z}$ er en delring af $\mathbb{C}$). Faktisk gælder samtlige resultater i dette kursus over ethvert algebraisk afsluttet legeme af karakteristik 0.

(2) **Rummet.** I det 3–dimensionale komplekse rum $\mathbb{C}^3$ betegnes elementerne – dvs. vektorerne – med understregning: $\underline{x} = (x_1, x_2, x_3)$, mens elementerne i $\mathbb{C}^2$ skrives som talpar: (x_1, x_2). Specielt skrives nulvektorerne i $\mathbb{C}^3$ og $\mathbb{C}^2$ som henholdsvis $\underline{0}$ og $(0, 0)$.

Ofte betragtes det *udprikkede* rum $\mathbb{C}^3_{\varnothing} = \mathbb{C}^3 \setminus \{\underline{0}\}$, og nogle gange også den *udprikkede* plan $\mathbb{C}^2_{\varnothing} = \mathbb{C}^2 \setminus \{(0, 0)\}$.

To vektorer $\underline{u}, \underline{v} \in \mathbb{C}^3_{\varnothing}$ er *proportionale*, netop når der findes $a \in \mathbb{C}$, så $\underline{u} = a\underline{v}$. Bemærk, at i bekræftende fald er $a \neq 0$. Proportionalitet er en *ækvivalensrelation*:

(r) $\underline{u} = 1\underline{u}\,;$
(s) $\underline{u} = a\underline{v} \quad \Rightarrow \quad \underline{v} = a^{-1}\underline{u}\,;$ og
(t) $\underline{u} = a\underline{v} \ \wedge \ \underline{v} = b\underline{w} \quad \Rightarrow \quad \underline{u} = (ab)\underline{w}\,.$

Ækvivalensklassen repræsenteret af $\underline{u} = (u_1, u_2, u_3) \in \mathbb{C}^3_{\varnothing}$ betegnes kort med $\underline{\underline{u}}$ og mere udførligt som $(u_1 : u_2 : u_3)$; altså $\underline{\underline{u}} = (u_1 : u_2 : u_3)$, og for alle $\underline{u}, \underline{v} \in \mathbb{C}^3_{\varnothing}$ gælder:

(3) $$\underline{\underline{u}} = \underline{\underline{v}} \quad \Leftrightarrow \quad \underline{u} \text{ og } \underline{v} \text{ er proportionale.}$$

(4) **Linier i rummet.** Enhver vektor $\underline{u} \in \mathbb{C}^3_{\varnothing}$ udspænder i $\mathbb{C}^3$ en linie gennem $\underline{0}$, nemlig linien $\{\, a\underline{u} \mid a \in \mathbb{C}\,\}$. Vektorerne $\underline{u}$ og $\underline{v}$ i $\mathbb{C}^3_{\varnothing}$ udspænder samme linie, netop når $\underline{u}$ og $\underline{v}$ er proportionale, altså netop når $\underline{\underline{u}} = \underline{\underline{v}}$, dvs. netop når $(u_1 : u_2 : u_3) = (v_1 : v_2 : v_3)$.

(5) **Den projektive plan.** Mængden af linier i rummet $\mathbb{C}^3$ gennem $\underline{0}$ betegnes $\mathbb{P}^2_{\mathbb{C}}$ og kaldes den *projektive plan* (over $\mathbb{C}$), og er det samme som mængden af ækvivalensklasser under proportionalitet. Elementerne i $\mathbb{P}^2_{\mathbb{C}}$ kaldes *punkter*, betegnes derfor kort som $\underline{\underline{u}}$ med $\underline{u} = (u_1, u_2, u_3) \in \mathbb{C}^3_{\varnothing}$ og mere udførligt som et *projektivt koordinatsæt* $(u_1 : u_2 : u_3)$. En omformulering af (3) giver, at der for alle $\underline{u}, \underline{v} \in \mathbb{C}^3_{\varnothing}$ gælder:

(6) $$\underline{\underline{u}} \neq \underline{\underline{v}} \quad \Leftrightarrow \quad \text{sættet } (\underline{u}, \underline{v}) \text{ af vektorer i } \mathbb{C}^3 \text{ er lineært uafhængigt}$$

(7) **Linier i den projektive plan.** For $\underline{a} = (a_1, a_2, a_3) \in \mathbb{C}^3_{\varnothing}$ har det mening at definere:

$$\mathcal{L}_{\underline{a}} = \{\, \underline{\underline{x}} \in \mathbb{P}^2_{\mathbb{C}} \mid a_1x_1 + a_2x_2 + a_3x_3 = 0 \,\}\,.$$

Hvis nemlig $\underline{\underline{x}} = \underline{\underline{y}}$, altså $(x_1, x_2, x_3) = c(y_1, y_2, y_3)$ for et $c \in \mathbb{C}$, da gælder $a_1x_1 + a_2x_2 + a_3x_3 = 0$, netop hvis $a_1y_1 + a_2y_2 + a_3y_3 = 0$.

For $\underline{\underline{a}} = (a_1 : a_2 : a_3) \in \mathbb{P}^2_{\mathbb{C}}$ har det nu mening at definere:

$$\mathcal{L}_{\underline{\underline{a}}} = \{\, \underline{\underline{x}} \in \mathbb{P}^2_{\mathbb{C}} \mid a_1x_1 + a_2x_2 + a_3x_3 = 0 \,\}\,.$$

Hvis nemlig $\underline{\underline{a}} = \underline{\underline{b}}$, da er $\mathcal{L}_{\underline{a}}$ og $\mathcal{L}_{\underline{b}}$ ens, idet der findes $d \in \mathbb{C}$, så $(a_1, a_2, a_3) = d(b_1, b_2, b_3)$, og for $\underline{x} \in \mathbb{C}^3$ haves dermed: $a_1x_1 + a_2x_2 + a_3x_3 = 0$, netop hvis $b_1x_1 + b_2x_2 + b_3x_3 = 0$.

Man siger, at $\mathcal{L}_{\underline{\underline{a}}}$ er *linien givet ved ligningen* $a_1x_1 + a_2x_2 + a_3x_3 = 0$, eller blot *linien givet ved punktet* $\underline{\underline{a}}$.

(1) **Sætning.** *For ethvert* $\underline{\underline{a}} \in \mathbb{P}^2_{\mathbb{C}}$ *består linien* $\mathcal{L}_{\underline{\underline{a}}}$ *af uendelig mange punkter.*

(2) *Bevis.* Da $\underline{a} \neq \underline{0}$ har 1×3–matricen $(\,a_1 \quad a_2 \quad a_3\,)$ rang 1. Løsningsrummet til det homogene lineære ligningssystem $a_1x_1 + a_2x_2 + a_3x_3 = 0$ (med én ligning og tre variable) har derfor dimension $3 - 1 = 2$. Vælg to løsninger $\underline{u} = (u_1, u_2, u_3)$ og $\underline{v} = (v_1, v_2, v_3)$, så sættet $(\underline{u}, \underline{v})$ er lineært uafhængigt. Sæt $\underline{w}_t = \underline{u} + t\underline{v} = (u_1, u_2, u_3) + t(v_1, v_2, v_3)$ for $t \in \mathbb{C}$, og bemærk, at $\underline{w}_t$ er en løsning til ligningsystemet, dvs. det tilsvarende projektive punkt $\underline{\underline{w}}_t$ tilhører $\mathcal{L}_{\underline{\underline{a}}}$. For $t \neq t'$ er $\underline{w}_t$ og $\underline{w}_{t'}$ ikke proportionale, og dermed gælder $\underline{\underline{w}}_t \neq \underline{\underline{w}}_{t'}$. Mængden $\{\,\underline{\underline{w}}_t \mid t \in \mathbb{C}\,\}$ er derfor uendelig, og da den er indeholdt i $\mathcal{L}_{\underline{\underline{a}}}$, er det ønskede bevist. $\square$

(3) **Sætning.** *Hvis punkterne* $\underline{\underline{a}}$ *og* $\underline{\underline{b}}$ *i* $\mathbb{P}^2_{\mathbb{C}}$ *er forskellige, da har linierne* $\mathcal{L}_{\underline{\underline{a}}}$ *og* $\mathcal{L}_{\underline{\underline{b}}}$ *netop ét punkt fælles.*

(4) *Bevis.* Idet $\underline{\underline{a}} \neq \underline{\underline{b}}$, giver 1(6), at sættet $(\underline{a}, \underline{b})$ er lineært uafhængigt i $\mathbb{C}^3$, og dette medfører at 2×3–matricen

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix}$$

har rang 2. Løsningsrummet til det homogene lineære ligningssystem:

$$(*) \qquad \begin{aligned} a_1x_1 + a_2x_2 + a_3x_3 &= 0 \\ b_1x_1 + b_2x_2 + b_3x_3 &= 0 \end{aligned}$$

har derfor dimension $3 - 2 = 1$. Lad $\underline{x} = (x_1, x_2, x_3) \in \mathbb{C}^3_{\emptyset}$ være en løsning til $(*)$, og dermed tilhører $\underline{\underline{x}} = (x_1\!:\!x_2\!:\!x_3)$ fællesmængden $\mathcal{L}_{\underline{\underline{a}}} \cap \mathcal{L}_{\underline{\underline{b}}}$, som således består af mindst ét punkt.

Lad nu $\underline{\underline{x}}' = (x'_1\!:\!x'_2\!:\!x'_3)$ også tilhøre $\mathcal{L}_{\underline{\underline{a}}} \cap \mathcal{L}_{\underline{\underline{b}}}$, dvs. $\underline{x}' = (x'_1, x'_2, x'_3) \in \mathbb{C}^3_{\emptyset}$ er ligeledes en løsning til $(*)$ og er dermed proportional med løsningen $\underline{x}$; altså $\underline{\underline{x}}' = \underline{\underline{x}}$. Hermed er det ønskede bevist: $\mathcal{L}_{\underline{\underline{a}}} \cap \mathcal{L}_{\underline{\underline{b}}} = \{\underline{\underline{x}}\}$. $\square$

(5) **Korollar.** *Hvis linierne* $\mathcal{L}_{\underline{\underline{a}}}$ *og* $\mathcal{L}_{\underline{\underline{b}}}$ *i* $\mathbb{P}^2_{\mathbb{C}}$ *er ens, da er punkterne* $\underline{\underline{a}}$ *og* $\underline{\underline{b}}$ *i* $\mathbb{P}^2_{\mathbb{C}}$ *ens.*

(6) *Bevis.* Dette fås ved at sammenholde (1) med (3). $\square$

(7) **Den affine plan.** Delmængden af $\mathbb{P}^2_{\mathbb{C}}$ bestående af punkter med projektive koordinatsæt $\underline{\underline{u}} = (u_1 : u_2 : u_3)$ med $u_3 \neq 0$ betegnes $\mathbb{A}^2_{\mathbb{C}}$ og kaldes den *affine plan* (over $\mathbb{C}$). Bemærk, at hvis $u_3 \neq 0$ er opfyldt for ét projektivt koordinatsæt $(u_1\!:\!u_2\!:\!u_3)$ for et punkt i $\mathbb{P}^2_{\mathbb{C}}$, da er det opfyldt for ethvert projektivt koordinatsæt for dette punkt

Ethvert punkt i $\mathbb{A}^2_{\mathbb{C}}$ kan repræsenteres ved et projektivt koordinatsæt af formen $(y_1 : y_2 \!:\! 1)$. Planen $\mathbb{C}^2$ identificeres med $\mathbb{A}^2_{\mathbb{C}}$ ved at sætte $(y_1, y_2) = (y_1\!:\!y_2\!:\!1)$.

(8) **Linien i uendelig.** Bemærk, at linien $\mathcal{L}_{(0:0:1)}$ givet ved punktet $(0 : 0 : 1)$ netop består af punkterne med projektivt koordinatsæt $(x_1 : x_2 : 0)$ med $(x_1, x_2) \in \mathbb{C}^2_{\emptyset}$. Linien $\mathcal{L}_{(0:0:1)}$ er dermed netop komplementærmængden $\mathbb{P}^2_{\mathbb{C}} \setminus \mathbb{A}^2_{\mathbb{C}}$ til den affine plan, og den kaldes *linien i uendelig* og betegnes kort $\mathcal{L}_\infty$. Punktet $\underline{\underline{x}} = (x_1 : x_2 : 0)$ på $\mathcal{L}_\infty$ kaldes *punktet i uendelig i retningen* (x_1, x_2). For $\underline{\underline{a}} = (a_1\!:\!a_2\!:\!a_3) \in \mathbb{P}^2_{\mathbb{C}}$ gælder:

$$(9) \qquad \mathcal{L}_{\underline{\underline{a}}} = \mathcal{L}_\infty \quad \Leftrightarrow \quad a_1 = 0 \;\wedge\; a_2 = 0\,.$$

(10) **Opgave.** Hvad er $\mathcal{L}_{\underline{\underline{a}}} \cap \mathcal{L}_\infty$?

(1) **Linier i den affine plan.** Hvis $\underline{\underline{a}} \in \mathbb{P}^2_{\mathbb{C}}$ har $(a_1, a_2) \neq (0,0)$, da er $\mathcal{L}_{\underline{\underline{a}}} \cap \mathbb{A}^2_{\mathbb{C}}$ netop linien i $\mathbb{C}^2$ givet ved ligningen: $a_1x_1 + a_2x_2 + a_3 = 0$, og enhver linie i $\mathbb{C}^2$ er af denne form.

(2) **Opgave.** Lad der være givet to *forskellige* linier i $\mathbb{C}^2$ ved ligningerne:

$$\begin{aligned} L: &\quad a_1x_1 + a_2x_2 + a_3 = 0 \\ M: &\quad b_1x_1 + b_2x_2 + b_3 = 0\,. \end{aligned}$$

Altså $L = \mathcal{L}_{\underline{\underline{a}}} \cap \mathbb{A}^2_{\mathbb{C}}$ og $M = \mathcal{L}_{\underline{\underline{b}}} \cap \mathbb{A}^2_{\mathbb{C}}$. Antag, at $\mathcal{L}_{\underline{\underline{a}}} \cap \mathcal{L}_{\underline{\underline{b}}} = \{\underline{\underline{x}}\}$. Bevis, at der gælder:

$$\underline{\underline{x}} \in \mathcal{L}_\infty \quad \Leftrightarrow \quad L \text{ og } M \text{ er parallelle}\,.$$

(3) **Dualitetsprincippet.** For alle $\underline{\underline{a}}, \underline{\underline{x}} \in \mathbb{P}^2_{\mathbb{C}}$ gælder:

$$\boxed{\underline{\underline{x}} \in \mathcal{L}_{\underline{\underline{a}}} \quad \Leftrightarrow \quad \underline{\underline{a}} \in \mathcal{L}_{\underline{\underline{x}}}}\,.$$

Begge sider af biimplikationspilen er nemlig ensbetydende med $a_1x_1 + a_2x_2 + a_3x_3 = 0$.

Nu følger første – men måske lidt banale – anvendelse af dette dualitetsprincip; nemlig et dualt resultat til 2(3).

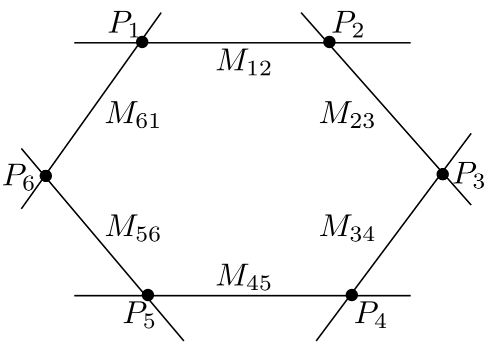
(4) **Sætning.** *Hvis $\underline{\underline{a}}, \underline{\underline{b}} \in \mathbb{P}^2_{\mathbb{C}}$ er forskellige, da findes netop en linie gennem $\underline{\underline{a}}$ og $\underline{\underline{b}}$.*

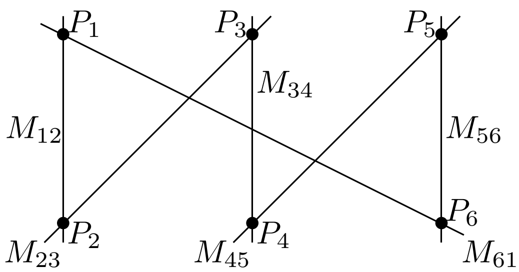
(5) *Bevis.* For $\underline{\underline{x}} \in \mathbb{P}^2_{\mathbb{C}}$ giver dualitetsprincippet, at

$$\underline{\underline{a}}, \underline{\underline{b}} \in \mathcal{L}_{\underline{\underline{x}}} \quad \Leftrightarrow \quad \underline{\underline{x}} \in \mathcal{L}_{\underline{\underline{a}}} \cap \mathcal{L}_{\underline{\underline{b}}}\,.$$

Det ønskede følger nu af 2(3). $\square$

(6) **Sekskanter.** I enhver – gerne "krøllet" – sekskant $(P_1, P_2, P_3, P_4, P_5, P_6)$ er der 3 par af modstående sider:

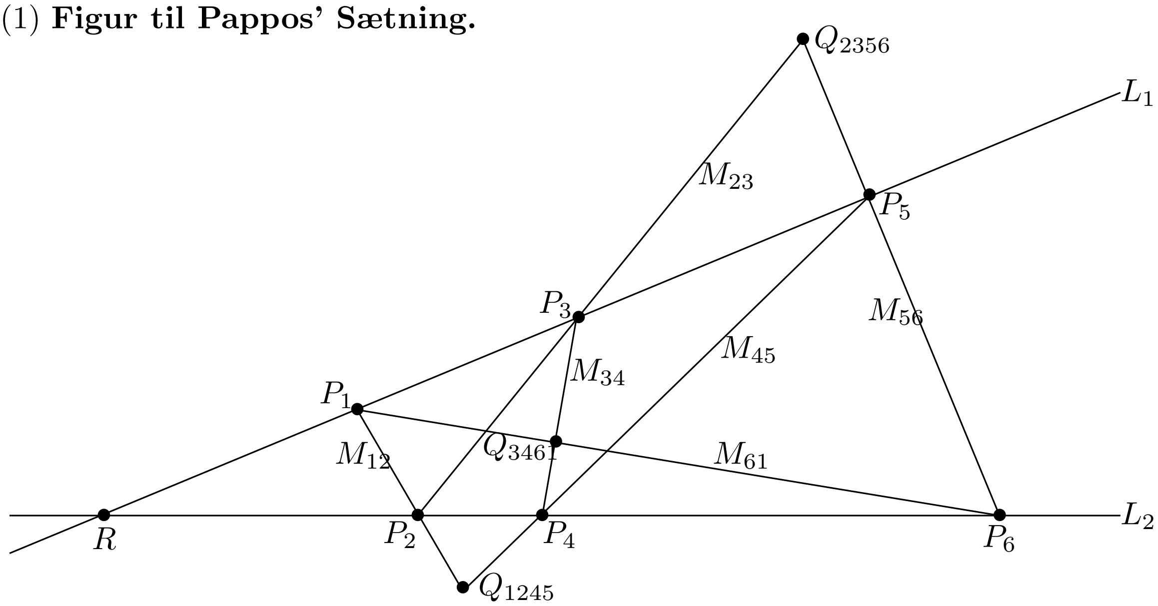




nemlig parrene (M_{12}, M_{45}), (M_{23}, M_{56}) og (M_{34}, M_{61}), hvor $M_{i,i+1}$ er (hele) linien gennem P_i og P_{i+1} (ikke kun liniestykket). (Her regnes indekser modulo 6.) For enhver sekskant i $\mathbb{P}^2_{\mathbb{C}}$ kan man altså tale om de modstående siders skæringspunkter, og der er tre sådanne i $\mathbb{P}^2_{\mathbb{C}}$, sml. 2(3), idet de modstående sider forudsættes at være forskellige.

(7) **Pappos' Sætning.** *Lad L_1 og L_2 være 2 forskellige linier i $\mathbb{P}^2_{\mathbb{C}}$ med fællespunkt R. Lad der være givet en sekskant $(P_1, \cdots, P_6)$, så $P_1, P_3, P_5 \in L_1 \setminus \{R\}$ og $P_2, P_4, P_6 \in L_2 \setminus \{R\}$. Da ligger de modstående siders skæringspunkter på linie.* Sml. figur 4(1).

(1) **Figur til Pappos' Sætning.**

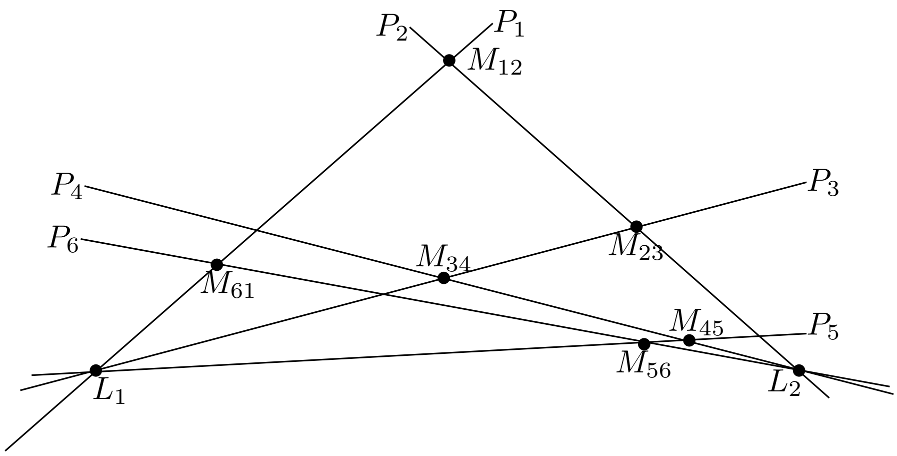


(2) **Kommentarer.** På figur (1) er skæringspunktet mellem $M_{i,i+1}$ og $M_{i+3,i+4}$ betegnet $Q_{i,i+1,i+3,i+4}$ (og indekser regnes stadig modulo 6). Påstanden i Pappos' Sætning er altså, at Q_{1245}, Q_{2356} og Q_{3461} ligger på linie.

Pappos' Sætning bevises senere. Først dualiseres den; dette er en mere subtil anvendelse af dualitetsprincippet.

(3) **Sætning.** *Lad L_1 og L_2 være 2 forskellige punkter i $\mathbb{P}^2_{\mathbb{C}}$, og lad R betegne linien gennem dem. Lad P_1, P_3 og P_5, henholdsvis P_2, P_4 og P_6, være indbyrdes forskellige linier gennem henholdsvis L_1 og L_2, således at alle 6 linier er forskellige fra R. Lad M_{ij} betegne skæringspunktet mellem P_i og P_j, og lad Q_{ijkl} betegne linien gennem M_{ij} og M_{kl}. Da findes et punkt S i $\mathbb{P}^2_{\mathbb{C}}$, som Q_{1245}, Q_{2356} og Q_{3461} går gennem.*

(4) **Figur.**



(1) *Bevis.* Lad L_1' og L_2' være linierne givet ved (projektive koordinatsæt for) punkterne L_1 og L_2, lad R' være punktet, der giver linien R, og lad P_i' være punktet, der giver linien P_i. Iflg. dualitetsprincippet og forudsætningerne gælder, at $P_1', P_3', P_5' \in L_1' \setminus \{R'\}$ og $P_2', P_4', P_6' \in L_2' \setminus \{R'\}$, og disse punkter er indbyrdes forskellige, så de udgør en sekskant. Siderne i denne, $M_{i,i+1}'$, er linierne givet ved skæringspunkterne $M_{i,i+1}$, så de modstående siders skæringspunkter, Q_{1245}', Q_{2356}' og Q_{3461}', er netop punkterne, der giver linierne Q_{1245}, Q_{2356} og Q_{3461}. Da Q_{1245}', Q_{2356}' og Q_{3461}' ligger på en linie S' (ifl. Pappos' Sætning), går Q_{1245}, Q_{2356} og Q_{3461} gennem punktet S (der giver linien S') $\square$

(2) **Desargues' Trekantssætning.** *Lad L_1, L_2 og L_3 være 3 indbyrdes forskellige linier, der går gennem punktet R. Antag $P_1, P_1' \in L_1 \setminus \{R\}$, $P_2, P_2' \in L_2 \setminus \{R\}$ og $P_3, P_3' \in L_3 \setminus \{R\}$. Lad $Q_{i,i+1}$ betegne skæringspunktet mellem siden P_iP_{i+1} (i trekanten (P_1, P_2, P_3)) og siden $P_i'P_{i+1}'$ (i trekanten (P_1', P_2', P_3')). Da ligger Q_{12}, Q_{23} og Q_{31} på linie*

(3) **Opgave.** Tegn (2).

(4) **Opgave.** Bevis (2), når beviset for 3(7) er gennemført i næste afsnit.

(5) **Opgave.** Dualisér (2), tegn og bevis.

(6) **Sætning om punkter på linie.** *For $\underline{\underline{a}}, \underline{\underline{b}}, \underline{\underline{c}} \in \mathbb{P}^2_{\mathbb{C}}$ betragtes sættet $(\underline{a}, \underline{b}, \underline{c})$ af vektorer i $\mathbb{C}^3$. Der gælder:*

$$\underline{\underline{a}}, \underline{\underline{b}}, \underline{\underline{c}} \ \textit{ ligger på linie } \quad \Leftrightarrow \quad (\underline{a}, \underline{b}, \underline{c}) \ \textit{ er lineært afhængigt.}$$

(7) *Bevis.* Betragt 3×3–matricen D:

$$D = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix} \in \mathbb{C}^3_3 \,.$$

(Her – og i det følgende – betegner $\mathbb{C}^m_n$ mængden af $m\times n$–matricer.) Det ønskede følger af biimplikationskæden:

$$\begin{aligned} \underline{\underline{a}}, \underline{\underline{b}}, \underline{\underline{c}} \text{ ligger på linie } &\Leftrightarrow \ \exists\, \underline{\underline{x}} \in \mathbb{P}^2_{\mathbb{C}} : \underline{\underline{a}}, \underline{\underline{b}}, \underline{\underline{c}} \in \mathcal{L}_{\underline{\underline{x}}} \quad \Leftrightarrow \quad \exists\, X_| \in \mathbb{C}^3_1 \setminus \{O_|\} : DX_| = O_| \\ &\Leftrightarrow \ \text{rg}\, D < 3 \quad \Leftrightarrow \quad \text{rækkerne i } D \text{ er lineært afhængige} \\ &\Leftrightarrow \ (\underline{a}, \underline{b}, \underline{c}) \text{ er lineært afhængigt.} \end{aligned}$$

$$\text{Her er } \ X_| = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{C}^3_1 \ \text{ søjlen svarende til } \ \underline{x} \in \mathbb{C}^3 \ \text{ og } \ \underline{\underline{x}} \in \mathbb{P}^2_{\mathbb{C}} \,. \ \square$$

(8) **Definition.** Punkterne $\underline{\underline{u}}, \underline{\underline{v}}, \underline{\underline{w}}, \underline{\underline{x}} \in \mathbb{P}^2_{\mathbb{C}}$ er *i generel position*, netop hvis ikke tre af dem ligger på linie.

(9) **Opgave.** Bevis at følgende er ensbetydende for $\underline{\underline{u}}, \underline{\underline{v}}, \underline{\underline{w}}, \underline{\underline{x}} \in \mathbb{P}^2_{\mathbb{C}}$.

- (i) $\underline{\underline{u}}, \underline{\underline{v}}, \underline{\underline{w}}$ og $\underline{\underline{x}}$ er i generel position.
- (ii) For enhver ikke-triviel lineær relation $a\underline{u} + b\underline{v} + c\underline{w} + d\underline{x} = \underline{0}$ gælder, at alle koefficienterne a, b, c, d er ulig nul.

(10) **Opgave.** Hvad betyder det, at linierne L, M, N, P er i generel position?

2. Projektivt koordinatskift

(1) **Lineære afbildninger og matricer.** Lad $\underline{\varphi}\colon \mathbb{C}^3 \to \mathbb{C}^3$ være en lineær afbildning, og lad $Q \in \mathbb{C}^3_3$ være den *naturlige matrix* for $\underline{\varphi}$, dvs. matricen for $\underline{\varphi}$ mht. den (sædvanlige) naturlige basis; der gælder altså for alle $\underline{x}, \underline{y} \in \mathbb{C}^3$, at

$$\underline{y} = \underline{\varphi}(\underline{x}) \quad \Leftrightarrow \quad Y_| = QX_|$$

med notation fra 1.5(7).

(2) **Induceret afbildning.** Lad $\underline{\varphi}\colon \mathbb{C}^3 \to \mathbb{C}^3$ være en isomorfi. Bemærk, at $\underline{\varphi}(\underline{x}) \neq \underline{0}$, hvis $\underline{x} \neq \underline{0}$ og $\underline{x} \in \mathbb{C}^3$, dvs. $\underline{\varphi}$ afbilder $\mathbb{C}^3_\emptyset$ ind i $\mathbb{C}^3_\emptyset$. Hvis nu $\underline{\underline{x}} = \underline{\underline{x}}'$ i $\mathbb{P}^2_\mathbb{C}$, dvs. $\underline{x} = c\underline{x}'$ for et $c \in \mathbb{C}$, da er $\underline{\varphi}(\underline{x}) = c\underline{\varphi}(\underline{x}')$, og dermed giver $\underline{\varphi}(\underline{x})$ og $\underline{\varphi}(\underline{x}')$ samme punkt i $\mathbb{P}^2_\mathbb{C}$, nemlig $\underline{\underline{\varphi}(\underline{x})} = \underline{\underline{\varphi}(\underline{x}')}$. Isomorfien $\underline{\varphi}$ inducerer derfor en veldefineret afbildning $\underline{\underline{\varphi}} : \mathbb{P}^2_\mathbb{C} \to \mathbb{P}^2_\mathbb{C}$ ved at sætte $\underline{\underline{\varphi}}(\underline{\underline{x}}) = \underline{\underline{y}}$, når $\underline{y} = \underline{\varphi}(\underline{x})$; altså $\underline{\underline{\varphi}}(\underline{\underline{x}}) = \underline{\underline{\varphi}(\underline{x})}$.

(3) **Eksempel.** Lad $\underline{\varphi}$ have naturlig matrix

$$Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} \end{pmatrix} .$$

Da er $\underline{\underline{\varphi}}(\underline{\underline{x}}) = (x_1 : -\frac{1}{2}x_2 + \frac{1}{2}x_3 : \frac{1}{2}x_2 + \frac{1}{2}x_3) = (2x_1 : -x_2 + x_3 : x_2 + x_3)$. Specielt er $\underline{\underline{\varphi}}(0 : 0 : 1) = (0 : 1 : 1)$ og $\underline{\underline{\varphi}}(0 : 1 : 0) = (0 : -1 : 1)$, dvs. punktet $(0, 0)$ i $\mathbb{A}^2_\mathbb{C}$ bliver afbildet i $(0, 1) \in \mathbb{A}^2_\mathbb{C}$, mens punktet i uendelig i retningen $(0, 1)$ bliver afbildet i $(0, -1) \in \mathbb{A}^2_\mathbb{C}$.

(4) **Sætning.** *Hvis $\underline{\varphi}, \underline{\psi}\colon \mathbb{C}^3 \to \mathbb{C}^3$ er isomorfier, da inducerer den sammensatte isomorfi $\underline{\psi} \circ \underline{\varphi}$ netop den sammensatte afbildning $\underline{\underline{\psi}} \circ \underline{\underline{\varphi}}$; altså $\underline{\underline{\underline{\psi} \circ \underline{\varphi}}} = \underline{\underline{\psi}} \circ \underline{\underline{\varphi}}$.*

Identitets-isomorfien $\mathrm{id}_{\mathbb{C}^3} : \mathbb{C}^3 \to \mathbb{C}^3$ inducerer den identiske afbildning $\mathrm{id}_{\mathbb{P}^2_\mathbb{C}} : \mathbb{P}^2_\mathbb{C} \to \mathbb{P}^2_\mathbb{C}$; altså $\underline{\mathrm{id}_{\mathbb{C}^3}} = \mathrm{id}_{\mathbb{P}^2_\mathbb{C}}$.

(5) *Bevis.* For $\underline{x} \in \mathbb{C}^3_\emptyset$, $\underline{y} = \underline{\varphi}(\underline{x})$ og $\underline{z} = \underline{\psi}(\underline{y})$ har vi $\underline{\underline{z}} = \underline{\underline{\psi}}(\underline{\underline{y}}) = \underline{\underline{\psi}}(\underline{\underline{\varphi}}(\underline{\underline{x}})) = (\underline{\underline{\psi}} \circ \underline{\underline{\varphi}})(\underline{\underline{x}})$. Endvidere giver $\underline{z} = (\underline{\psi} \circ \underline{\varphi})(\underline{x})$, at $\underline{\underline{z}} = \underline{\underline{\underline{\psi} \circ \underline{\varphi}}}(\underline{\underline{x}})$, og første påstand er bevist.

Anden påstand er (også) oplagt: $\underline{\mathrm{id}_{\mathbb{C}^3}}(\underline{\underline{x}}) = \underline{\mathrm{id}_{\mathbb{C}^3}(\underline{x})} = \underline{\underline{x}}$. □

(6) **Korollar.** *Lad $\underline{\varphi}\colon \mathbb{C}^3 \to \mathbb{C}^3$ være en isomorfi. Den inducerede afbildning $\underline{\underline{\varphi}}\colon \mathbb{P}^2_\mathbb{C} \to \mathbb{P}^2_\mathbb{C}$ er da bijektiv med invers induceret af $\underline{\varphi^{-1}}$, dvs. $(\underline{\underline{\varphi}})^{-1} = \underline{\underline{\varphi^{-1}}}$.*

(7) *Bevis.* (4) giver

$$\underline{\underline{\varphi^{-1}}} \circ \underline{\underline{\varphi}} = \underline{\underline{\underline{\varphi^{-1}} \circ \underline{\varphi}}} = \underline{\mathrm{id}_{\mathbb{C}^3}} = \mathrm{id}_{\mathbb{P}^2_\mathbb{C}} \quad \text{og} \quad \underline{\underline{\varphi}} \circ \underline{\underline{\varphi^{-1}}} = \underline{\underline{\underline{\varphi} \circ \underline{\varphi^{-1}}}} = \underline{\mathrm{id}_{\mathbb{C}^3}} = \mathrm{id}_{\mathbb{P}^2_\mathbb{C}} \ . \quad \square$$

(1) **Sætning.** *Lad* $\underline{\varphi}\colon \mathbb{C}^3 \longrightarrow \mathbb{C}^3$ *være en isomorfi. Hvis* $\underline{\underline{a}}$ *er et punkt i* $\mathbb{P}^2_{\mathbb{C}}$*, da er billedet* $\underline{\underline{\varphi}}(\mathcal{L}_{\underline{\underline{a}}})$ *af linien* $\mathcal{L}_{\underline{\underline{a}}}$ *igen en linie, nemlig linien* $\mathcal{L}_{\underline{\underline{b}}}$*, hvor* $\underline{\underline{b}} \in \mathbb{P}^2_{\mathbb{C}}$ *er givet ved* $B_- = A_- Q^{-1}$*, idet* A_- *og* B_- *er rækkerne (dvs.* 1×3*–matricerne) svarende til henholdsvis* $\underline{\underline{a}}$ *og* $\underline{\underline{b}}$*, og* $Q \in \mathbb{C}^3_3$ *er den naturlige matrix for* $\underline{\varphi}$*.*

(2) *Bevis.* Kæden

$$\underline{\underline{x}} \in \mathcal{L}_{\underline{\underline{a}}} \quad \Leftrightarrow \quad A_- X_| = 0 \quad \Leftrightarrow \quad B_-(QX_|) = 0 \quad \Leftrightarrow \quad \underline{\underline{\varphi}}(\underline{\underline{x}}) \in \mathcal{L}_{\underline{\underline{b}}}$$

giver $\underline{\underline{\varphi}}(\mathcal{L}_{\underline{\underline{a}}}) = \mathcal{L}_{\underline{\underline{b}}}$. $\square$

(3) **Projektivt koordinatskift.** En afbildning $\alpha : \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ kaldes et *projektivt koordinatskift*, netop hvis den er induceret af en isomorfi $\underline{\varphi} : \mathbb{C}^3 \longrightarrow \mathbb{C}^3$ (dvs. $\alpha = \underline{\underline{\varphi}}$).

(4) **Sætning.** *Antag, at punkterne* $\underline{\underline{x}}, \underline{\underline{y}}, \underline{\underline{z}} \in \mathbb{P}^2_{\mathbb{C}}$ *ikke ligger på linie, og at punkterne* $\underline{\underline{x}}', \underline{\underline{y}}', \underline{\underline{z}}' \in \mathbb{P}^2_{\mathbb{C}}$ *heller ikke ligger på linie. Der findes da et projektivt koordinatskift* α*, så*

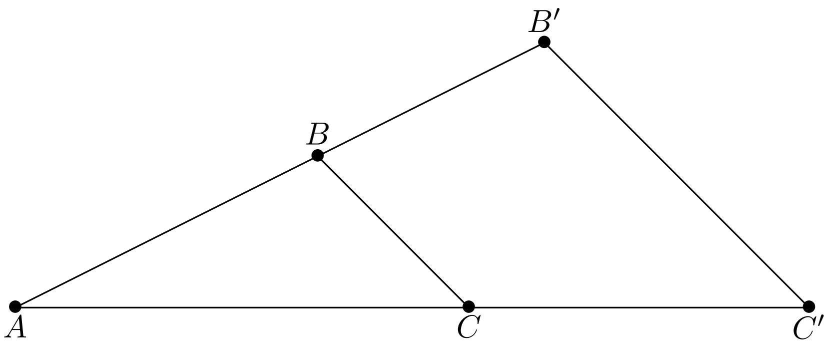
$$\alpha(\underline{\underline{x}}) = \underline{\underline{x}}', \quad \alpha(\underline{\underline{y}}) = \underline{\underline{y}}' \quad \textit{og} \quad \alpha(\underline{\underline{z}}) = \underline{\underline{z}}' .$$

(5) *Bevis.* Vektorsættet $(\underline{x}, \underline{y}, \underline{z})$ er iflg. 1.5(6) lineært uafhængigt, og der findes derfor en lineær afbildning $\underline{\varphi} : \mathbb{C}^3 \longrightarrow \mathbb{C}^3$, så $\underline{\varphi}(\underline{x}) = \underline{x}'$, $\underline{\varphi}(\underline{y}) = y'$ og $\underline{\varphi}(\underline{z}) = \underline{z}'$. Sættet $(\underline{x}', \underline{y}', \underline{z}')$ udspænder $\mathbb{C}^3$ (da det er lineært uafhængigt og består af tre vektorer), og derfor er $\underline{\varphi}$ surjektiv og dermed også injektiv, dvs. en isomorfi. Sæt $\alpha = \underline{\underline{\varphi}}$. $\square$

(6) **Opgave.** Antag, at punkterne $\underline{\underline{u}}, \underline{\underline{v}}, \underline{\underline{w}}, \underline{\underline{x}} \in \mathbb{P}^2_{\mathbb{C}}$ og $\underline{\underline{u}}', \underline{\underline{v}}', \underline{\underline{w}}', \underline{\underline{x}}' \in \mathbb{P}^2_{\mathbb{C}}$ er i generel position, sml. 1.5(8).

Bevis, at der findes *netop et* projektivt koordinatskift α, der fører de førstnævnte fire punkter over i de sidstnævnte.

(7) **Ensvinklede trekanter.** Betragt de to trekanter ABC og $AB'C'$:

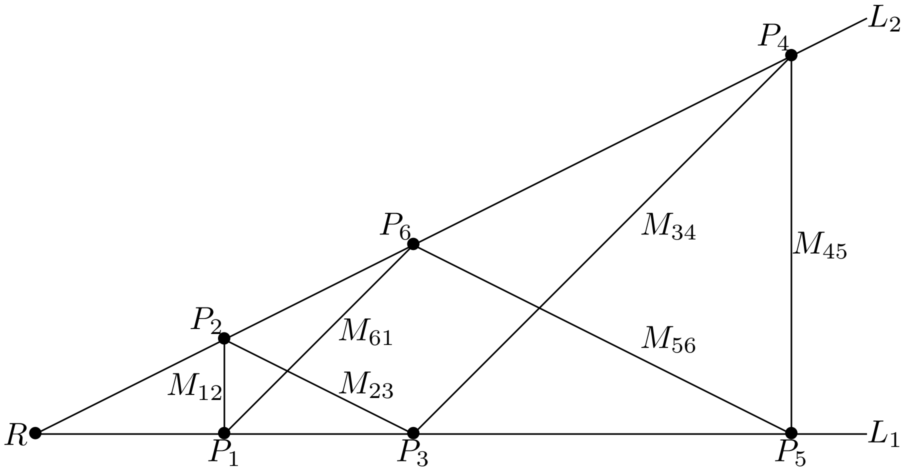


og liniestykkelængderne $b = |AB|$, $b' = |AB'|$, $c = |AC|$ og $c' = |AC'|$.

Der gælder $b/c = b'/c'$, netop hvis linierne BC og $B'C'$ er parallelle (dvs. trekanterne ABC og $AB'C'$ er ensvinklede).

(1) *Bevis* for Pappos' Sætning 1.3(7).

Tilfælde 1°: Hvis punkterne Q_{1245}, Q_{2356} og R ikke ligger på linie, da kan man efter et projektivt koordinatskift antage, at Q_{1245} og Q_{2356} tilhører $\mathcal{L}_\infty$, og at R tilhører $\mathbb{A}^2_{\mathbb{C}}$:



altså at M_{12} og M_{45} er parallelle, at M_{23} og M_{56} er parallelle (sml. evt. 1.3(2)), og at L_1 og L_2 skærer hinanden i det affine punkt R [og vi ønsker at bevise, at også Q_{3461} ligger på $\mathcal{L}_\infty$, dvs. at M_{34} og M_{61} er parallelle]. Sæt $p_i = |RP_i|$. Da M_{12} og M_{45}, hhv. M_{23} og M_{56}, er parallelle, har vi fra 2(7), at

$$\frac{p_1}{p_2} = \frac{p_5}{p_4} \quad \text{hhv.} \quad \frac{p_2}{p_3} = \frac{p_6}{p_5} \ .$$

Heraf fås: $p_1p_4 = p_2p_5 = p_3p_6$, dvs. $p_3/p_4 = p_1/p_6$; altså at M_{34} og M_{61} er parallelle – som ønsket.

Tilfælde 2°: Hvis punkterne Q_{1245}, Q_{2356} og R ligger på linie, da kan man efter et projektivt koordinatskift antage, at Q_{1245} og Q_{2356} tilhører $\mathcal{L}_\infty$, og dermed tilhører R også $\mathcal{L}_\infty$. Det overlades til læseren at tegne figuren i dette tilfælde samt at bevise det ønskede. $\square$

(2) **Opgave.** Bestem linierne $\underline{\underline{\varphi}}(\mathcal{L}_{(1:0:0)})$, $\underline{\underline{\varphi}}(\mathcal{L}_{(0:1:0)})$ og $\underline{\underline{\varphi}}(\mathcal{L}_\infty)$ for $\underline{\underline{\varphi}}$ som i 1(3). Tegn de affine dele af de seks her nævnte linier samt de affine blandt punkterne i 1(3). Bemærk, at

$$Q^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \ .$$

(3) **Opgave.** I den projektive plan $\mathbb{P}^2_{\mathbb{C}}$ er der givet en trekant med hjørner $\underline{\underline{a}}_1 = (1:0:0)$, $\underline{\underline{a}}_2 = (0:1:0)$ og $\underline{\underline{a}}_3 = (0:0:1)$. Tegn den affine del af denne trekant.

Bestem $\underline{\underline{b}}_1$, $\underline{\underline{b}}_2$ og $\underline{\underline{b}}_3$ i $\mathbb{P}^2_{\mathbb{C}}$, så $\mathcal{L}_{\underline{\underline{b}}_i}$ en den modstående linie til hjørnet $\underline{\underline{a}}_i$ i trekanten, dvs. linien gennem $\underline{\underline{a}}_{i-1}$ og $\underline{\underline{a}}_{i+1}$ for alle i, idet der regnes modulo 3.

Bestem projektivt koordinatskift $\alpha\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$, som afbilder trekanten over i den affine trekant med hjørner $A_1 = (1,0)$, $A_2 = (0,1)$ og $A_3 = (0,0)$. Den naturlige matrix Q for en tilhørende isomorfi $\underline{\varphi}\colon \mathbb{C}^3 \to \mathbb{C}^3$ ønskes angivet. Tegn den affine trekant.

Bestem $\underline{\underline{c}}_1$, $\underline{\underline{c}}_2$ og $\underline{\underline{c}}_3$ i $\mathbb{P}^2_{\mathbb{C}}$, så $\mathcal{L}_{\underline{\underline{c}}_i} = \underline{\underline{\varphi}}(\mathcal{L}_{\underline{\underline{b}}_i})$ for alle i. Er det her nødvendigt at benytte 2(1)?

3. POLYNOMIER

(1) **Polynomier i to variable.** Med $\mathbb{C}[x_1, x_2]$ betegnes mængden af *komplekse polynomier i de to variable* x_1 og x_2. Til ethvert $f \in \mathbb{C}[x_1, x_2]$ findes altså endelig mange $a_{ij} \in \mathbb{C}$, så $f = \sum_{i,j} a_{ij} x_1^i x_2^j$. Dette er en formel sum, men ofte betragtes $f \in \mathbb{C}[x_1, x_2]$ konkret som en *polynomial* funktion $f\colon \mathbb{C}^2 \to \mathbb{C}$, dvs. til f findes endelig mange $a_{ij} \in \mathbb{C}$, så $f(x_1, x_2) = \sum_{i,j} a_{ij} x_1^i x_2^j$ for alle $(x_1, x_2) \in \mathbb{C}^2$, og $f(x_1, x_2)$ omtales som et polynomium.

Med polynomiers addition og multiplikation udgør $\mathbb{C}[x_1, x_2]$ en kommutativ ring. Betragt polynomiumsringen $\mathbb{C}[x_1]$ i variablen x_1, og dan polynomiumsringen over denne i variablen x_2. Herved fås ringen $\mathbb{C}[x_1][x_2]$, hvis elementer er endelige summer af formen $\sum_j (\sum_i a_{ij} x_1^i) x_2^j = \sum_{i,j} a_{ij} x_1^i x_2^j$, og ringene $\mathbb{C}[x_1][x_2]$ og $\mathbb{C}[x_1, x_2]$ identificeres. Heraf følger specielt, at $\mathbb{C}[x_1, x_2]$ er et integritetsområde.

Når summen $f(x_1, x_2) = \sum_{i,j} a_{ij} x_1^i x_2^j$ skrives ledvis, fås

$$\begin{aligned} f(x_1, x_2) = & a_{00} + (a_{10}x_1 + a_{01}x_2) + (a_{20}x_1^2 + a_{11}x_1x_2 + a_{02}x_2^2) \\ & + (a_{30}x_1^3 + a_{21}x_1^2x_2 + a_{12}x_1x_2^2 + a_{03}x_2^3) \\ & + \dots \\ & + (a_{n0}x_1^n + a_{(n-1)1}x_1^{n-1}x_2 + \dots + a_{1(n-1)}x_1x_2^{n-1} + a_{0n}x_2^n) \,. \end{aligned}$$

Nulte led er *konstantleddet*, første led det *lineære led*, andet led er det *kvadratiske led*, tredie led er *trediegradsleddet*, ... , n'te led er *n'te gradsleddet*.

Nulpolynomiet er konstanten nul o (defineret ved $o(x_1, x_2) = 0$ for alle $(x_1, x_2) \in \mathbb{C}^2$). De øvrige polynomier er de *ikke-trivielle* polynomier.

Graden $\deg f$ af $f \in \mathbb{C}[x_1, x_2]$ er

$$\deg f = \sup\{\, i + j \mid a_{ij} \neq 0 \,\} \,.$$

Graden af nulpolynomiet er $-\infty$, da $\sup \varnothing$ (per definition) er $-\infty$, mens graden af et ikke-trivielt polynomium er et ikke-negativt helt tal (dvs. tilhørende $\mathbb{N}_0$); altså $\deg f \in \mathbb{N}_0 \cup \{-\infty\}$. Polynomiet f er ikke-konstant, netop hvis $\deg f > 0$.

Ordenen $\operatorname{ord} f$ af $f \in \mathbb{C}[x_1, x_2]$ er

$$\operatorname{ord} f = \inf\{\, i + j \mid a_{ij} \neq 0 \,\} \in \mathbb{N}_0 \cup \{\infty\} \,.$$

Ordenen af nulpolynomiet er ∞ (da $\inf \varnothing = \infty$), mens ordenen af et ikke-trivielt polynomium er et ikke-negativt helt (endeligt) tal.

(2) **Eksempler.** For $a, b, c, d \in \mathbb{C}[x_1, x_2]$ givet ved:

$$\begin{aligned} a(x_1, x_2) &= x_2 - x_1^2 \,; & b(x_1, x_2) &= x_1^2 - x_2^2 \,; \\ c(x_1, x_2) &= x_1^2 - x_2^2 + x_1^3 \ \text{ og } & d(x_1, x_2) &= x_1^2 - x_2^2 + x_1^2x_2^2 \end{aligned}$$

gælder:

gælder:	$\deg a = 2$	$\deg b = 2$	$\deg c = 3$	$\deg d = 4$
	$\operatorname{ord} a = 1$	$\operatorname{ord} b = 2$	$\operatorname{ord} c = 2$	$\operatorname{ord} d = 2$.

(1) **Homogene polynomier.** For $f \in \mathbb{C}[x_1, x_2]$ og $n \in \mathbb{N}_0$ siges f at være *homogent af grad* n, netop hvis alle led har grad n; altså netop hvis der findes $c_0, c_1, \dots, c_n \in \mathbb{C}$, så $f(x_1, x_2) = \sum_{i=0}^{n} c_i x_1^i x_2^{n-i}$. Specielt er nulpolynomiet homogent af alle grader! Et polynomium $f \neq o$ er konstant, netop hvis det er homogent af grad 0, og generelt er det homogent, netop hvis $\operatorname{ord} f = \deg f$. I eksempel 1(2) er netop b homogent.

Hvis $f, g \in \mathbb{C}[x_1, x_2]$ er homogene af grad henholdsvis n og s, da er produktet fg et homogent polynomium af grad $n + s$.

Når $f \in \mathbb{C}[x_1, x_2]$ er ikke-trivielt og har $m = \operatorname{ord} f$ og $n = \deg f$, da kan f skrives som sum af homogene polynomier: $f = f_m + \dots + f_n$, hvor hvert f_i er homogent af grad i (evt. nulpolynomiet). Hvis omvendt $f = f_r + \dots + f_s$ er en sum af homogene af indbyrdes forskellige grader, da er $\operatorname{ord} f = \inf\{\, i \in \mathbb{N}_0 \mid f_i \neq 0 \,\}$ og $\deg f = \sup\{\, i \in \mathbb{N}_0 \mid f_i \neq 0 \,\}$.

(2) **Sætning.** *For alle* $f, g \in \mathbb{C}[x_1, x_2]$ *gælder* $\operatorname{ord}(fg) = \operatorname{ord} f + \operatorname{ord} g$ *og* $\deg(fg) = \deg f + \deg g$.

(3) *Bevis.* Antag, at f og g er ikke-trivielle (thi ellers er de to ligheder trivielt opfyldt), og sæt $m = \operatorname{ord} f$, $n = \deg f$, $r = \operatorname{ord} g$ og $s = \deg g$. Da kan f og g skrives som summer af homogene: $f = f_m + \dots + f_n$ og $g = g_r + \dots + g_s$, og multiplikation giver en sum $fg = f_m g_r + \dots + \left(\sum_{h+j=i} f_h g_j\right) + \dots + f_n g_s$ af homogene polynomier. Da $\mathbb{C}[x_1, x_2]$ er et integritetsområde, er polynomierne $f_m g_r$ og $f_n g_s$ ikke-trivielle og af graderne henholdsvis $m + r$ og $n + s$, så $\operatorname{ord}(fg) = \inf\{\, i \in \mathbb{N}_0 \mid (fg)_i \neq 0 \,\} = m + r$ tilsvarende $\deg(fg) = n + s$. $\square$

(4) **Homogenisering og dehomogenisering; 1 og 2 variable.** Ethvert polynomium $f \in \mathbb{C}[x_1]$ i *én* variabel af grad m kan *homogeniseres* til et *homogent* polynomium $f^* \in \mathbb{C}[x_1, x_2]$ i *to* variable af grad m: Hvis $f(x_1) = a_0 + a_1 x_1 + \dots + a_m x_1^m$, da er

$$f^*(x_1, x_2) = a_0 x_2^m + a_1 x_1 x_2^{m-1} + \dots + a_{m-1} x_1^{m-1} x_2 + a_m x_1^m \,.$$

Omvendt kan ethvert *homogent* polynomium $h \in \mathbb{C}[x_1, x_2]$ i *to* variable *dehomogeniseres* til et polynomium $h_* \in \mathbb{C}[x_1]$ i *én* variabel, nemlig $h_*(x_1) = h(x_1, 1) \in \mathbb{C}[x_1]$.

(5) **Eksempler.** Hvis $f(x_1) = 1 + 2x_1 + 3x_1^2$, da er $f^*(x_1, x_2) = x_2^2 + 2x_1 x_2 + 3x_1^2$. Hvis $h(x_1, x_2) = x_1^3 x_2 + x_1^2 x_2^2 + x_1 x_2^3$ (der er homogent), da er $h_*(x_1) = x_1^3 + x_1^2 + x_1$.

(6) **Sætning.** *Der gælder* $(fg)^* = f^* g^*$ *for alle* $f, g \in \mathbb{C}[x_1]$.

(7) *Bevis.* [Vi ønsker at bevise $(fg)^*(x_1, x_2) = f^*(x_1, x_2) g^*(x_1, x_2)$ for alle $(x_1, x_2) \in \mathbb{C}^2$.] Lad f og g være givet ved henholdsvis $f(x_1) = \sum_{i=0}^{m} a_i x_1^i$ og $g(x_1) = \sum_{j=0}^{n} b_j x_1^j$ med $a_m \neq 0$ og $b_n \neq 0$ (og dermed $\deg f = m$ og $\deg g = n$). Vi har

$$(fg)(x_1) = \sum_{h=0}^{m+n} \left(\sum_{i+j=h} a_i b_j \right) x_1^h \quad \text{og}$$

$$\begin{aligned}
(fg)^*(x_1, x_2) &= \sum_{h=0}^{m+n} \left(\sum_{i+j=h} a_i b_j \right) x_1^h x_2^{m+n-h} \\
&= \left(\sum_{i=0}^{m} a_i x_1^i x_2^{m-i} \right) \left(\sum_{j=0}^{n} b_j x_1^j x_2^{n-j} \right) \\
&= f^*(x_1, x_2) g^*(x_1, x_2) \,. \quad \square
\end{aligned}$$

(1) **Divisorer.** For polynomier $h, p \in \mathbb{C}[x_1, x_2]$ siges p at være en *divisor i* (eller gå op i) h, hvis der findes $q \in \mathbb{C}[x_1, x_2]$, så $h = pq$, og i så fald skrives $p \mid h$. Til ethvert $h \in \mathbb{C}[x_1, x_2]$ findes $r \in \mathbb{N}_0$ og $k \in \mathbb{C}[x_1, x_2]$, så $h(x_1, x_2) = x_2^r k(x_1, x_2)$, og så x_2 ikke er divisor i k. F.eks. er $x_1^2 x_2^2 + x_1 x_2^3 = x_2^2(x_1^2 + x_1 x_2)$.

(2) **Sætning.** *Hvis $k \in \mathbb{C}[x_1, x_2]$ er homogent og ikke har x_2 som divisor, da gælder $(k_*)^* = k$.*

(3) *Bevis.* Idet $n = \deg k$, findes $c_0, c_1, \ldots, c_n \in \mathbb{C}$, så $k(x_1, x_2) = c_0 x_2^n + c_1 x_1 x_2^{n-1} + \cdots + c_n x_1^n$; her er $c_n \neq 0$ (da x_2 ikke går op i k). Polynomiet $k_*(x_1) = c_0 + c_1 x_1 + \cdots + c_n x_1^n$ har grad n (da $c_n \neq 0$), og derfor har vi

$$(k_*)^*(x_1, x_2) = \sum_{i=0}^{n} c_i x_1^i x_2^{n-i} = k(x_1, x_2)\,. \quad \square$$

(4) **Eksempel.** Betragt $h(x_1, x_2) = x_1 x_2$, der er homogent. Her er $h_*(x_1) = x_1$ og $(h_*)^*(x_1, x_2) = x_1 \neq h(x_1, x_2)$ (men $x_2 \mid h(x_1, x_2)$).

(5) **Sætning.** *Ethvert* **homogent** *polynomium $h \in \mathbb{C}[x_1, x_2]$ i* **to** *variable af grad $n \in \mathbb{N}$ er produkt af n homogene førstegradspolynomier: der findes $a_{11}, \cdots, a_{n1}, a_{12}, \cdots, a_{n2} \in \mathbb{C}$, så $h(x_1, x_2) = (a_{11}x_1 + a_{12}x_2) \cdots (a_{n1}x_1 + a_{n2}x_2)$.*

(6) *Bevis.* Vælg $r \in \mathbb{N}_0$ og $k \in \mathbb{C}[x_1, x_2]$, så $h(x_1, x_2) = x_2^r k(x_1, x_2)$, og x_2 ikke går op i k. Algebraens Fundamentalsætning anvendt på $k_* \in \mathbb{C}[x_1]$ giver $a_{11}, \cdots, a_{m1}, a_{12}, \cdots, a_{m2}$ i $\mathbb{C}$, så $k_*(x_1) = (a_{11}x_1 + a_{12}) \cdots (a_{m1}x_1 + a_{m2})$. Sætningerne 3(2) og 2(6) giver nu det ønskede:

$$\begin{aligned}
h(x_1, x_2) &= x_2^r k(x_1, x_2) \\
&= x_2^r (k_*(x_1))^* \\
&= x_2^r \big((a_{11}x_1 + a_{12}) \cdots (a_{m1}x_1 + a_{m2})\big)^* \\
&= x_2^r (a_{11}x_1 + a_{12})^* \cdots (a_{m1}x_1 + a_{m2})^* \\
&= x_2^r (a_{11}x_1 + a_{12}x_2) \cdots (a_{m1}x_1 + a_{m2}x_2) \\
&= (a_{11}x_1 + a_{12}x_2) \cdots (a_{m1}x_1 + a_{m2}x_2)(0x_1 + x_2)^r\,. \quad \square
\end{aligned}$$

(7) **Opgave.** Gælder $(f^*)_* = f$ for alle $f \in \mathbb{C}[x_1]$?

(8) **Homogenisering og dehomogenisering;** 2 **og** 3 **variable.** Ethvert polynomium

$$f(x_1, x_2) = \sum_{h=0}^{m} \left(\sum_{i+j=h} a_{ij} x_1^i x_2^j \right) \in \mathbb{C}[x_1, x_2]$$

i *to* variable af grad m *homogeniseres* til det *homogene* polynomium

$$f^*(x_1, x_2, x_3) = \sum_{h=0}^{m} \left(\sum_{i+j=h} a_{ij} x_1^i x_2^j \right) x_3^{m-h} \in \mathbb{C}[x_1, x_2, x_3] \; (= \mathbb{C}[x_1, x_2][x_3])$$

i *tre* variable og af grad m.

Ethvert *homogent* polynomium $h \in \mathbb{C}[x_1, x_2, x_3]$ i *tre* variable *dehomogeniseres* til et polynomium $h_*(x_1, x_2) = h(x_1, x_2, 1) \in \mathbb{C}[x_1, x_2]$.

Beviserne for de næste to sætninger er analoge til 2(7) og (3), henholdsvis.

(1) **Sætning.** *For alle* $f, g \in \mathbb{C}[x_1, x_2]$ *gælder* $(fg)^* = f^*g^*$. $\square$

(2) **Sætning.** *Hvis* $k \in \mathbb{C}[x_1, x_2, x_3]$ *er homogent og ikke har* x_3 *som divisor, da gælder* $(k_*)^* = k$. $\square$

(3) **Opgave.** Gælder $(hk)_* = h_*k_*$ for alle $h, k \in \mathbb{C}[x_1, x_2, x_3]$?

(4) **Opgave.** Bevis, at ikke alle homogene $h \in \mathbb{C}[x_1, x_2, x_3]$ er produkt af homogene førstegradspolynomier. Betragt f.eks. $h(x_1, x_2, x_3) = x_1^2 - x_2x_3$, antag $h = fg$, hvor f og g er begge er homogene af grad 1, og udnyt $h_* = f_*g_*$, der er et produkt af polynomier af grad højst 1, til en modstrid, sml. (11) nedenfor.

(5) **Hovedidealer.** For $f \in \mathbb{C}[x_1, x_2]$ betegner (f) *hovedidealet* frembragt af f; altså $(f) = \{\, af \mid a \in \mathbb{C}[x_1, x_2] \,\}$. For $f, g \in \mathbb{C}[x_1, x_2]$ gælder

(6) $$f \mid g \iff (f) \supseteq (g)\,.$$

Et polynomium u er et invertibelt element (eller en enhed) i ringen $\mathbb{C}[x_1, x_2]$, hvis og kun hvis u er en ikke-triviel konstant, dvs. $u \in \mathbb{C} \setminus \{o\}$. To polynomier $f, g \in \mathbb{C}[x_1, x_2]$ frembringer samme hovedideal, netop hvis de er *associerede*; altså

(7) $$(f) = (g) \iff \exists\, c \in \mathbb{C} \setminus \{o\}\colon f = cg\,.$$

Bemærk i øvrigt, at der gælder

(8) $$(f) = (g) \;\Rightarrow\; \deg f = \deg g \;\wedge\; \operatorname{ord} f = \operatorname{ord} g\,.$$

(9) **Irreducible polynomier.** Et polynomium $p \in \mathbb{C}[x_1, x_2]$ kaldes *irreducibelt*, når $p \notin \mathbb{C}$, dvs. p er ikke er konstant, og der gælder

$$\forall\, a, b \in \mathbb{C}[x_1, x_2]\colon\; p = ab \;\Rightarrow\; a \in \mathbb{C} \;\vee\; b \in \mathbb{C}\,.$$

Da $\mathbb{C}[x_1, x_2]$ er en *faktoriel* ring, dvs. *UFD*, altså *unique factorization domain*, findes der til ethvert ikke-trivielt $f \in \mathbb{C}[x_1, x_2]$ et $m \in \mathbb{N}_0$ og irreducible $p_1, \dots, p_m \in \mathbb{C}[x_1, x_2]$, så $f = p_1 \cdots p_m$, og denne faktorisering er entydig pånær rækkefølge og associering: Hvis også $f = q_1 \cdots q_n$ med $q_1, \dots, q_n \in \mathbb{C}[x_1, x_2]$ irreducible, da er $n = m$, og q_i'erne kan omnummereres, så $(q_i) = (p_i)$ for alle i.

Endvidere følger, at ethvert irreducibelt $p \in \mathbb{C}[x_1, x_2]$ er et *primelement* i ringen $\mathbb{C}[x_1, x_2]$, dvs.

$$\forall\, a, b \in \mathbb{C}[x_1, x_2]\colon\; p \mid ab \;\Rightarrow\; p \mid a \;\vee\; p \mid b\,,$$

og dermed gælder for alle $p \in \mathbb{C}[x_1, x_2]$, at

(10) $$p \text{ er et irreducibelt polynomium} \iff (p) \text{ er et primideal i } \mathbb{C}[x_1, x_2]\,.$$

Til implikationen mod venstre blev benyttet, at ethvert primelement er irreducibelt.

Hvis $f \in \mathbb{C}[x_1, x_2]$ er lineært, dvs. $\deg f = 1$, da er f irreducibelt, sml. 2(2). Hvis $h \in \mathbb{C}[x_1, x_2]$ er homogent og af grad mindst 2, da er h ikke irreducibelt, sml. 3(5).

(11) **Opgave.** Bevis, at polynomiet $x_1^2 - x_2$ er irreducibelt.

(1) **Opgave.** Antag, at $m, n \in \mathbb{N}$ ikke har fælles primdivisor og $m > n$. Bevis, at polynomiet $x_1^m - cx_2^n$ er irreducibelt for alle $c \in \mathbb{C} \setminus \{0\}$ (f.eks. ved at udnytte og bevise, at hvis $f \in \mathbb{C}[x_1, x_2]$ har $\deg f < m$, og der findes $d \in \mathbb{C} \setminus \{0\}$, så $f(dt^n, t^m) = 0$ for alle $t \in \mathbb{C}$, da er $f = 0$).

(2) **Irreducible homogene polynomier.** Teorien for irreducible polynomier i tre varible – altså for irreducible elementer i ringen $\mathbb{C}[x_1, x_2, x_3]$ – er helt analog med den i 4(9)&(10) beskrevne vedrørende to variable – dvs. ringen $\mathbb{C}[x_1, x_2]$. Specielt kan ethvert ikke-trivielt $f \in \mathbb{C}[x_1, x_2, x_3]$ skrives som produkt af irreducible, og denne fremstilling er entydig pånær rækkefølge og associering. Ifølge 2(2) gælder for $f, g, h \in \mathbb{C}[x_1, x_2, x_3]$, at

(3) $$h = fg \quad \wedge \quad h \text{ er homogent} \qquad \Rightarrow \qquad f \text{ og } g \text{ er homogene.}$$

Heraf følger, at ethvert ikke-trivielt *homogent* polynomium er produkt af irreducible *homogene* polynomier.

(4) **Lemma.** *Hvis f tilhører $\mathbb{C}[x_1, x_2]$, da gælder*

(5) $$f \text{ er irreducibelt} \quad \Longleftrightarrow \quad f^* \text{ er irreducibelt.}$$

Hvis $h \in \mathbb{C}[x_1, x_2, x_3]$ er homogent og uden x_3 som divisor, da gælder

(6) $$h \text{ er irreducibelt} \quad \Longleftrightarrow \quad h_* \text{ er irreducibelt.}$$

(7) *Bevis.* Først bevises "$\Leftarrow$" i (5). Antag, at f er reducibel: $f = ab$ med $a, b \in \mathbb{C}[x_1, x_2]$ ikke-konstante. 4(1) giver $f^* = a^* b^*$, som viser, at f^* er reducibel, da a^* og b^* ikke er konstante.

Nu følger "$\Rightarrow$" i (6) af det lige beviste, da $(h_*)^* = h$ ifølge 4(2).

Dernæst bevises "$\Leftarrow$" i (6). Antag, at h er reducibel: $h = fg$ med $f, g \in \mathbb{C}[x_1, x_2]$ ikke-konstante. Da x_3 ikke er divisor i h, kan den heller ikke være divisor i f eller g, og derfor er f_* og g_* ikke-konstante. Da $h_* = f_* g_*$, er h_* reducibel.

Nu følger "$\Rightarrow$" i (5) direkte, da $(f^*)_* = f$. $\square$

(8) **Homogene polynomier og lineære afbildninger.** Lad $h \in \mathbb{C}[x_1, x_2, x_3]$ være et homogent polynomium af grad n, og lad $\underline{\psi} = (\psi_1, \psi_2, \psi_3) \colon \mathbb{C}^3 \to \mathbb{C}^3$ være en lineær afbildning bestående af de lineære funktioner $\psi_1, \psi_2, \psi_3 \colon \mathbb{C}^3 \to \mathbb{C}$; for $\underline{x} = (x_1, x_2, x_3) \in \mathbb{C}^3$ gælder altså $\underline{\psi}(\underline{x}) = (\psi_1(\underline{x}), \psi_2(\underline{x}), \psi_3(\underline{x}))$. For hvert i er $\psi_i(x_1, x_2, x_3)$ et homogent polynomium af grad 1, og dermed er

$$(h \circ \underline{\psi})(x_1, x_2, x_3) = h(\psi_1(x_1, x_2, x_3), \psi_2(x_1, x_2, x_3), \psi_3(x_1, x_2, x_3))$$

et homogent polynomium af grad n (eventuelt nulpolynomiet).

(9) **Eksempel.** For det homogene polynomium $h(x_1, x_2, x_3) = x_1^2 - x_2 x_3 \in \mathbb{C}[x_1, x_2, x_3]$ og den lineære afbildning $\underline{\psi} \colon \mathbb{C}^3 \to \mathbb{C}^3$ givet ved $\underline{\psi}(x_1, x_2, x_3) = (x_1, -x_2 + x_3, x_2 + x_3)$ gælder $(h \circ \underline{\psi})(x_1, x_2, x_3) = x_1^2 - (-x_2 + x_3)(x_2 + x_3) = x_1^2 + x_2^2 - x_3^2$.

(10) **Opgave.** Bestem h og $\underline{\psi}$ som i (8) med $h \neq o$ og $\underline{\psi} \neq \underline{o}$ (idet $\underline{o} \colon \mathbb{C}^3 \to \mathbb{C}^3$ er nulafbildningen), så $h \circ \underline{\psi} = o$.

(1) **Sætning.** *Hvis* $h \in \mathbb{C}[x_1, x_2, x_3]$ *er et homogent polynomium, der ikke er trivielt (dvs.* $h \neq o$*), og* $\underline{\psi}\colon \mathbb{C}^3 \to \mathbb{C}^3$ *er en isomorfi, da er polynomiet* $h \circ \underline{\psi}$ *ikke-trivielt.*

(2) *Bevis.* Dette følger af: $(h \circ \underline{\psi}) \circ \underline{\psi}^{-1} = h \circ (\underline{\psi} \circ \underline{\psi}^{-1}) = h \neq o.$ $\square$

(3) **Sætning.** *Hvis* $\underline{\psi}\colon \mathbb{C}^3 \to \mathbb{C}^3$ *er en isomorfi, og* $h \in \mathbb{C}[x_1, x_2, x_3]$ *er et irreducibelt homogent polynomium, da er polynomiet* $h \circ \underline{\psi}$ *irreducibelt.*

(4) *Bevis.* Dette følger af, at der gælder $(fg)\circ\underline{\psi} = (f\circ\underline{\psi})(g\circ\underline{\psi})$ for $f, g \in \mathbb{C}[x_1, x_2, x_3]$. $\square$

(5) **Lemma.** *Antag, at* $\underline{\varphi}, \underline{\psi}\colon \mathbb{C}^3 \to \mathbb{C}^3$ *er isomorfier, der inducerer ens koordinatskift i* $\mathbb{P}^2_{\mathbb{C}}$ *. Da findes* $c \in \mathbb{C}$*, så* $\underline{\varphi} = c\underline{\psi}$*.*

(6) *Bevis.* Antagelsen $\underline{\underline{\varphi}} = \underline{\underline{\psi}}$ betyder, at for alle $\underline{u} \in \mathbb{C}^3_{\varnothing}$ er vektorerne $\underline{\varphi}(\underline{u})$ og $\underline{\psi}(\underline{u})$ proportionale. Lad nu $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$ være en basis for $\mathbb{C}^3$ (f.eks. den naturlige basis). Vælg for hvert i et $c_i \in \mathbb{C}$, så $\underline{\varphi}(\underline{e}_i) = c_i\underline{\psi}(\underline{e}_i)$. Sæt $\underline{w} = \underline{e}_1 + \underline{e}_2 + \underline{e}_3$, og vælg $c \in \mathbb{C}$, så $\underline{\varphi}(\underline{w}) = c\underline{\psi}(\underline{w})$. Vi har

(7)
$$\begin{aligned} c_1\underline{\psi}(\underline{e}_1) + c_2\underline{\psi}(\underline{e}_2) + c_3\underline{\psi}(\underline{e}_3) &= \underline{\varphi}(\underline{e}_1) + \underline{\varphi}(\underline{e}_2) + \underline{\varphi}(\underline{e}_3) = \underline{\varphi}(\underline{w}) = c\underline{\psi}(\underline{w}) \\ &= c\underline{\psi}(\underline{e}_1) + c\underline{\psi}(\underline{e}_2) + c\underline{\psi}(\underline{e}_3) \end{aligned}$$

Da $\underline{\psi}$ er en isomorfi, er $(\underline{\psi}(\underline{e}_1), \underline{\psi}(\underline{e}_2), \underline{\psi}(\underline{e}_3))$ er en basis for $\mathbb{C}^3$, og (7) giver derfor, at $c_1 = c$, $c_2 = c$ og $c_3 = c$. Heraf fås for $\underline{v} = v_1\underline{e}_1 + v_2\underline{e}_2 + v_3\underline{e}_3 \in \mathbb{C}^3$, at

$$\begin{aligned} \underline{\varphi}(\underline{v}) &= v_1\underline{\varphi}(\underline{e}_1) + v_2\underline{\varphi}(\underline{e}_2) + v_3\underline{\varphi}(\underline{e}_3) \qquad = v_1c_1\underline{\psi}(\underline{e}_1) + v_2c_2\underline{\psi}(\underline{e}_2) + v_3c_3\underline{\psi}(\underline{e}_3) \\ &= v_1c\underline{\psi}(\underline{e}_1) + v_2c\underline{\psi}(\underline{e}_2) + v_3c\underline{\psi}(\underline{e}_3) = c(v_1\underline{\psi}(\underline{e}_1) + v_2\underline{\psi}(\underline{e}_2) + v_3\underline{\psi}(\underline{e}_3)) \\ &= c\underline{\psi}(\underline{v})\,; \end{aligned}$$

altså $\underline{\varphi} = c\underline{\psi}$. $\square$

(8) **Kommentar.** Det næste resultat er vigtigt ved koordinatskifte af projektive kurver, sml. 4.5(1).

(9) **Korollar.** *Hvis* $\underline{\varphi}, \underline{\psi}\colon \mathbb{C}^3 \to \mathbb{C}^3$ *er isomorfier, der inducerer ens koordinatskift i* $\mathbb{P}^2_{\mathbb{C}}$ *, og* $h \in \mathbb{C}[x_1, x_2, x_3]$ *er homogent, da er hovedidealerne* $(h \circ \underline{\varphi}^{-1})$ *og* $(h \circ \underline{\psi}^{-1})$ *i ringen* $\mathbb{C}[x_1, x_2, x_3]$ *ens.*

(10) *Bevis.* Ifølge (5) findes $c \in \mathbb{C}$, så $\underline{\varphi} = c\underline{\psi}$, og dermed gælder $h \circ \underline{\varphi}^{-1} = c^{-1}h \circ \underline{\psi}^{-1}$; altså $(h \circ \underline{\varphi}^{-1}) = (h \circ \underline{\psi}^{-1})$. $\square$

4. KURVER

(1) **Affin nulpunktsmængde.** Lad $f(x_1,x_2)$ være et komplekst polynomium i to variable. *Den affine nulpunktsmængde* for f er

$$\mathrm{V}(f) = \{\, (p_1,p_2) \in \mathbb{A}^2_{\mathbb{C}} \mid f(p_1,p_2) = 0 \,\}\,.$$

Hvis $c \in \mathbb{C}[x_1,x_2]$ er konstant og ikke o, da er $\mathrm{V}(c) = \varnothing$, mens $\mathrm{V}(o) = \mathbb{A}^2_{\mathbb{C}}$. Ordet "affin" udelades ofte, når det ikke giver anledning til misforståelser. Hvis to polynomier er associerede, da har de samme nulpunktsmængde, dvs. (sml. 3.4(7))

(2)
$$(f) = (g) \quad \Rightarrow \quad \mathrm{V}(f) = \mathrm{V}(g)\,.$$

Da $(fg)(p_1,p_2) = f(p_1,p_2)g(p_1,p_2)$ (per definition), har vi

(3)
$$\mathrm{V}(fg) = \mathrm{V}(f) \cup \mathrm{V}(g)\,.$$

(4) **Sætning.** *Hvis $f \in \mathbb{C}[x_1,x_2]$ ikke er konstant, da er* $\mathrm{V}(f)$ *en uendelig mængde.*

(5) *Bevis.* Idet $f(x_1,x_2) = \sum_{i,j} a_{ij}x_1^i x_2^j$ med $a_{ij} \in \mathbb{C}$ betragtes graden $\deg_1 f$ af f som polynomium kun i x_1 samt graden $\deg_2 f$ af f som polynomium kun i x_2 , dvs.

(6)
$$\begin{aligned}&\deg_1 f = \sup\{\, i \in \mathbb{N}_0 \mid \exists\, j \in \mathbb{N}_0 \colon a_{ij} \neq 0 \,\} \text{ samt}\\ &\deg_2 f = \sup\{\, j \in \mathbb{N}_0 \mid \exists\, i \in \mathbb{N}_0 \colon a_{ij} \neq 0 \,\}\,.\end{aligned}$$

Da f ikke er konstant er disse grader ikke begge nul; antag f.eks. $n = \deg_2 f > 0$. Vi kan altså skrive f på følgende måde

$$f(x_1,x_2) = p_0(x_1) + p_1(x_1)x_2 + \cdots + p_n(x_1)x_2^n \in \mathbb{C}[x_1][x_2]$$

med $p_i(x_1) \in \mathbb{C}[x_1]$ og $p_n(x_1) \neq 0$. Da p_n kun har endelig mange nulpunkter, findes en *uendelig* delmængde A af $\mathbb{C}$, så $p_n(a) \neq 0$ for alle $a \in A$. Til ethvert $a \in A$ vælges et nulpunkt b_a for n'te grads polynomiet

$$f(a,x_2) = p_0(a) + p_1(a)x_2 + \cdots + p_n(a)x_2^n \in \mathbb{C}[x_2]\,;$$

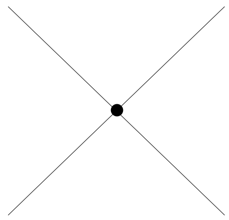
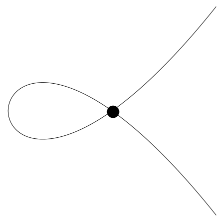
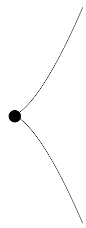
dvs. $b_a \in \mathbb{C}$ vælges så $f(a,b_a) = p_0(a) + p_1(a)b_a + \cdots + p_n(a)b_a^n = 0$. Dermed indeholder $\mathrm{V}(f)$ den uendelige mængde $\{\, (a,b_a) \mid a \in A \,\}$. $\square$

(6) **Affine kurver.** En *plan affin algebraisk kurve* er et hovedideal (f) frembragt af et ikke-konstant polynomium $f \in \mathbb{C}[x_1,x_2]$ og illustreres ved nulpunktsmængden $\mathrm{V}(f)$ (og (2) viser, at dette har mening). Kurverne (x_1) og (x_1^2) er *forskellige* (da polynomierne x_1 og x_1^2 ikke er associerede), men har ens nulpunktsmængde, nemlig $\{\, (0,c) \mid c \in \mathbb{C} \,\}$. Ofte underforstås ordene "plan" og "algebraisk", og man taler blot om affine kurver. For affin kurve (f) og affint punkt $P = (p_1,p_2) \in \mathbb{A}^2_{\mathbb{C}}$, der tilhører $\mathrm{V}(f)$, siges P at *ligge på* kurven (f), eller man siger, at kurven (f) *går igennem* P, og dette skrives også $f(P) = 0$.

(1) **Eksempler.** De fire affine kurver (a), (b), (c) og (d) givet ved

$$a(x_1,x_2) = x_1^2 - x_2\ , \qquad b(x_1,x_2) = x_1^2 - x_2^2\ ,$$
$$c(x_1,x_2) = x_1^2 - x_2^2 + x_1^3 \ \text{ og } \ d(x_1,x_2) = x_1^3 - x_2^2\,,$$

går alle gennem $\bullet\,(0,0)$ og illustreres ved

$(a) = (x_1^2 - x_2)$ $\qquad (b) = (x_1^2 - x_2^2)$ $\qquad (c) = (x_1^2 - x_2^2 + x_1^3)$ $\qquad (d) = (x_1^3 - x_2^2)$

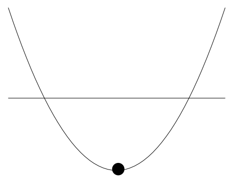
(2) **Irreducible affine kurver.** En affin kurve (f) kaldes *irreducibel*, når (f) er et primideal, dvs. netop når polynomiet f er irreducibelt, sml. 3.4(10).

(3) **Opgave.** Hvilken af kurverne i (1) ovenfor er ikke irreducibel? Bevis, at de andre er det.

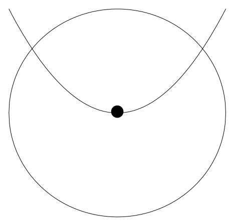
(4) **Fælles komponenter.** Den affine kurve (h) siges at være fælles komponent for de affine kurver (f) og (g), når $(f) \subseteq (h)$ og $(g) \subseteq (h)$, dvs. netop når $h \mid f$ og $h \mid g$.

To forskellige irreducible kurver har ikke fælles komponent.

(5) **Eksempel.** Idet $f = x_2 - x_1^2 - x_2^2 + x_1^2x_2$, $g = x_2 - x_1^2 - x_1^2x_2 - x_2^3 + x_1^4 + x_1^2x_2^2$ og $h = x_2 - x_1^2$, er kurven (h) fælles komponent for kurverne (f) og (g), da $f = (1-x_2)h$ og $g = (1 - x_1^2 - x_2^2)h$.



$((1-x_2)(x_2-x_1^2))$



$((1-x_1^2-x_2^2)(x_2-x_1^2))$

(6) **Opgave.** Har kurverne $3x_1^2 + 5x_1x_2 + 2x_2^2 = 0$ og $x_1^2 + x_1x_2 - 2x_2^2 = 0$ fælles komponent? Sml. 3.3(5).

(7) **Lemma.** *Antag, at $h, k \in \mathbb{C}[x_1,x_2,x_3]$ er homogene, at $(h) = (k)$, dvs. h og k frembringer samme hovedideal i $\mathbb{C}[x_1,x_2,x_3]$, og at $\underline{p}, \underline{q} \in \mathbb{C}^3_\varnothing$ har $\underline{\underline{p}} = \underline{\underline{q}}$ i $\mathbb{P}^2_{\mathbb{C}}$. Da gælder*

$$h(p_1,p_2,p_3) = 0 \iff k(q_1,q_2,q_3) = 0\,.$$

(1) *Bevis.* Antagelserne giver $c, d \in \mathbb{C}$, så $h = ck$ og $\underline{p} = d\underline{q}$. Sæt $n = \deg k$ ($= \deg h$), og vælg $a_{uvw} \in \mathbb{C}$ for $u, v, w \in \mathbb{N}_0$ med $u + v + w = n$, så $k(x_1, x_2, x_3) = \sum_{u+v+w=n} a_{uvw} x_1^u x_2^v x_3^w$. Da har vi

$$\begin{aligned} h(p_1, p_2, p_3) &= ck(p_1, p_2, p_3) \\ &= c \sum_{u+v+w=n} a_{uvw} p_1^u p_2^v p_3^w \\ &= c \sum_{u+v+w=n} a_{uvw} (dq_1)^u (dq_2)^v (dq_3)^w \\ &= cd^n \sum_{u+v+w=n} a_{uvw} q_1^u q_2^v q_3^w \\ &= cd^n k(q_1, q_2, q_3)\,, \end{aligned}$$

hvoraf det ønskede følger. $\square$

(2) **Projektiv nulpunktsmængde.** Antag, at $h \in \mathbb{C}[x_1, x_2, x_3]$ er et *homogent* polynomium. Lemma 2(7) viser, at det har mening at sætte

$$\mathrm{W}(h) = \{\, \underline{\underline{p}} \in \mathbb{P}^2_{\mathbb{C}} \mid h(p_1, p_2, p_3) = 0 \,\}\,,$$

og at der gælder $\mathrm{W}(k) = \mathrm{W}(h)$, hvis $k \in \mathbb{C}[x_1, x_2, x_3]$ og $(h) = (k)$.

(3) **Eksempler.** $\mathrm{W}(x_3^r) = \mathcal{L}_\infty$ for $r \in \mathbb{N}$, og $\mathrm{W}(a_1x_1 + a_2x_2 + a_3x_3) = \mathcal{L}_{\underline{\underline{a}}}$ for $\underline{\underline{a}} \in \mathbb{P}^2_{\mathbb{C}}$.

(4) **Eksempler.** For a, b, c og d i eksempel 2(1) gælder

$$\begin{aligned} a^*(x_1, x_2, x_3) &= x_1^2 - x_2x_3\,, & b^*(x_1, x_2, x_3) &= x_1^2 - x_2^2\,, \\ c^*(x_1, x_2, x_3) &= x_1^2x_3 - x_2^2x_3 + x_1^3 \quad \text{og} & d^*(x_1, x_2, x_3) &= x_1^3 - x_2^2x_3\,, \end{aligned}$$

og dermed

$$\begin{aligned} &\mathrm{W}(a^*) = \mathrm{V}(a) \cup \{(0{:}1{:}0)\} && (\text{dvs. } \mathrm{W}(a^*) \cap \mathcal{L}_\infty = \{(0{:}1{:}0)\}\,); \\ &\mathrm{W}(b^*) = \mathrm{V}(b) \cup \{(1{:}1{:}0), (1{:}{-1}{:}0)\} && (\text{dvs. } \mathrm{W}(b^*) \cap \mathcal{L}_\infty = \{(1{:}1{:}0), (1{:}{-1}{:}0)\}\,); \\ &\mathrm{W}(c^*) = \mathrm{V}(c) \cup \{(0{:}1{:}0)\} && (\text{dvs. } \mathrm{W}(c^*) \cap \mathcal{L}_\infty = \{(0{:}1{:}0)\}\,); \\ &\mathrm{W}(d^*) = \mathrm{V}(d) \cup \{(0{:}1{:}0)\} && (\text{dvs. } \mathrm{W}(d^*) \cap \mathcal{L}_\infty = \{(0{:}1{:}0)\}\,)\,. \end{aligned}$$

(5) **Sætning.** *For enhver affin kurve* (f) *gælder* $\mathrm{W}(f^*) \cap \mathbb{A}^2_{\mathbb{C}} = \mathrm{V}(f)$.

(6) *Bevis.* For $(p_1, p_2) = (p_1 : p_2 : 1) \in \mathbb{A}^2_{\mathbb{C}}$ har vi $f^*(p_1, p_2, 1) = (f^*)_*(p_1, p_2) = f(p_1, p_2)$. $\square$

(7) **Bemærkning.** Lad $f \in \mathbb{C}[x_1, x_2]$ være ikke-trivielt, sæt $m = \operatorname{ord} f$ og $n = \deg f$, og skriv f som sum $f = f_m + f_{m+1} + \cdots + f_{n-1} + f_n$ af homogene polynomier af grader $m, m+1, \ldots, n-1, n$. Da er

(8)
$$\begin{aligned} &f^*(x_1, x_2, x_3) = \\ &f_m(x_1, x_2)x_3^{n-m} + f_{m+1}(x_1, x_2)x_3^{n-m-1} + \cdots + f_{n-1}(x_1, x_2)x_3 + f_n(x_1, x_2)\,. \end{aligned}$$

Endvidere viser 3.3(5), at der findes $a_{11}, a_{12}, \ldots, a_{n1}, a_{n2} \in \mathbb{C}$, så

(9)
$$f_n(x_1, x_2) = (a_{11}x_1 + a_{12}x_2) \cdots (a_{n1}x_1 + a_{n2}x_2)\,.$$

(1) **Sætning.** *Lad* (f) *være en affin kurve af grad* n*, og lad* $a_{11}, a_{12}, \dots, a_{n1}, a_{n2} \in \mathbb{C}$ *give en faktorisering af højestegradsleddet* f_n*:*

$$f_n(x_1, x_2) = (a_{11}x_1 + a_{12}x_2) \cdots (a_{j1}x_1 + a_{j2}x_2) \cdots (a_{n1}x_1 + a_{n2}x_2)\,.$$

Da gælder

$$\mathrm{W}(f^*) \cap \mathcal{L}_\infty = \{(-a_{12} : a_{11} : 0), \dots, (-a_{j2} : a_{j1} : 0), \dots, (-a_{n2} : a_{n1} : 0)\}\,.$$

(2) *Bevis.* For $P = (p_1 : p_2 : 0) \in \mathcal{L}_\infty$ giver 3(8) og faktoriseringen af f_n, at

$$\begin{aligned} f^*(p_1, p_2, 0) &= f_m(p_1, p_2)0^{n-m} + f_{m+1}(p_1, p_2)0^{n-m-1} + \cdots + f_{n-1}(p_1, p_2)0 + f_n(p_1, p_2) \\ &= f_n(p_1, p_2) \\ &= (a_{11}p_1 + a_{12}p_2) \cdots (a_{j1}p_1 + a_{j2}p_2) \cdots (a_{n1}p_1 + a_{n2}p_2)\,. \end{aligned}$$

Hvis P yderligere tilhører $\mathrm{W}(f^*)$, dvs. $f^*(p_1, p_2, 0) = 0$, da viser dette, at der findes et j, så $a_{j1}p_1 + a_{j2}p_2 = 0$, dvs. så (p_1, p_2) er proportional med $(-a_{j2}, a_{j1})$, og dermed $P = (p_1 : p_2 : 0) = (-a_2 : a_1 : 0)$. Nu er inklusionen $\subseteq$ bevist.

Den omvendte inklusion følger også af udtrykket for $f^*(p_1, p_2, 0)$ ovenfor. $\square$

(3) **Forsvinding i uendelig.** Med notation fra (1) ovenfor, siger man, at den affine kurve (f) *forsvinder i uendelig i retningerne* $(-a_{12}, a_{11}), \dots, (-a_{j2}, a_{j1}), \dots, (-a_{n2}, a_{n1})$. Bemærk, at der højst er $n = \deg f$ forskellige retninger.

(4) **Eksempel.** I eksempel 2(1) forsvinder kurverne (a), (c) og (d) i uendelig i retningen $(0, 1)$, altså i lodret retning, mens kurven (b) forsvinder i uendelig i retningerne $(1, 1)$ og $(1, -1)$.

(5) **Projektive kurver.** En *plan projektiv algebraisk kurve* er et hovedideal $C = (h)$ i ringen $\mathbb{C}[x_1, x_2, x_3]$ frembragt af et *ikke-konstant homogent* polynomium $h \in \mathbb{C}[x_1, x_2, x_3]$ og illustreres ved den affine del af nulpunktsmængden $\mathrm{W}(h)$. Ordene "plan" og "algebraisk" udelades for det meste, så man taler blot om projektive kurver, og $\mathrm{W}(h)$ betegnes ofte $\mathrm{W}(C)$.

Lad nu $C = (h)$ være en projektiv kurve. Da alle frembringere for hovedidealet C har samme grad, taler man om graden $\deg C$ af kurven C, og denne grad er positiv, da h ikke er konstant. Lad yderligere $P = \underline{\underline{p}} \in \mathbb{P}^2_{\mathbb{C}}$ være et projektiv punkt, der tilhører $\mathrm{W}(C)$. Man siger, at P *ligger på* kurven C, eller at kurven C *går igennem* P, og dette skrives også $h(P) = 0$.

(6) **Opgave.** Bevis, at $\mathrm{W}(C)$ er uendelig for enhver projektiv kurve C.

(7) **Eksempler.** De 4 projektive kurver A, B, C og D givet ved de homogene polynomier

$$\begin{aligned} a^*(x_1, x_2, x_3) &= x_1^2 - x_2x_3\ , & b^*(x_1, x_2, x_3) &= x_1^2 - x_2^2\ , \\ c^*(x_1, x_2, x_3) &= x_1^2x_3 - x_2^2x_3 + x_1^3 \quad \text{og} & d^*(x_1, x_2, x_3) &= x_1^3 - x_2^2x_3\ , \end{aligned}$$

der fås ved homogenisering af polynomierne fra eksempel 2(1), illustreres på samme måde som dér, sml. 3(5). Kurverne A, C og D går gennem punktet $(0 : 1 : 0) \in \mathcal{L}_\infty$, mens $\mathrm{W}(B) \cap \mathcal{L}_\infty = \{(1 : 1 : 0), (1 : -1 : 0)\}$, sml. 3(4). Punkterne i uendelig er sprogligt beskrevet i 4(4) og studeres grundigere ved at udføre projektive koordinatskift, der nu beskrives.

(1) **Koordinatskifte af projektive kurver.** Lad $C = (h)$ være en projektiv kurve af grad n, og lad $\alpha\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ være et projektivt koordinatskift. Lad $\underline{\varphi}\colon \mathbb{C}^3 \to \mathbb{C}^3$ være en isomorfi, der inducerer α, dvs. $\underline{\underline{\varphi}} = \alpha$. Ifølge 3.5(8) og 3.6(1) er $h \circ \underline{\varphi}^{-1}$ et ikke-trivielt homogent polynomium af grad n, og derfor er $(h \circ \underline{\varphi}^{-1})$ en projektiv kurve af grad n. Hvis også $\underline{\psi}\colon \mathbb{C}^3 \to \mathbb{C}^3$ er en isomorfi, der inducerer α, da viser 3.6(9), at $(h \circ \underline{\varphi}^{-1}) = (h \circ \underline{\psi}^{-1})$. Den projektive kurve $(h \circ \underline{\varphi}^{-1})$ betegnes C_α. Bemærk, at $\deg C_\alpha = \deg C$.

(2) **Sætning.** *Hvis C er en projektiv kurve, og $\alpha\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ er et projektivt koordinatskift, da gælder*

$$\alpha(\mathrm{W}(C)) = \mathrm{W}(C_\alpha)\,.$$

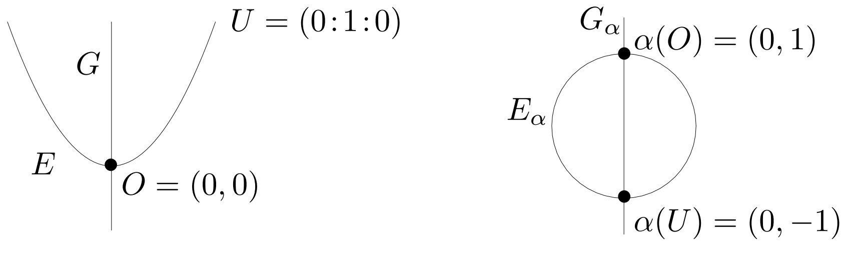
(3) *Bevis.* Antag først, at $\underline{\underline{p}}$ tilhører $\mathrm{W}(C)$, dvs. $\underline{p} \in \mathbb{C}^3_{\emptyset}$ og $h(\underline{p}) = 0$. Da $(h \circ \underline{\varphi}^{-1})(\underline{\varphi}(\underline{p})) = h(\underline{p}) = 0$, har vi $\alpha(\underline{\underline{p}}) = \underline{\underline{\varphi(\underline{p})}} \in \mathrm{W}(h \circ \underline{\varphi}^{-1}) = \mathrm{W}(C_\alpha)$.

Antag dernæst, at $\underline{\underline{q}}$ tilhører $\mathrm{W}(C_\alpha)$, dvs. $\underline{q} \in \mathbb{C}^3_{\emptyset}$ og $(h \circ \underline{\varphi}^{-1})(\underline{q}) = 0$. For $\underline{p} = \underline{\varphi}^{-1}(\underline{q})$ har vi $h(\underline{p}) = (h \circ \underline{\varphi}^{-1})(\underline{q}) = 0$, dvs. $\underline{\underline{p}} \in \mathrm{W}(C)$, og dermed $\underline{\underline{q}} = \underline{\underline{\varphi(\underline{p})}} = \alpha(\underline{\underline{p}}) \in \alpha(\mathrm{W}(C))$. $\square$

(4) **Eksempel.** Lad de projektive kurver $E = (e)$ og $G = (g)$ være givet ved

$$e(x_1, x_2, x_3) = x_1^2 - x_2x_3 \quad \text{og} \quad g(x_1, x_2, x_3) = x_1\,;$$

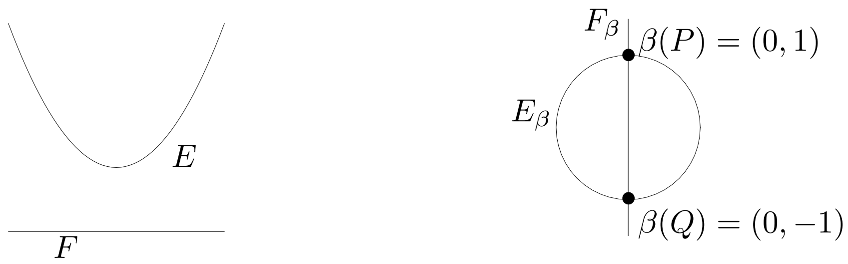
de illustreres som 0.1(3). Betragt koordinatskiftet $\alpha = \underline{\underline{\varphi}}\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ med isomorfien $\underline{\varphi}\colon \mathbb{C}^3 \to \mathbb{C}^3$ givet ved $\underline{\varphi}(\underline{x}) = (x_1, -\frac{1}{2}x_2 + \frac{1}{2}x_3, \frac{1}{2}x_2 + \frac{1}{2}x_3)$ som i eksempel 2.1(3). Da $\underline{\varphi}^{-1}(\underline{x}) = (x_1, -x_2+x_3, x_2+x_3)$, sml. opgave 2.3(2), er $E_\alpha = (x_1^2+x_2^2-x_3^2)$, sml. eksempel 3.5(9), så $\mathrm{W}(E_\alpha) \cap \mathbb{A}^2_{\mathbb{C}} = \mathrm{V}(x_1^2 + x_2^2 - 1)$, dvs. enhedscirklen. Endvidere er



Dette beskriver, hvordan 0.1(3) føres over i 0.3(1), hvor man kan se begge skæringspunkterne mellem E og G.

(5) **Eksempel.** Betragt de projektive kurver $E = (x_1^2 - x_2x_3)$ og $F = (x_2 + x_3)$, der illustreres som 0.1(2), samt koordinatskiftet $\beta(\underline{\underline{x}}) = (x_2 + x_3 : 2ix_1 : -x_2 + x_3)$. Da man let efterviser, at $\beta^{-1}(\underline{\underline{x}}) = (-ix_2 : x_1 - x_3 : x_1 + x_3)$, giver nogle få udregninger, at $E_\beta = (x_1^2 + x_2^2 - x_3^2)$ og $F_\beta = (x_1)$. Kurverne E og F skærer hinanden i $P = (-i, -1)$

$(=(-i:-1:1)\,)$ og $Q=(i,-1)$, og der gælder $\beta(P)=(0:2:2)=(0:1:1)=(0,1)$ og $\beta(Q)=(0,-1)$.



Dette beskriver, hvordan 0.1(2) føres over i 0.3(1) med begge skæringspunkterne.

(1) **Opgave.** Begrund, at 2.2(1) er et specialtilfælde af 5(2).

(2) **Opgave.** Betragt de to projektive kurver $C=(c^*)$ og $D=(d^*)$, hvor $c(x_1,x_2)=1-x_1x_2$ og $d(x_1,x_2)=1+x_1(x_1-x_2)$. Bestem $\mathrm{W}(C)\cap\mathcal{L}_\infty$ og $\mathrm{W}(D)\cap\mathcal{L}_\infty$, og tegn de affine reelle dele af C og D.

(3) **Opgave.** Betragt de tre projektive kurver $F=(x_1x_2-x_3^2)$, $G=(x_1)$ og $H=(x_2)$. Tegn de affine reelle dele af disse kurver. Bestem fællesmængderne $\mathrm{W}(F)\cap\mathrm{W}(G)$, $\mathrm{W}(G)\cap\mathrm{W}(H)$ og $\mathrm{W}(H)\cap\mathrm{W}(F)$.

Begrund, at $\alpha(\underline{x})=(2x_3:-x_1+x_2:x_1+x_2)$ definerer et projektivt koordinatskift $\alpha\colon\mathbb{P}^2_{\mathbb{C}}\longrightarrow\mathbb{P}^2_{\mathbb{C}}$. Bestem kurverne F_α, G_α og H_α. Tegn de affine reelle dele af disse kurver, og angiv fællesmængderne $\mathrm{W}(F_\alpha)\cap\mathrm{W}(G_\alpha)$, $\mathrm{W}(G_\alpha)\cap\mathrm{W}(H_\alpha)$ og $\mathrm{W}(H_\alpha)\cap\mathrm{W}(F_\alpha)$.

(4) **Opgave.** Lad C og L være projektive kurver uden fælles komponent og af grader henholdsvis n og 1. Bevis, at $\mathrm{W}(C)\cap\mathrm{W}(L)$ består af højst n punkter (ved f.eks. at koordinatskifte L over i $\mathcal{L}_\infty$ og udnytte 4.4(1)). (Dette er et specialtilfælde af Bezout's sætning, som er nævnt – men ikke bevist – på side 0.3.)

(5) **Opgave.** Bevis, at $\mathrm{W}(h)\cap\mathbb{A}^2_{\mathbb{C}}=\mathrm{V}(h_*)$ for enhver projektiv kurve (h). (Tag hensyn til, at x_3 kan være divisor i h.)

(6) **Irreducible projektive kurver.** En projektiv kurve (h) kaldes *irreducibel*, når (h) er et primideal, dvs. netop når polynomiet h er irreducibelt.

Den projektive kurve (x_3) er irreducibel med nulpunktsmængde $\mathcal{L}_\infty$. Mere generelt er $a_1x_1+a_2x_2+a_3x_3$ for ethvert $\underline{\underline{a}}\in\mathbb{P}^2_{\mathbb{C}}$ en irreducibel projektiv kurve med nulpunktsmængde $\mathcal{L}_{\underline{\underline{a}}}$.

(7) **Sætning.** *Hvis C er en irreducibel projektiv kurve forskellig fra (x_3), da findes irreducibel affin kurve (f), så $C=(f^*)$ og $\mathrm{W}(C)\cap\mathbb{A}^2_{\mathbb{C}}=\mathrm{V}(f)$.*

(8) *Bevis.* Idet $C=(h)$ for homogent $h\in\mathbb{C}[x_1,x_2,x_3]$, går x_3 ikke op i h (thi ellers er $(h)=(x_3)$, da h er irreducibel). Ifølge 3.4(2) er $h=(h_*)^*$, og ifølge 3.5(6) er h_* irreducibelt, så første påstand er bevist (med $f=h_*$), og den anden følger af 3(5). □

(9) **Eksempel.** Antag, at $m,n\in\mathbb{N}$ ikke har fælles primdivisor og $m>n$. Da er den projektive kurve $(x_1^m-x_2^nx_3^{m-n})$ irreducibel, sml. 3.5(1)&(5).

(1) **Opgave.** Betragt det homogene polynomium

$$h = x_1^5x_2 + x_1^5x_3 - x_1^4x_2^2 + x_1^3x_2x_3^2 - x_1x_2^3x_3^2 + x_2^5x_3 \in \mathbb{C}[x_1, x_2, x_3]\,,$$

og sæt $f = h_*$. Angiv f samt $m = \operatorname{ord} f$ og $n = \deg f$. Opskriv f som sum af homogene polynomier: $f = f_m + \cdots + f_n$. Bestem samtlige lineære faktorer i f_m og i f_n. Bestem $\mathrm{W}(h) \cap \mathcal{L}_\infty$.

Betragt isomorfien $\underline{\varphi}\colon \mathbb{C}^3 \to \mathbb{C}^3$ givet ved $\underline{\varphi}(x_1, x_2, x_3) = (x_3, x_2, x_1)$. Sæt $k = h \circ \underline{\varphi}^{-1}$ og $g = k_*$. Angiv g samt $r = \operatorname{ord} g$ og $s = \deg g$. Opskriv g som sum af homogene polynomier: $g = g_r + \cdots + g_s$. Bestem samtlige lineære faktorer i g_r og i g_s. Bestem $\mathrm{W}(k) \cap \mathcal{L}_\infty$.

Er der noget system i leddenes rækkefølge i angivelsen af polynomiet h ovenfor?

5. TANGENTER

(1) **Begyndelsespunktet** $(0\!:\!0\!:\!1) \in \mathbb{P}^2_{\mathbb{C}}$ betegnes O og tilhører den affine plan:

$$O = (0,0) = (0\!:\!0\!:\!1) \in \mathbb{C}^2 = \mathbb{A}^2_{\mathbb{C}} \subset \mathbb{P}^2_{\mathbb{C}}\,.$$

(Og O er altså ikke nulvektoren $\underline{0} \in \mathbb{C}^3$, der ikke svarer til noget punkt i $\mathbb{P}^2_{\mathbb{C}}$.)

En affin kurve (f) går gennem O, netop hvis $\operatorname{ord} f > 0$, altså netop når f er uden konstantled. Specielt går en lineær affin kurve (ℓ) gennem O, netop hvis ℓ er homogent, altså netop når der findes $a_1, a_2 \in \mathbb{C}$, så $\ell = a_1x_1 + a_2x_2$. For ethvert $\underline{\underline{a}} \in \mathbb{P}^2_{\mathbb{C}}$ tilhører O linien $\mathcal{L}_{\underline{\underline{a}}}$, netop hvis $\underline{\underline{a}}$ tilhører $\mathcal{L}_\infty$.

(2) **Koordinatskift, der bevarer O.** Lad $\alpha\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ være et koordinatskift, der afbilder O i O. Vælg en isomorfi $\underline{\varphi}\colon \mathbb{C}^3 \to \mathbb{C}^3$, der inducerer α, dvs. $\underline{\underline{\varphi}} = \alpha$. Da $\alpha(O) = O = (0\!:\!0\!:\!1)$, findes $c \in \mathbb{C} \setminus \{0\}$, så $\underline{\varphi}(0,0,1) = (0,0,c)$, så vi kan gerne antage $\underline{\varphi}(0,0,1) = (0,0,1)$, og dermed også $\underline{\varphi}^{-1}(0,0,1) = (0,0,1)$. Den naturlige matrix for $\underline{\varphi}^{-1}$ har derfor formen

$$\begin{pmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & 1 \end{pmatrix}.$$

Heraf følger, at $\underline{\varphi}^{-1}(\underline{x}) = (g_1, g_2, g_3 + x_3)$, hvor $g_i = a_{i1}x_1 + a_{i2}x_2$ er homogene lineære polynomier i de *to* variable x_1 og x_2. Der gælder derfor

$$e \circ \underline{\varphi}^{-1} = e(g_1, g_2) \quad \text{for} \quad e \in \mathbb{C}[x_1, x_2] \;\; \text{homogent.} \tag{3}$$

Bemærk, at polynomiet e her kun er i de to variable x_1 og x_2, men det tilhører selvfølgelig også $\mathbb{C}[x_1, x_2, x_3]$, så sammensætningen $e \circ \underline{\varphi}^{-1}$ har mening.

(4) **Linier.** Når (ℓ) er en lineær affin kurve, altså $\ell \in \mathbb{C}[x_1, x_2]$ og $\deg \ell = 1$, omtales (ℓ) ofte som en *affin linie.* Tilsvarende omtales en lineær projektiv kurve (ℓ), altså $\ell \in \mathbb{C}[x_1, x_2, x_3]$ og $\operatorname{ord} \ell = \deg \ell = 1$, ofte som en *projektiv linie.* For $r > 1$ omtales (ℓ^r) ikke som en linie.

For en projektiv linie $L = (a_1x_1 + a_2x_2 + a_3x_3)$ benyttes ofte betegnelsen $\mathcal{L}_{\underline{\underline{a}}}$ (og der gælder jo $\mathrm{W}(L) = \mathcal{L}_{\underline{\underline{a}}}$). Hvis $\alpha\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ er et projektivt koordinatskift, da betegnes linien L_α ofte $\alpha(\mathcal{L}_{\underline{\underline{a}}})$ (og der gælder jo $\mathrm{W}(L_\alpha) = \alpha(\mathcal{L}_{\underline{\underline{a}}})$, sml. 4.5(2)).

(5) **Tangent til kurve i O.** Lad $L = (\ell)$ være en affin linie, og lad $F = (f)$ være en affin kurve med $m = \operatorname{ord} f$ og lavestegradsled f_m; altså $f = \sum_{i+j \geq m} a_{ij}x_1^ix_2^j$ og $f_m = \sum_{i+j=m} a_{ij}x_1^ix_2^j \neq o$. Da siges L at være *tangent til F i O*, netop hvis ℓ er divisor i f_m. Ifølge 3.3(5) er f_m produkt af m lineære homogene polynomier; idet der tages hensyn til, at en lineær faktor kan optræde mere end én gang, fås $f_m = \ell_1^{r_1} \cdots \ell_v^{r_v}$, hvor $\ell_1, \dots, \ell_v \in \mathbb{C}[x_1, x_2]$ er indbyrdes ikke–associerede (sml. 3.4(7)) homogene lineære polynomier, hvor antallet v af lineære faktorer tilhører $\mathbb{N}$, hvor multipliciteterne $r_1, \dots, r_v$ tilhører $\mathbb{N}$, og hvor $r_1 + \cdots + r_v = m$. Linien L er således tangent til F i O, netop hvis $L = (\ell_i)$ for et i. (Her blev benyttet, at lineære polynomier er irreducible, og at faktoriseringen i irreducible polynomier er entydig.) Man siger, at (ℓ_i) er tangent til (f) i O med *multiplicitet* r_i, og når $r_i > 2$, siger man også, at (ℓ_i) er *r_i–dobbelt tangent til F i O.*

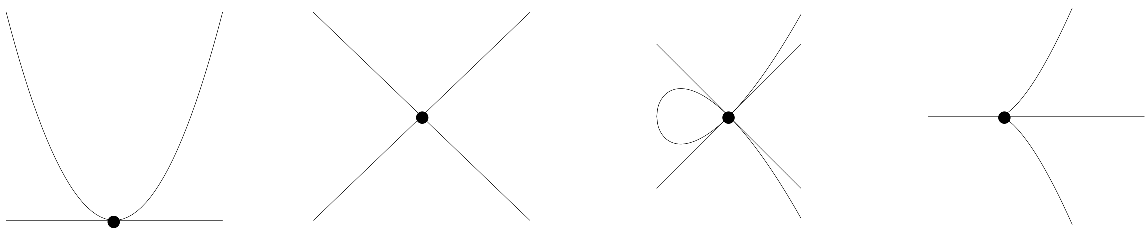
At $r_1 + \cdots + r_v = m = \operatorname{ord} f$ betyder, at kurven (f) har netop $\operatorname{ord} f$ tangenter i O, når disse regnes med multiplicitet.

Lad nu $L = (\ell)$ være en projektiv linie, og lad $C = (h)$ være en projektiv kurve. Da siges L at være *tangent til C i O*, netop hvis (ℓ_*) er tangent til (h_*) i O. Endvidere defineres *multipliciteten* af (ℓ) som tangent til den projektive kurve C i O som værende lig med multipliciteten af (ℓ_*) som tangent til den affine kurve (h_*) i O. For $r \in \mathbb{N}$ kan dette sammenfattes som

$$(1)\qquad \begin{aligned} \ell_* \mid h_{*m} \quad &\iff \quad L \ \text{ er tangent til } \ C \ \text{ i } \ O\,. \\ \ell_*^{\,r} \mid h_{*m} \quad &\iff \quad \begin{cases} L \ \text{ er tangent til } \ C \ \text{ i } \ O \\ \text{af multiplicitet mindst } \ r\,. \end{cases} \end{aligned}$$

Her er $m = \operatorname{ord} h_*$, og h_{*m} er lavestegradsleddet i h_*. Endvidere er $\ell_*^{\,r} = (\ell_*)^{\,r}$, som er lig med $(\ell^{\,r})_*$.

(2) **Eksempler.** De fire affine kurver $(x_1^2 - x_2)$; $(x_1^2 - x_2^2)$; $(x_1^2 - x_2^2 + x_1^3)$ samt $(x_1^3 - x_2^2)$ i eksempel 4.2(1) har tangenter i O henholdsvis (x_2); $(x_1 - x_2)$ og $(x_1 + x_2)$; $(x_1 - x_2)$ og $(x_1 + x_2)$ samt (x_2) som dobbelttangent.



Kurve:	$(x_1^2 - x_2)$	$(x_1^2 - x_2^2)$	$(x_1^2 - x_2^2 + x_1^3)$	$(x_1^3 - x_2^2)$,
Tangent(er):	(x_2)	$(x_1 - x_2), (x_1 + x_2)$	$(x_1 - x_2), (x_1 + x_2)$	$(x_2), (x_2)$.

De fire projektive kurver $(x_1^2 - x_2x_3)$; $(x_1^2 - x_2^2)$; $(x_1^2x_3 - x_2^2x_3 + x_1^3)$ samt $(x_1^3 - x_2^2x_3)$ i eksempel 4.4(7) har tangenter i O henholdsvis (x_2); $(x_1 - x_2)$ og $(x_1 + x_2)$; $(x_1 - x_2)$ og $(x_1 + x_2)$ samt (x_2) som dobbelttangent, og dette illustreres som ovenfor.

(3) **Komponent, der ikke går gennem O.** Betragt projektiv kurve (h) med komponent (f), der ikke går gennem O; altså $h = fk$, hvor $f, k \in \mathbb{C}[x_1, x_2, x_3]$ er homogene, og $f(O) \neq 0$. Da $\operatorname{ord} f_* = 0$, kan konstantleddet i f_* antages at være 1, dvs. $f_{*0} = 1$. Da $h_* = f_*k_*$, har h_* og k_* samme orden m og samme lavestegradsled $h_{*m} = k_{*m}$. Derfor gælder for enhver projektiv linie L, at

$$L \ \text{ er tangent til } \ (h) \ \text{ i } \ O \quad \iff \quad L \ \text{ er tangent til } \ (k) \ \text{ i } \ O\,,$$

og multipliciteten af L som tangent til (h) i O er lig med multipliciteten af L som tangent til (k) i O.

(4) **Sætning.** *Lad L være en projektiv linie, og lad C være en projektiv kurve. For ethvert koordinatskift $\alpha\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ med $\alpha(O) = O$ gælder da:*

$$L \ \textit{ er tangent til } \ C \ \textit{ i } \ O \quad \iff \quad L_\alpha \ \textit{ er tangent til } \ C_\alpha \ \textit{ i } \ O\,,$$

og multipliciteten af L som tangent til C i O er lig med multipliciteten af L_α som tangent til C_α i O.

(1) *Bevis.* Først antages, at (x_3) ikke er komponent i C. Vælg $\ell, h \in \mathbb{C}[x_1, x_2, x_3]$ homogene, så $L = (\ell)$ og $C = (h)$, sæt $f = h_*$, bemærk $f^* = h$ ifølge 3.4(2). Sæt $m = \operatorname{ord} f$ og $n = \deg f$, og skriv $f = f_m + \cdots + f_n$ som sum af homogene led. Med betegnelser fra 1(2) giver 4.3(8)

$$(h \circ \underline{\varphi}^{-1})(\underline{x}) = f_m(g_1, g_2)(g_3 + x_3)^{n-m} + \cdots + f_{n-1}(g_1, g_2)(g_3 + x_3) + f_n(g_1, g_2)\,,$$

hvor hvert $f_i(g_1, g_2) \in \mathbb{C}[x_1, x_2]$ er homogent af grad i. Ved dehomogenisering fås

$$(h \circ \underline{\varphi}^{-1})_*(x_1, x_2) = f_m(g_1, g_2)(g_3 + 1)^{n-m} + \cdots + f_{n-1}(g_1, g_2)(g_3 + 1) + f_n(g_1, g_2)\,,$$

der ved udvikling af $(g_3 + 1)^k$ ses at have orden m og lavestegradsled $f_m(g_1, g_2)$, som er lig med $f_m \circ \underline{\varphi}^{-1}$ (ifølge 1(3)). Da $h_* = f$ giver dette:

(2) $$(h \circ \underline{\varphi}^{-1})_{*m} = h_{*m} \circ \underline{\varphi}^{-1}\,.$$

For $h = \ell^r$ (og $m = r$) giver dette:

(2') $$(\ell^r \circ \underline{\varphi}^{-1})_* = \ell^r_* \circ \underline{\varphi}^{-1}\,.$$

For $p, q \in \mathbb{C}[x_1, x_2]$ gælder følgende formel for produkter af polynomier

$$(pq) \circ \underline{\varphi}^{-1} = (p \circ \underline{\varphi}^{-1})(q \circ \underline{\varphi}^{-1})\,,$$

og dermed også det næste lighedstegn

$$(\ell^r_* q) \circ \underline{\varphi}^{-1} = (\ell^r_* \circ \underline{\varphi}^{-1})(q \circ \underline{\varphi}^{-1}) = (\ell \circ \underline{\varphi}^{-1})^r_*(q \circ \underline{\varphi}^{-1})\,;$$

det sidste lighedstegn følger af (2) og (2').

Det lige beviste giver den første biimplikation i kæden

$$\ell^r_* \mid h_{*m} \iff \ell^r_* \circ \underline{\varphi}^{-1} \mid h_{*m} \circ \underline{\varphi}^{-1} \iff (\ell \circ \underline{\varphi}^{-1})^r_* \mid (h \circ \underline{\varphi}^{-1})_{*m}\,;$$

den anden følger af (2) og (2'). Da $L_\alpha = (\ell \circ \underline{\varphi}^{-1})$ og $C_\alpha = (h \circ \underline{\varphi}^{-1})$, er det ønskede nu bevist, når $\mathcal{L}_\infty$ ikke er komponent i C.

Dernæst antages, at $h = fk$ med $f = x_3^r$, $r \in \mathbb{N}$ og $k \in \mathbb{C}[x_1, x_2, x_3]$ homogent uden x_3 som divisor. Kurven (f) går ikke gennem O, og det gør $(f \circ \underline{\varphi}^{-1})$ derfor heller ikke. Da $(h \circ \underline{\varphi}^{-1}) = (f \circ \underline{\varphi}^{-1})(k \circ \underline{\varphi}^{-1})$, følger det ønskede af det allerede beviste sammenholdt med 2(3). □

(3) **Korollar.** *Lad L være en projektiv linie, lad C være en projektiv kurve, lad P være et punkt i $\mathbb{P}^2_{\mathbb{C}}$, og lad $\beta, \gamma\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ være projektive koordinatskift med $\beta(P) = O$ og $\gamma(P) = O$. Der gælder da:*

$$L_\beta \text{ er tangent til } C_\beta \text{ i } O \iff L_\gamma \text{ er tangent til } C_\gamma \text{ i } O\,,$$

og multipliciteten af L_β som tangent til C_β i O er lig med multipliciteten af L_γ som tangent til C_γ i O.

(4) *Bevis.* Lad $\underline{\varphi}, \underline{\psi}\colon \mathbb{C}^3 \to \mathbb{C}^3$ være isomorfier med $\beta = \underline{\underline{\varphi}}$ og $\gamma = \underline{\underline{\psi}}$, og sæt $\alpha = \gamma \circ \beta^{-1}$, som er det projektive koordinatskift induceret af $\underline{\psi} \circ \underline{\varphi}^{-1}$, sml. 2.1(4)&(6). Bemærk, at $\alpha(O) = O$. Vælg lineært homogent $\ell \in \mathbb{C}[x_1, x_2, x_3]$, så $L = (\ell)$. Der gælder da:

$$(L_\beta)_\alpha = ((\ell \circ \underline{\varphi}^{-1}) \circ (\underline{\psi} \circ \underline{\varphi}^{-1})^{-1}) = (\ell \circ \underline{\psi}^{-1}) = L_\gamma\,.$$

Tilsvarende fås $(C_\beta)_\alpha = C_\gamma$. Anvendes 2(4) på linien L_β og kurven C_β, opnås det ønskede. $\square$

(1) **Tangent til kurve i vilkårligt punkt.** Lad L være en projektiv linie, lad C være en projektiv kurve, lad P være et punkt i $\mathbb{P}^2_{\mathbb{C}}$, og lad r tilhøre $\mathbb{N}$. Da siges L at være *tangent til C i P med multiplicitet r*, netop hvis L_α er tangent til C_α i O med multiplicitet r for *ét* projektivt koordinatskift $\alpha\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ med $\alpha(P) = O$, og 3(3) viser, at det dermed gælder for *alle* sådanne α.

Lad nu $L = (\ell)$ være en affin linie, lad $F = (f)$ være en affin kurve, og lad $\underline{p} = (p_1, p_2)$ være et punkt i $\mathbb{C}^2 = \mathbb{A}^2_{\mathbb{C}}$. Da siges L at være *tangent til C i P med multiplicitet r*, netop hvis den projektive linie (ℓ^*) er tangent til den projektive kurve (f^*) i punktet $\underline{p} = (p_1 : p_2 : 1)$ med multiplicitet r.

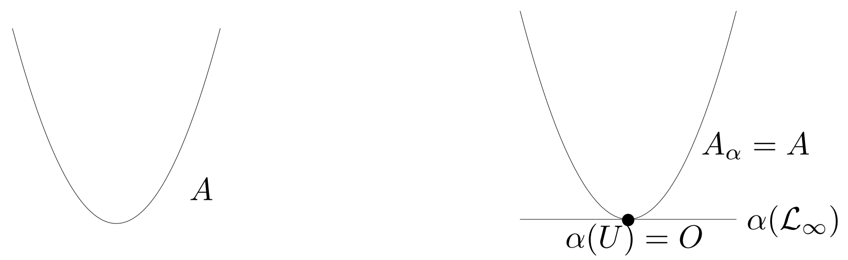
(2) **Sætning.** *Lad L være en projektiv linie, lad C være en projektiv kurve, lad P være et punkt i $\mathbb{P}^2_{\mathbb{C}}$, og lad $\alpha\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ være et projektivt koordinatskift. Der gælder da:*

$$L \text{ er tangent til } C \text{ i } P \iff L_\alpha \text{ er tangent til } C_\alpha \text{ i } \alpha(P),$$

og multipliciteten af L som tangent til C i P er lig med multipliciteten af L_α som tangent til C_α i $\alpha(P)$.

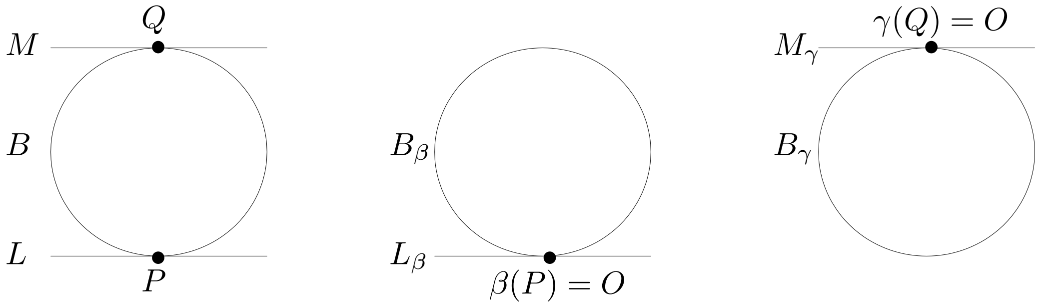
(3) *Bevis.* Vælg et projektivt koordinatskift $\beta\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ med $\beta(\alpha(P)) = O$. Sammensætningen $\beta \circ \alpha\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ er et projektivt koordinatskift med $(\beta\circ\alpha)(P) = O$, så det ønskede følger af definitionen, da $(L_\alpha)_\beta = L_{\beta\circ\alpha}$ og $(C_\alpha)_\beta = C_{\beta\circ\alpha}$. $\square$

(4) **Eksempel.** Betragt den projektive kurve $A = (x_1^2 - x_2x_3)$, som går gennem punktet $U = (0{:}1{:}0)$, der tilhører $\mathcal{L}_\infty$. Lad det projektive koordinatskift $\alpha\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ være givet ved $\alpha(x_1{:}x_2{:}x_3) = (x_1{:}x_3{:}x_2)$. Der gælder $\alpha^{-1} = \alpha$, og α bringer kurven, punktet og linien over i henholdsvis kurven $A_\alpha = (x_1^2 - x_2x_3) = A$, punktet O og linien (x_2), som er tangent til A i O med multiplicitet 1. Derfor er $\mathcal{L}_\infty$ er tangent til A i $(0:1:0)$ med multiplicitet 1.



(5) **Eksempel.** Betragt den projektive kurve $B = (x_1^2 + x_2^2 - x_3^2)$, der går gennem punkterne $P = (0, -1) = (0 : -1 : 1)$ og $Q = (0, 1) = (0 : 1 : 1)$. Betragt også linierne $L = (x_2 + x_3)$ og $M = (x_2 - x_3)$. De projektive koordinatskift $\beta, \gamma\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ givet ved $\beta(x_1 : x_2 : x_3) = (x_1 : x_2 + x_3 : x_3)$ og $\gamma(x_1 : x_2 : x_3) = (x_1 : x_2 - x_3 : x_3)$ er hinandens inverse. β sender kurven B, linien L og punktet P over i henholdsvis kurven $B_\beta = (x_1^2 + (x_2 - x_3)^2 - x_3^2)$, punktet $\beta(P) = O$ og linien $L_\beta = (x_2)$. Tilsvarende sendes B, Q og M ved γ over i $B_\gamma = (x_1^2 + (x_2 + x_3)^2 - x_3^2)$, punktet $\gamma(Q) = O$ og $M_\gamma = (x_2)$. Da

linien (x_2) er tangent til både B_β og B_γ i O (med multiplicitet 1), er L og M tangenter til B i henholdsvis P og Q (begge med multiplicitet 1).



(1) **Kommentar.** Ovennævnte indikerer, at det her indførte tangentbegreb er det samme som det (fra analysen) kendte. Dette uddybes yderligere i næste afsnit.

(2) **Kurvemultiplicitet i O.** Lad $F = (f)$ være en affin kurve. *Multipliciteten af F i O* er tallet $\mathrm{m}_O(F) = \operatorname{ord} f \in \mathbb{N}_0$.

I eksempel 2(2) er kurvemultipliciteterne i O henholdsvis 1, 2, 2 og 2.

Lad nu $C = (h)$ være en projektiv kurve. *Multipliciteten af C i O* er tallet $\mathrm{m}_O(C) = \mathrm{m}_O(h_*) = \operatorname{ord} h_* \in \mathbb{N}_0$.

I eksempel 4(4) er $\mathrm{m}_O(A_\alpha) = 1$. I eksempel 4(5) er $\mathrm{m}_O(B_\beta) = 1$ og $\mathrm{m}_O(B_\gamma) = 1$.

Der gælder:

$$\begin{aligned} O \text{ ligger på } C \quad &\iff \quad \mathrm{m}_O(C) > 0 \\ \mathrm{m}_O(C) \; = \; &\text{antal tangenter til } C \text{ i } O \text{ regnet med multiplicitet.} \end{aligned}$$

(3) **Lemma.** *Lad C være en projektiv kurve. Da gælder $\mathrm{m}_O(C) = \mathrm{m}_O(C_\alpha)$ for ethvert koordinatskift $\alpha\colon \mathbb{P}^2_\mathbb{C} \to \mathbb{P}^2_\mathbb{C}$ med $\alpha(O) = O$.*

(4) *Bevis.* Vælg $h \in \mathbb{C}[x_1, x_2, x_3]$ homogent, så $C = (h)$, og sæt $m = \operatorname{ord} h_*$ som i 3(1), hvor det er bevist, at $m = \operatorname{ord}(h \circ \underline{\varphi}^{-1})_*$. Dette giver det ønskede, da $C_\alpha = (h \circ \underline{\varphi}^{-1})$. $\square$

(5) **Lemma.** *Lad C være en projektiv kurve, lad P tilhøre $\mathbb{P}^2_\mathbb{C}$, og lad $\beta, \gamma\colon \mathbb{P}^2_\mathbb{C} \to \mathbb{P}^2_\mathbb{C}$ være projektive koordinatskift med $\beta(P) = O$ og $\gamma(P) = O$. Da er $\mathrm{m}_O(C_\beta) = \mathrm{m}_O(C_\gamma)$.*

(6) *Bevis.* Betragt $\alpha = \gamma \circ \beta^{-1}$ som i 3(4), og udnyt (3). $\square$

(7) **Kurvemultiplicitet i vilkårligt punkt.** Lad C være en projektiv kurve, og lad P være et punkt i $\mathbb{P}^2_\mathbb{C}$. *Multipliciteten af C i P* er tallet $\mathrm{m}_P(C) = \mathrm{m}_O(C_\alpha)$ for *ét* – og derfor ifølge (5) for *alle* – projektive koordinatskift $\alpha\colon \mathbb{P}^2_\mathbb{C} \to \mathbb{P}^2_\mathbb{C}$ med $\alpha(P) = O$. Der gælder:

$$\begin{aligned} P \text{ ligger på } C \quad &\iff \quad \mathrm{m}_P(C) > 0 \\ \mathrm{m}_P(C) \; = \; &\text{antal tangenter til } C \text{ i } P \text{ regnet med multiplicitet.} \end{aligned}$$

For affin kurve $F = (f)$ og punkt $P \in \mathbb{A}^2_\mathbb{C}$ sættes $\mathrm{m}_P(F) = \mathrm{m}_P(C)$, hvor $C = (f^*)$ er den tilsvarende projektive kurve.

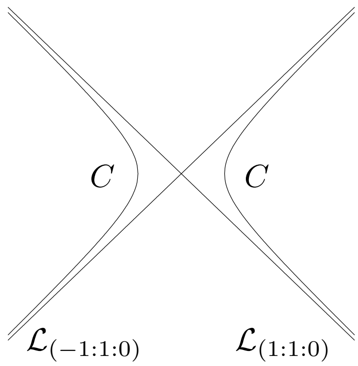
I eksempel 4(4) er $\mathrm{m}_U(A) = \mathrm{m}_O(A_\alpha) = 1$. I eksempel 4(5) er $\mathrm{m}_P(B) = \mathrm{m}_O(B_\beta) = 1$ og $\mathrm{m}_Q(B) = \mathrm{m}_O(B_\gamma) = 1$.

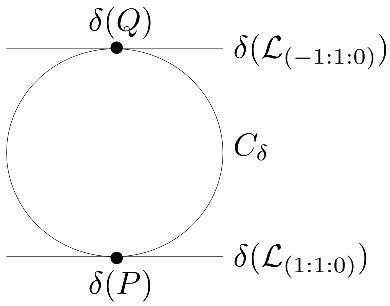
(1) **Opgave.** Lad C være en projektiv kurve, lad P tilhøre $\mathbb{P}^2_{\mathbb{C}}$, og lad $\alpha\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ være et projektivt koordinatskift. Bevis, at $\mathrm{m}_P(C) = \mathrm{m}_{\alpha(P)}(C_\alpha)$.

(2) **Opgave.** Betragt den affine kurve $F = (f) = (x_1^2 - x_2^2 + x_1^3)$ fra 2(2). Bestem samtlige tangenter til (f^*) i punktet $U = (0:1:0)$ (der jo ligger på $\mathcal{L}_\infty$) og tallet $\mathrm{m}_U(f^*)$.

(3) **Opgave.** Betragt den affine kurve $G = (g) = (x_1 + x_2 - x_1^3)$ (der er graf for trediegradspolynomiet $(t+1)t(t-1)$). Bestem samtlige tangenter til (g^*) i punktet $U = (0:1:0)$ og tallet $\mathrm{m}_U(g^*)$.

(4) **Eksempel.** Betragt den projektive kurve $C = (x_1^2 - x_2^2 - x_3^2)$, der går gennem punkterne $P = (1 : -1 : 0)$ og $Q = (1 : 1 : 0)$, der tilhører $\mathcal{L}_\infty$, samt linierne $\mathcal{L}_{(1:1:0)}$ og $\mathcal{L}_{(-1:1:0)}$. Det projektive koordinatskift $\delta\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$, $(x_1 : x_2 : x_3) \mapsto (x_3 : x_2 : x_1)$, har $\delta^{-1} = \delta$ og bringer kurven C, punkterne P og Q samt linierne $\mathcal{L}_{(1:1:0)}$ og $\mathcal{L}_{(-1:1:0)}$ over i henholdsvis $C_\delta = (x_1^2 + x_2^2 - x_3^2)$, $\delta(P) = (0, -1)$ og $\delta(Q) = (0, 1)$, samt linierne $\delta(\mathcal{L}_{(1:1:0)}) = (x_2 + x_3)$ og $\delta(\mathcal{L}_{(-1:1:0)}) = (x_2 - x_3)$. Disse linier er tangenter til C_δ i henholdsvis $(0, -1)$ og $(0, 1)$ (begge med multiplicitet 1). Derfor er $\mathcal{L}_{(1:1:0)}$ og $\mathcal{L}_{(-1:1:0)}$ tangenter til C i henholdsvis $(1:-1:0)$ og $(1:-1:0)$ (begge med multiplicitet 1).





(5) **Asymptoter.** Den affine linie $L = (a_1x_1 + a_2x_2 + a_3)$ er *asymptote* til den affine kurve $F = (f)$ med multiplicitet r, netop hvis $\mathcal{L}_{\underline{\underline{a}}}$ er tangent til (f^*) i $(-a_2 : a_1 : 0)$ med multiplicitet r.

I eksempel (4) er linierne $\mathcal{L}_{(1:1:0)}$ og $\mathcal{L}_{(-1:1:0)}$ begge asymptoter til $(x_1^2 - x_2^2 - 1)$ med multiplicitet 1.

(6) **Opgave.** Betragt den affine kurve $(c) = (1 + x_1x_2 - x_1^2x_2)$. Sammenlign $\mathrm{V}(c) \cap \mathbb{R}^2$ med grafen for funktionen $\omega\colon \mathbb{R} \setminus \{0, 1\} \to \mathbb{R}$ defineret ved $\omega(t) = \big(t(t-1)\big)^{-1}$.

(7) **Opgave.** Betragt kurven (c) fra (6). Bestem mængden $\mathrm{W}(c^*) \cap \mathcal{L}_\infty$. Bestem for ethvert $P \in \mathrm{W}(c^*) \cap \mathcal{L}_\infty$ samtlige tangenter til (c^*) i punktet P. Angiv samtlige assymptoter til (c). Tegn kurven.

(8) **Opgave.** Udfør samme program som i (7) for $(d) = (x_2 - x_1x_2 + x_1^3)$.

(9) **Opgave.** Udfør samme program som i (7) for enhedscirklen $(e) = (x_1^2 + x_2^2 - 1)$. (Husk, at vi arbejder over $\mathbb{C}$.)

(1) **Stilopgave.** *Multipliciteter og tangenter.* Lad $C = (h)$ være en projektiv kurve, og lad $L = (\ell)$ være en projektiv linie.

(a) Angiv definitionen af multipliciteten af C i begyndelsespunktet O, og angiv definitionen af multipliciteten af L som tangent til C i O. Hvis definitionerne gives ved henvisning til tilsvarende definitioner for affine kurver, ønskes disse affine definitioner også angivet.

Angiv et resultat, der giver den præcise sammenhæng mellem multipliciteten af C i O og antallet af tangenter til C i O.

(b) Lad nu $\alpha\colon \mathbb{P}^2_{\mathbb{C}} \longrightarrow \mathbb{P}^2_{\mathbb{C}}$ være et projektivt koordinatskift med $\alpha(O) = O$.

Formulér et resultat, der sammenligner multipliciteterne i O af kurverne C og C_α.

Formulér et resultat, der sammenligner multipliciteterne af linierne L og L_α som tangenter til henholdsvis kurverne C og C_α i O.

Bevis begge disse resultater. Uden yderligere kommentarer kan anvendes, at et sådant koordinatskift er induceret af en isomorfi $\psi\colon \mathbb{C}^3 \longrightarrow \mathbb{C}^3$ af formen

$$(*) \qquad \psi(\underline{x}) = (a_{11}x_1 + a_{12}x_2, a_{21}x_1 + a_{22}x_2, a_{31}x_1 + a_{32}x_2 + x_3)\,.$$

(c) Lad nu P være et vilkårligt punkt i $\mathbb{P}^2_{\mathbb{C}}$.

Formulér et resultat, der muliggør definition af multipliciteten af C i P, og et resultat, der muliggør definition af multipliciteten af L som tangent til C i P.

Angiv disse definitioner.

Bevis ovennævnte resultat.

(d) Antag nu, at $\alpha\colon \mathbb{P}^2_{\mathbb{C}} \longrightarrow \mathbb{P}^2_{\mathbb{C}}$ er et vilkårligt projektivt koordinatskift.

Formulér et resultat, der sammenligner multipliciteten af C i punktet P med multipliciteten af C_α i $\alpha(P)$.

Formulér et resultat, der sammenligner multipliciteten af L som tangent til C i P med multipliciteten af L_α som tangent til C_α i $\alpha(P)$.

Bevis det sidste af disse resultater.

6. Lokal ring i punkt

(1) **Kommentar.** Dette afsnit handler om, at en kurves geometriske egenskaber i "nærheden" af et punkt kan beskrives ved algebraiske egenskaber ved en bestemt ring, der indføres nedenfor, men først bringes lidt nødvendig notation samt et par småresultater (i form af opgaver).

(2) **Endeligt frembragte idealer.** For elementer $a_1, \dots, a_n \in R$ betegner $(a_1, \dots, a_n)$ idealet i R frembragt af $a_1, \dots, a_n$; altså

$$(a_1, \dots, a_n) \overset{\text{def}}{=\!=} \operatorname{span}_R\{a_1, \dots, a_n\} = Ra_1 + \cdots + Ra_n \,,$$

hvis elementer er linearkombinationer af $a_1, \dots, a_n$ med koefficienter fra den *underliggende ring* R. For $n = 1$ (og $a_1 = a$) genfindes hovedidealet $(a) = Ra$, og for $n = 2$ (og $a_1 = a$, $a_2 = b$) haves idealet $(a, b) = Ra + Rb$. Notationen $(a_1, \dots, a_n)$, og dermed specielt notationerne (a) og (a, b), forudsætter således, at den underliggende ring fremgår af den øvrige sammenhæng, som f.eks. er tilfældet ved restklasseringen $R/(a_1, \dots, a_n)$, specielt restklasseringene $R/(a)$ og $R/(a, b)$. Når der er mulighed for forveksling, benyttes en mere udførlig betegnelse: $R(a_1, \dots, a_n) \overset{\text{def}}{=\!=} (a_1, \dots, a_n)$.

(3) **Opgave.** Lad $a \in R$ være givet. Bevis (f.eks. ved polynomiers division med rest), at der til ethvert $p \in R[x]$ findes $q \in R[x]$ og $r \in R$, så $p = (x - a)q + r$. Betragt *evalueringsafbildningen* $\varepsilon_a^R \colon R[x] \to R$ givet ved $p \mapsto p(a)$. Bevis, at den er en surjektiv ringhomomorfi med $\operatorname{Ker} \varepsilon_a^R = (x - a)$ (dvs. hovedidealet i $R[x]$ frembragt af elementet $x - a \in R[x]$), og at ε_a^R inducerer en isomorfi $R[x]/(x - a) \xrightarrow{\cong} R$.

(4) **Opgave.** Betragt for $P = (a_1, a_2) \in \mathbb{A}^2_{\mathbb{C}}$ *evalueringsfunktionen* $\varepsilon_P^{\mathbb{C}} \colon \mathbb{C}[x_1, x_2] \to \mathbb{C}$ givet ved $f \mapsto f(P) = f(a_1, a_2)$, og sæt

(5) $$\mathfrak{m}_P \overset{\text{def}}{=\!=} \operatorname{Ker} \varepsilon_P^{\mathbb{C}} = \{\, f \in \mathbb{C}[x_1, x_2] \mid f(P) = 0 \,\} \,.$$

Begrund, at $\varepsilon_P^{\mathbb{C}}$ inducerer en isomorfi $\mathbb{C}[x_1, x_2]/\mathfrak{m}_P \xrightarrow{\cong} \mathbb{C}$. Bevis:

(6) $$\mathfrak{m}_P = (x_1 - a_1, x_2 - a_2) \,,$$

(7) $$\mathfrak{m}_P \in \operatorname{Max} \mathbb{C}[x_1, x_2] \ (\subseteq \operatorname{Spec} \mathbb{C}[x_1, x_2]) \,.$$

Lad yderligere $F = (f)$ være en affin kurve. Begrund, at der gælder:

(8) $$F \ \text{ går gennem } \ P \quad \Longleftrightarrow \quad (f) \subseteq \mathfrak{m}_P \,.$$

(9) **Lokal ring i et punkt; affint tilfælde.** Lad $P = (a_1, a_2)$ være et punkt i den affine plan $\mathbb{A}^2_{\mathbb{C}}$. Når ringen $\mathbb{C}[x_1, x_2]$ lokaliseres i primidealet $\mathfrak{m}_P$ fås brøkringen

$$\mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}}) \overset{\text{def}}{=\!=} \mathbb{C}[x_1, x_2]_{\mathfrak{m}_P} = \{\, f/s \mid f, s \in \mathbb{C}[x_1, x_2] \ \wedge s(P) \neq 0 \,\} \,,$$

som ifølge ROM 3.7(1) er lokal med maksimalidealet

$$\mathcal{M}_P(\mathbb{A}^2_{\mathbb{C}}) \overset{\text{def}}{=\!=} (\mathfrak{m}_P)_{\mathfrak{m}_P} = \{\, f/s \mid f, s \in \mathbb{C}[x_1, x_2] \ \wedge \ f(P) = 0 \ \wedge \ s(P) \neq 0 \,\} \,.$$

Den kaldes den *lokale ring* for $\mathbb{A}^2_{\mathbb{C}}$ i punktet P; den indeholder integritetsområdet $\mathbb{C}[x_1, x_2]$; og den er en delring af dettes brøklegeme $\mathbb{C}(x_1, x_2)$, sml. ROM 3.3(4).

For $f \in \mathbb{C}[x_1, x_2]$ $(\subseteq \mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}}))$ betragtes restklasseringen:

$$\mathcal{O}_P(f) \stackrel{\text{def}}{=} \mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})/(f).$$

(Her er (f) hovedidealet i $\mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})$ frembragt af f.) Hvis $f = gh$ med $g, h \in \mathbb{C}[x_1, x_2]$ og $h(P) \neq 0$, da er h et invertibelt element i ringen $\mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})$, så f og g frembringer samme hovedideal i denne ring. Altså:

(1) $$f = gh \ \wedge \ h(P) \neq 0 \quad \Rightarrow \quad \mathcal{O}_P(f) = \mathcal{O}_P(g).$$

Restklasseringen $\mathcal{O}_P(f) = \mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})/(f)$ er ikke triviel, netop hvis $(f) \subseteq \mathfrak{m}_P$; altså netop hvis $f(a_1, a_2) = 0$.

For en affin kurve $F = (f)$ sættes:

$$\mathcal{O}_P(F) \stackrel{\text{def}}{=} \mathcal{O}_P(f) = \mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})/(f).$$

Advarsel: I de to linier ovenfor har notationen (f) to forskellige betydninger: først betegner den hovedidealet $\mathbb{C}[x_1, x_2]f$ i $\mathbb{C}[x_1, x_2]$ og dernæst hovedidealet $\mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})f$ i $\mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})$; her fremgår dette selvfølgelig af den øvrige sammenhæng, men ofte benyttes de udførlige betegnelser henholdsvis $\mathbb{C}[x_1, x_2]f$ og $\mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})f$.

Hvis F ikke går gennem P, da er $\mathcal{O}_P(F) = 0$, og vi sætter $\mathcal{M}_P(F) \stackrel{\text{def}}{=} 0$.

Hvis F går gennem P, da er $\mathcal{O}_P(F)$ en lokal ring med maksimalidealet $\mathcal{M}_P(F) \stackrel{\text{def}}{=} \mathcal{M}_P(\mathbb{A}^2_{\mathbb{C}})/(f)$; den kaldes den *lokale ring* for kurven F i punktet P. Brøkringlemmaets isomorfi ROM 3.5(2) giver:

(2) $$\mathcal{O}_P(F) \cong \big(\mathbb{C}[x_1, x_2]/(f)\big)_{\mathfrak{m}'_P},$$

hvor $\mathfrak{m}'_P \stackrel{\text{def}}{=} \mathfrak{m}_P/(f) \ \in \operatorname{Max}\big(\mathbb{C}[x_1, x_2]/(f)\big)$.

(3) **Funktionslegemet for $\mathbb{P}^2_{\mathbb{C}}$.** Brøklegemet $\mathbb{C}(x_1, x_2, x_3)$ for $\mathbb{C}[x_1, x_2, x_3]$ består af brøker h/s med $h, s \in \mathbb{C}[x_1, x_2, x_3]$ og $s \neq 0$. Betragt delmængden:

$$\mathbb{C}(\mathbb{P}^2_{\mathbb{C}}) \stackrel{\text{def}}{=} \{\, h/s \in \mathbb{C}(x_1, x_2, x_3) \mid \ h, s \in \mathbb{C}[x_1, x_2, x_3] \ \text{ homogene af samme grad} \,\}.$$

Dette er et dellegeme af $\mathbb{C}(x_1, x_2, x_3)$; f.eks. er $h/s + k/t = (th + sk)/(st) \in \mathbb{C}(\mathbb{P}^2_{\mathbb{C}})$ for $h/s, k/t \in \mathbb{C}(\mathbb{P}^2_{\mathbb{C}})$, og det kaldes *funktionslegemet for* $\mathbb{P}^2_{\mathbb{C}}$: for $f = h/s \in \mathbb{C}(\mathbb{P}^2_{\mathbb{C}})$ gives en funktion $f \colon \mathbb{P}^2_{\mathbb{C}} \setminus \mathrm{W}(s) \to \mathbb{C}$ ved $f(\underline{a}) = h(\underline{a})/s(\underline{a})$, og dette er en korrekt definition: hvis $\underline{\underline{a}} = \underline{\underline{b}}$, og dermed $\underline{a} = c\underline{b}$ for et $c \in \mathbb{C}$, da er $h(\underline{a})/s(\underline{a}) = c^d h(\underline{b})/c^d s(\underline{b}) = h(\underline{b})/s(\underline{b})$, idet $d = \deg h = \deg s$.

(4) **Lokal ring i et punkt; projektivt tilfælde.** Lad P være et punkt i den projektive plan $\mathbb{P}^2_{\mathbb{C}}$, og betragt følgende delmængde af funktionslegemet:

$$\mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}}) \stackrel{\text{def}}{=} \{\, h/s \in \mathbb{C}(\mathbb{P}^2_{\mathbb{C}}) \mid s(P) \neq 0 \,\}$$

(sml. evt. 4.2(7) vedrørende $s(P) \neq 0$). Det eftervises direkte, at $\mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}})$ er en delring af $\mathbb{C}(\mathbb{P}^2_{\mathbb{C}})$: $0, 1(= 1/1) \in \mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}})$ og $-f, f + g, fg \in \mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}})$ for $f, g \in \mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}})$; og $\mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}})$

er således selv en ring. Betragt nu et elementet $t/s \in \mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}})$ (og i denne notation underforstås her – og i det følgende – at $t, s \in \mathbb{C}[x_1, x_2, x_3]$ er homogene af samme grad og $s(P) \neq 0$). Elementet t/s er invertibelt i $\mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}})$, netop hvis $t(P) \neq 0$. ROM 3.6(6) giver derfor, at $\mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}})$ er en lokal ring med maksimalideal:

$$\mathcal{M}_P(\mathbb{P}^2_{\mathbb{C}}) \stackrel{\text{def}}{=\!=} \{\, h/s \in \mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}}) \mid h(P) = 0 \ \wedge \ s(P) \neq 0 \,\}\,.$$

Ringen $\mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}})$ kaldes den *lokale ring* for $\mathbb{P}^2_{\mathbb{C}}$ i punktet P.

For projektiv kurve $C = (c)$ (med $c \in \mathbb{C}[x_1, x_2, x_3]$ homogent og ikke–konstant) sættes

$$\mathcal{I}_P(C) \stackrel{\text{def}}{=\!=} \{\, h/s \in \mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}}) \mid h \in \mathbb{C}[x_1, x_2, x_3]\, c \,\}\,;$$
$$\mathcal{O}_P(C) \stackrel{\text{def}}{=\!=} \mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}})/\mathcal{I}_P(C)\,.$$

Elementerne i $\mathcal{I}_P(C)$ har således formen ac/s med $a, s \in \mathbb{C}[x_1, x_2, x_3]$ homogene af passende grader (dvs. $\deg a + \deg c = \deg s$ eller $a = 0$) og med $s(P) \neq 0$. Det eftervises let, at $\mathcal{I}_P(C)$ er et ideal i $\mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}})$, så den anden definition ovenfor har altså mening og giver en kommutativ ring, som dog kan være den trivielle, idet der gælder:

(1) $$P \ \text{ ligger på } \ C \quad \Longleftrightarrow \quad \mathcal{I}_P(C) \subseteq \mathcal{M}_P(\mathbb{P}^2_{\mathbb{C}})\,.$$

Hvis $c(P) = 0$, har vi nemlig for $ac/s \in \mathcal{I}_P(C)$, at $(ac)(P) = a(P)c(P) = 0$ og dermed $ac/s \in \mathcal{M}_P(\mathbb{P}^2_{\mathbb{C}})$. Hvis omvendt $c(P) \neq 0$, da har vi $1 = c/c \in \mathcal{I}_P(C)$.

Hvis kurven C går gennem punktet P, da er $\mathcal{O}_P(C)$ en lokal ring med maksimalideal:

$$\mathcal{M}_P(C) \stackrel{\text{def}}{=\!=} \mathcal{M}_P(\mathbb{P}^2_{\mathbb{C}})/\mathcal{I}_P(C)\,,$$

og ringen $\mathcal{O}_P(C)$ kaldes den *lokale ring* for kurven C i punktet P.

Hvis kurven C ikke går gennem P, da er $\mathcal{O}_P(C) = 0$, og vi sætter $\mathcal{M}_P(C) \stackrel{\text{def}}{=\!=} 0$.

(2) **Affin del af projektiv kurve.** Lad $C = (c)$ være en projektiv kurve. Hvis $\mathrm{W}(C) \neq \mathcal{L}_\infty$, da er polynomiet c_* ikke konstant, så (c_*) er en affin kurve; den betegnes C_* , og fra 4.6(5) vides, at $\mathrm{W}(C) \cap \mathbb{A}^2_{\mathbb{C}} = \mathrm{V}(C_*)$.

(3) **Sætning.** *Lad $P = (a_1, a_2)$ tilhøre $\mathbb{A}^2_{\mathbb{C}}$. Der er da en ringisomorfi:*

$$\mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}}) \xrightarrow[\upsilon]{\cong} \mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})$$
$$h/s \mapsto h_*/s_*\,.$$

Hvis C er en projektiv kurve gennem P, da inducerer υ en ringisomorfi:

(4) $$\mathcal{O}_P(C) \xrightarrow[\overline{\upsilon}]{\cong} \mathcal{O}_P(C_*)\,,$$

og for ethvert $n \in \mathbb{N}_0$ er der en isomorfi af vektorrum over $\mathbb{C}$:

(5) $$\mathcal{M}_P(C)^n/\mathcal{M}_P(C)^{n+1} \cong \mathcal{M}_P(C_*)^n/\mathcal{M}_P(C_*)^{n+1}\,.$$

(1) *Bevis.* Først bemærkes, at $P = (a_1 : a_2 : 1) \in \mathbb{A}^2_{\mathbb{C}} \subset \mathbb{P}^2_{\mathbb{C}}$, og at $s_*(P) = s_*(a_1, a_2) = s(a_1, a_2, 1) \neq 0$, da $s(P) \neq 0$, og dette giver $s_* \in \mathbb{C}[x_1, x_2] \setminus \mathfrak{m}_P$.

Dernæst bemærkes, at da dehomogeniseringen $\mathbb{C}[x_1, x_2, x_3] \to \mathbb{C}[x_1, x_2]$, $h \mapsto h_*$ er en ringhomomorfi, er det let at eftervise, at definitionen $\upsilon(h/s) = h_*/s_*$ er korrekt, og at υ er en ringhomomorfi.

Hvis $\upsilon(h/s) = 0$, da er $h_* = 0$ (idet $\mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})$ er et integritetsområde), og dermed $h = 0$ (idet h er homogen og $h = x_3^r(h_*)^*$ for passende $r \in \mathbb{N}_0$). Homomorfien υ er således injektiv. For at indse, at den også er surjektiv, betragt $f/g \in \mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})$ med $f, g \in \mathbb{C}[x_1, x_2]$ og $g(P) \neq 0$, og bemærk $(x_3^n f^*)/(x_3^m g^*) \in \mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}})$ for $m \overset{\text{def}}{=} \deg f$ og $n \overset{\text{def}}{=} \deg g$ samt $f/g = \upsilon\big((x_3^n f^*)/(x_3^m g^*)\big)$.

Nu har vi bevist, at $\upsilon\colon \mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}}) \to \mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})$ er en isomorfi. Da den afbilder idealet $\mathcal{I}_P(C)$ $(\subseteq \mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}}))$ på idealet $\mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})\, c_*$ $(\subseteq \mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}}))$ inducerer den en isomorfi $\overline{\upsilon}\colon \mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}})/\mathcal{I}_P(C) \to \mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})/(c_*)$ som ønsket.

Isomorfien 3(5) følger nu af (3) nedenfor. $\square$

(2) **Opgave.** Lad $(R, \mathcal{M})$ og $(\widetilde{R}, \widetilde{\mathcal{M}})$ være lokale ringe, og lad $\eta\colon R \to \widetilde{R}$ være en ringisomorfi. Bevis $\eta(\mathcal{M}^n) = \widetilde{\mathcal{M}}^n$ for alle $n \in \mathbb{N}_0$, og etablér en R–isomorfi[3]

(3) $$\mathcal{M}^n/\mathcal{M}^{n+1} \cong \widetilde{\mathcal{M}}^n/\widetilde{\mathcal{M}}^{n+1}\,.$$

(4) **Sætning.** *Lad P være et punkt i $\mathbb{P}^2_{\mathbb{C}}$, og lad $\alpha\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ være et projektivt koordinatskift. Der er da en ringisomorfi:*

$$\mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}}) \underset{\widetilde{\alpha}}{\overset{\cong}{\longrightarrow}} \mathcal{O}_{\alpha(P)}(\mathbb{P}^2_{\mathbb{C}})\,,$$

som for enhver projektiv kurve C gennem P inducerer en ringisomorfi:

(5) $$\mathcal{O}_P(C) \underset{\widehat{\alpha}}{\overset{\cong}{\longrightarrow}} \mathcal{O}_{\alpha(P)}(C_\alpha)\,,$$

og for ethvert $n \in \mathbb{N}_0$ er der en isomorfi af vektorrum over $\mathbb{C}$:

(6) $$\mathcal{M}_P(C)^n/\mathcal{M}_P(C)^{n+1} \cong \mathcal{M}_{\alpha(P)}(C_\alpha)^n/\mathcal{M}_{\alpha(P)}(C_\alpha)^{n+1}\,.$$

(7) *Bevis.* Vælg isomorfi $\underline{\varphi}\colon \mathbb{C}^3 \to \mathbb{C}^3$, så $\alpha = \underline{\underline{\varphi}}$. Betragt afbildningen $\widetilde{\underline{\varphi}}\colon \mathbb{C}[x_1, x_2, x_3] \to \mathbb{C}[x_1, x_2, x_3]$ defineret ved $\widetilde{\underline{\varphi}}(h) = h \circ \underline{\varphi}^{-1}$; den er en ringhomomorfi, der er bijektiv (med invers defineret ved $k \mapsto k \circ \underline{\varphi}$); $\widetilde{\underline{\varphi}}$ er altså en ringisomorfi. Da den afbilder et homogent polynomium over i et homogent polynomium af samme grad, inducerer den en ringisomorfi $\widetilde{\alpha}\colon \mathbb{C}(\mathbb{P}^2_{\mathbb{C}}) \to \mathbb{C}(\mathbb{P}^2_{\mathbb{C}})$ givet ved $\widetilde{\alpha}(h/s) = (h \circ \underline{\varphi}^{-1})/(s \circ \underline{\varphi}^{-1})$, og dette afhænger ikke af valg af $\underline{\varphi}$ med $\underline{\underline{\varphi}} = \alpha$. Delringen $\mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}})$ af $\mathbb{C}(\mathbb{P}^2_{\mathbb{C}})$ bliver ved $\widetilde{\alpha}$ afbildet på ringen $\mathcal{O}_{\alpha(P)}(\mathbb{P}^2_{\mathbb{C}})$. Dette giver den første isomorfi i sætningen, og den inducerer den anden, da $\widetilde{\alpha}\big(\mathcal{I}_P(C)\big) = \mathcal{I}_{\alpha(P)}(C_\alpha)$. (6) følger nu af (3). $\square$

---

[3] $\widetilde{R}$ er en R–modul ved R–multiplikationen $r\widetilde{r} \overset{\text{def}}{=} \eta(r)\widetilde{r}$, og $\widetilde{\mathcal{M}}^n$ bliver herved en R–undermodul af $\widetilde{R}$.

(1) **Multiplicitetssætningen.** *Lad P være et punkt i $\mathbb{P}^2_{\mathbb{C}}$, og lad C være en projektiv kurve. Der gælder da:*

$$\dim(\mathcal{M}_P(C)^n/\mathcal{M}_P(C)^{n+1}) = \mathrm{m}_P(C) \quad \textit{for} \ \ n \geq \mathrm{m}_P(C)\,.$$

(2) *Bevis.* Hvis P ikke ligger på C, da er $\mathcal{M}_P(C) = 0$ og $\mathrm{m}_P(C) = 0$, så ligheden bliver $0 = 0$, og den gælder derfor for alle $n \geq 0$.

Antag fra nu af, at P ligger på C. Vælg projektivt koordinatskift $\alpha\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$, så $\alpha(P) = O$. Ifølge 4(6) og 5.6(1) har vi henholdsvis:

(3)
$$\begin{gathered}\mathcal{M}_P(C)^n/\mathcal{M}_P(C)^{n+1} \cong \mathcal{M}_O(C_\alpha)^n/\mathcal{M}_O(C_\alpha)^{n+1}\,;\\ \mathrm{m}_P(C) = \mathrm{m}_O(C_\alpha)\,.\end{gathered}$$

Lad $F = (f)$ være den affine del af C_α. 3(5) og definitionen af multiplicitet af projektiv kurve i punktet O giver nu henholdsvis:

(4)
$$\begin{gathered}\mathcal{M}_O(C_\alpha)^n/\mathcal{M}_O(C_\alpha)^{n+1} \cong \mathcal{M}_O(F)^n/\mathcal{M}_O(F)^{n+1}\,;\\ \mathrm{m}_O(C_\alpha) = \mathrm{m}_O(F)\,.\end{gathered}$$

Idet $G \overset{\text{def}}{=\!=} \mathbb{C}[x_1, x_2]$, er $\mathcal{O}_O(\mathbb{A}^2_{\mathbb{C}}) = G_{\mathfrak{m}_O}$. Efter den næste kæde af ligheder følger begrundelse for hver enkelt af dem.

(5)
$$\begin{aligned}\mathcal{M}_O(F)^n &\overset{\text{(a)}}{=\!=} \big(\mathcal{M}_O(\mathbb{A}^2_{\mathbb{C}})/(f)\big)^n\\ &\overset{\text{(b)}}{=\!=} \big(\mathcal{M}_O(\mathbb{A}^2_{\mathbb{C}})^n + (f)\big)/(f)\\ &\overset{\text{(c)}}{=\!=} \big(((\mathfrak{m}_O)_{\mathfrak{m}_O})^n + (f)\big)/(f)\\ &\overset{\text{(d)}}{=\!=} \big((\mathfrak{m}_O{}^n)_{\mathfrak{m}_O} + (f)\big)/(f)\\ &\overset{\text{(e)}}{=\!=} \big((\mathfrak{m}_O{}^n)_{\mathfrak{m}_O} + (Gf)_{\mathfrak{m}_O}\big)/(Gf)_{\mathfrak{m}_O}\\ &\overset{\text{(f)}}{=\!=} (\mathfrak{m}_O{}^n + Gf)_{\mathfrak{m}_O}/(Gf)_{\mathfrak{m}_O}\,.\end{aligned}$$

(a) følger af definitionen af ($\mathcal{O}_O(F)$ og) $\mathcal{M}_O(F)$.
(b) følger af ROM 3.4(10).
(c) følger af definitionen af ($\mathcal{O}_O(\mathbb{A}^2_{\mathbb{C}})$ og) $\mathcal{M}_O(\mathbb{A}^2_{\mathbb{C}})$.
(d) følger af ROM 3.4(8).
(e) følger af: $(f) = \mathcal{O}_O(\mathbb{A}^2_{\mathbb{C}})f = G_{\mathfrak{m}_O}f = (Gf)_{\mathfrak{m}_O}$.
(f) ved inspektion.

Nu følger en kæde af isomorfier af vektorrum over $\mathbb{C}$ efterfulgt af begrundelser.

(6)
$$\begin{aligned}\mathcal{M}_O(F)^n/\mathcal{M}_O(F)^{n+1} &\overset{\text{(g)}}{=\!=} \big((\mathfrak{m}_O{}^n + Gf)_{\mathfrak{m}_O}/(Gf)_{\mathfrak{m}_O}\big)/\big((\mathfrak{m}_O{}^{n+1} + Gf)_{\mathfrak{m}_O}/(Gf)_{\mathfrak{m}_O}\big)\\ &\overset{\text{(h)}}{\cong} (\mathfrak{m}_O{}^n + Gf)_{\mathfrak{m}_O}/(\mathfrak{m}_O{}^{n+1} + Gf)_{\mathfrak{m}_O}\\ &\overset{\text{(i)}}{\cong} \big((\mathfrak{m}_O{}^n + Gf)/(\mathfrak{m}_O{}^{n+1} + Gf)\big)_{\mathfrak{m}_O}\\ &\overset{\text{(j)}}{\cong} (\mathfrak{m}_O{}^n + Gf)/(\mathfrak{m}_O{}^{n+1} + Gf)\,.\end{aligned}$$

(g) følger af 5(5).
(h) følger af Restklassemodullemmaets isomorfi ROM 2.2(6).
(i) følger af Brøkmodullemmaets isomorfi ROM 3.4(2).
(j) følger af isomorfien ROM 3.7(6).

Ifølge 5(3)(4)(6) er det nu tilstrækkeligt at bevise:

$$\text{(1)} \qquad \dim\big((\mathfrak{m}_O{}^n + Gf)/(\mathfrak{m}_O{}^{n+1} + Gf)\big) = \mathrm{m}_O(F) \quad \text{for} \quad n \geq \mathrm{m}_O(F)\,.$$

Sæt $m \overset{\text{def}}{=\!=} \mathrm{m}_O(F)$, dvs. $m = \operatorname{ord} f$ ifølge definitionen af multiplicitet. For $g \in G$ og $n \in \mathbb{N}_0$ har vi fra ROM 1.2(4) (sml. også ROM 1.6(2)), at

$$g \in \mathfrak{m}_O{}^n \quad \Longleftrightarrow \quad \operatorname{ord} g \geq n\,.$$

Da $\operatorname{ord}(gf) = \operatorname{ord} g + m$, fås heraf for $n \geq m$, at

$$\text{(2)} \qquad gf \in \mathfrak{m}_O{}^n \quad \Longleftrightarrow \quad g \in \mathfrak{m}_O{}^{n-m}\,.$$

For $n \geq m$ viser implikationen "$\Leftarrow$" i (2), at en afbildning $\varphi\colon G/\mathfrak{m}_O{}^{n-m} \longrightarrow G/\mathfrak{m}_O{}^n$ defineres korrekt ved $\varphi([g]_{\mathfrak{m}_O{}^{n-m}}) = [gf]_{\mathfrak{m}_O{}^n}$; den er oplagt en G–homomorfi, og den er injektiv pga. implikationen "$\Rightarrow$" i (2). Endvidere er $\operatorname{Im}\varphi = (\mathfrak{m}_O{}^n + Gf)/\mathfrak{m}_O{}^n$.

En afbildning $\psi\colon G/\mathfrak{m}_O{}^n \longrightarrow G/(\mathfrak{m}_O{}^n + Gf)$ er korrekt defineret ved $\psi([g]_{\mathfrak{m}_O{}^n}) = [g]_{\mathfrak{m}_O{}^n + Gf}$, da $\mathfrak{m}_O{}^n \subseteq \mathfrak{m}_O{}^n + Gf$. Dette er en G–homomorfi, som er surjektiv med $\operatorname{Ker}\psi = (\mathfrak{m}_O{}^n + Gf)/\mathfrak{m}_O{}^n$.

I alt er der for $n \geq m$ etableret en exakt følge af G–homomorfier:

$$\text{(3)} \qquad 0 \longrightarrow G/\mathfrak{m}_O{}^{n-m} \xrightarrow{\varphi} G/\mathfrak{m}_O{}^n \xrightarrow{\psi} G/(\mathfrak{m}_O{}^n + Gf) \longrightarrow 0\,.$$

Denne følge skal benyttes til at udregne $\dim\big(G/(\mathfrak{m}_O{}^n + Gf)\big)$. Først bemærkes, at der gælder:

$$\text{(4)} \qquad \dim(G/\mathfrak{m}_O{}^n) = \binom{n+1}{2} \quad \text{for alle} \quad n \geq 0\,.$$

Elementerne $[x_1^i x_2^j]_{\mathfrak{m}_O{}^n}$ med $i + j < n$ udgør nemlig en basis for vektorrummet $G/\mathfrak{m}_O{}^n$, og antallet af par $(i, j) \in \mathbb{N}_0 \times \mathbb{N}_0$ med $i + j < n$ er netop $\binom{n+1}{2}$.

$$\text{(5)} \qquad \begin{aligned} \dim\big(G/(\mathfrak{m}_O{}^n + Gf)\big) &\overset{\text{(k)}}{=\!=} \dim(G/\mathfrak{m}_O{}^n) - \dim(G/\mathfrak{m}_O{}^{n-m}) \\ &\overset{\text{(m)}}{=\!=} \binom{n+1}{2} - \binom{n-m+1}{2} \\ &\overset{\text{(n)}}{=\!=} mn - \binom{m}{2}\,. \end{aligned}$$

(k) ifølge den udvidede dimensionssætning ROM 2.5(3) anvendt på den exakte følge (3).
(m) følger af (4).
(n) følger ved direkte udregning.

Betragt følgen

(1) $\quad 0 \to (\mathfrak{m}_O{}^n + Gf)/(\mathfrak{m}_O{}^{n+1} + Gf) \xhookrightarrow{\iota} G/(\mathfrak{m}_O{}^{n+1} + Gf) \xrightarrow{\pi} G/(\mathfrak{m}_O{}^n + Gf) \to 0$

med inklusionshomomorfien ι og homomorfien π er defineret ved $\pi([g]_{\mathfrak{m}_O{}^{n+1}+Gf}) = [g]_{\mathfrak{m}_O{}^n+Gf}$ (og denne definition er korrekt, da $\mathfrak{m}_O{}^{n+1} + Gf \subseteq \mathfrak{m}_O{}^n + Gf$). Det er klart, at π er surjektiv, og at $\operatorname{Ker}\pi = (\mathfrak{m}_O{}^n + Gf)/(\mathfrak{m}_O{}^{n+1} + Gf)$. Følgen (1) er således exakt.

Den ønskede formel 6(1) følger nu:

$$\begin{aligned}\dim\big((\mathfrak{m}_O{}^n + Gf)/(\mathfrak{m}_O{}^{n+1} + Gf)\big) &\overset{\text{(p)}}{=} \dim\big(G/(\mathfrak{m}_O{}^{n+1} + Gf)\big) - \dim\big(G/(\mathfrak{m}_O{}^n + Gf)\big)\\ &\overset{\text{(q)}}{=} m(n+1) - \binom{m}{2} - mn + \binom{m}{2}\\ &\overset{\text{(r)}}{=} m\,.\end{aligned}$$

(p) ifølge Den udvidede Dimensionssætning ROM 2.5(3) anvendt på den exakte følge (1).
(q) følger af 6(5).
(r) følger ved udregning. □

(2) **Regulære punkter.** For punkt P og affin eller projektiv kurve C defineres:

$$P \text{ er et } \textit{regulært punkt på } C \quad \overset{\text{def}}{\iff} \quad \mathrm{m}_P(C) = 1\,;$$

altså netop hvis der – talt med multiplicitet – er netop én tangent til C i P (og dette medfører, at P ligger på C). Når P er et regulært punkt på C, siger man også, at P er *ikke–singulært på* C, og at C er *glat i* P.

For projektivt punkt P, projektiv kurve C og projektivt koordinatskift $\alpha\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ gælder ifølge 5.6(1), at

$$P \text{ er et regulært punkt på } C \quad \iff \quad \alpha(P) \text{ er et regulært punkt på } C_\alpha\,.$$

I eksempel 5.4(4) er U et regulært punkt på kurven A, og i 5.4(5) er punkterne P og Q regulære på kurven B.

(3) **Bemærkning.** Hvis P er et regulært punkt på C, da har C netop én komponent gennem P, sml. den næste opgave.

(4) **Opgave.** Bevis, at hvis en projektiv kurve $C = (c)$ består af to komponenter D og E, dvs. projektive kurver $D = (d)$ og $E = (e)$ med $(c) = (de)$, da gælder $\mathrm{m}_P(C) = \mathrm{m}_P(D) + \mathrm{m}_P(E)$ for ethvert $P \in \mathbb{P}^2_{\mathbb{C}}$. (Udnyt f.eks. 5.6(1) for passende α.)

(5) **Partielle afledede.** Ethvert $f \in \mathbb{C}[x_1, x_2]$ har to partielle afledede:

$$f'_1 \overset{\text{def}}{=} \frac{\partial f}{\partial x_1} \quad \text{og} \quad f'_2 \overset{\text{def}}{=} \frac{\partial f}{\partial x_2}\,.$$

(6) **Lemma.** *Hvis begyndelsespunktet O tilhører den affine kurve $G = (g)$, da gælder*

$$O \text{ er regulært på } G \quad \iff \quad g'_1(O) \neq 0 \;\vee\; g'_2(O) \neq 0\,;$$

og i bekræftende fald er tangenten til G i O netop linien $(g'_1(O)x_1 + g'_2(O)x_2)$.

(7) *Bevis.* Antag, at $g = a_{10}x_1 + a_{01}x_2 + \sum_{i+j\geq 2} a_{ij}x_1^i x_2^j$; der er intet konstantled, da $g(O) = 0$ ifølge forudsætning. Der gælder $\mathrm{m}_O(G) = 1$, netop hvis $a_{10} \neq 0$ eller $a_{01} \neq 0$, og i bekæftende fald er tangenten til G i O netop $(a_{10}x_1 + a_{01}x_2)$. Tilbage er blot at bemærke, at $g'_1(O) = a_{10}$ og $g'_2(O) = a_{01}$. □

(1) **Regularitetssætningen.** *Følgende er ensbetydende for punkt $P = (a_1, a_2)$ på affin kurve $F = (f)$.*

(*i*) *P er regulært på F.*
(*ii*) *$f'_1(P) \neq 0$ eller $f'_2(P) \neq 0$.*
(*iii*) *$\mathcal{O}_P(F)$ er en DVR.*

I bekræftende fald er tangenten til F i P netop $\big(f'_1(P)(x_1 - a_1) + f'_2(P)(x_2 - a_2)\big)$.

(2) *Bevis.* "(*i*) $\Leftrightarrow$ (*ii*)": Ved $\underline{\varphi}(\underline{x}) \stackrel{\text{def}}{=} (x_1 - a_1x_3, x_2 - a_2x_3, x_3)$ defineres en lineær afbildning $\underline{\varphi}\colon \mathbb{C}^3 \to \mathbb{C}^3$, der er bijektiv med $\underline{\varphi}^{-1}(\underline{x}) \stackrel{\text{def}}{=} (x_1 + a_1x_3, x_2 + a_2x_3, x_3)$. Det inducerede projektive koordinatskift $\alpha \stackrel{\text{def}}{=} \underline{\underline{\varphi}}$ har $\alpha(P) = O$ og sender den projektive kurve $C \stackrel{\text{def}}{=} (f^*)$ over i kurven C_α, hvis affine del $G \stackrel{\text{def}}{=} (C_\alpha)_*$ er givet ved polynomiet $g \stackrel{\text{def}}{=} f(x_1 + a_1, x_2 + a_2)$. Der gælder $g'_1(O) = f'_1(P)$, $g'_2(O) = f'_2(P)$ og $\mathrm{m}_O(G) = \mathrm{m}_P(F)$, så "(*i*) $\Leftrightarrow$ (*ii*)" følger af 7(6). Idet $L = \big(f'_1(P)(x_1 - a_1x_3) + f'_2(P)(x_2 - a_2x_3)\big)$, er den affine del af L_α givet ved polynomiet $g'_1(O)x_1 + g'_2(O)x_2$, så 7(6) giver også påstanden om tangenten.

"(*i*) $\Rightarrow$ (*iii*)": Ifølge 7(3) har F netop én komponent gennem P, så ifølge 2(1) kan vi gerne antage, at polynomiet f er irreducibelt og derfor frembringer et primideal i $\mathbb{C}[x_1, x_2]$, sml. 3.4(10). Da $\mathbb{C}[x_1, x_2]/(f)$ således er et integritetsområde, viser 2(2) og ROM 3.3(4), at $\mathcal{O}_P(F)$ er det samme. Da $\dim\big(\mathcal{M}_P(F)/\mathcal{M}_P(F)^2\big) = 1$ ifølge Multiplicitetssætningen 5(1), er $\mathcal{M}_P(F)/\mathcal{M}_P(F)^2$ frembragt af ét element som $\mathbb{C}$–vektorrum – og dermed også som $\mathcal{O}_P(F)$–modul; der findes altså et $t \in \mathcal{M}_P(F)$, så

$$\mathcal{M}_P(F)/\mathcal{M}_P(F)^2 = \mathcal{O}_P(F)[t]_{\mathcal{M}_P(F)^2} = \big((t) + \mathcal{M}_P(F)^2\big)/\mathcal{M}_P(F)^2\,,$$

og dermed $\mathcal{M}_P(F) = (t) + \mathcal{M}_P(F)^2$. Ifølge Nakayama's Korollar ROM 4.4(8) (med $M = \mathcal{M}_P(F)$, $N = (t)$ og $\mathcal{M} = \mathcal{M}_P(F)$) medfører dette, at $\mathcal{M}_P(F) = (t)$, og ROM 4.5(6) giver, at $\mathcal{O}_P(F)$ er DVR.

"(*iii*) $\Rightarrow$ (*i*)": Vælg $t \in \mathcal{M}_P(F)$, så $\mathcal{M}_P(F) = (t)$, og dermed $\mathcal{M}_P(F)^n = (t^n)$ for alle $n \in \mathbb{N}_0$. Dette medfører, at:

$$\mathcal{M}_P(F)^n/\mathcal{M}_P(F)^{n+1} = \big((t^n) + \mathcal{M}_P(F)^{n+1}\big)/\mathcal{M}_P(F)^{n+1}\,,$$

som er frembragt af elementet $[t^n]_{\mathcal{M}_P(F)^{n+1}}$ som $\mathcal{O}_P(F)$–modul – og dermed også som vektorrum over $\mathcal{O}_P(F)/\mathcal{M}_P(F)$, sml. opgave ROM 2.6(2), og dermed som $\mathbb{C}$–vektorrum ifølge opgave (3) nedenfor, dvs. $\dim\big(\mathcal{M}_P(F)^n/\mathcal{M}_P(F)^{n+1}\big) = 1$. Multiplicitetssætningen 5(1) giver nu $\mathrm{m}_P(F) = 1$ som ønsket. $\square$

(3) **Opgave.** Bevis, at $\mathcal{O}_P(F)/\mathcal{M}_P(F) \cong \mathbb{C}$, når P er et punkt på den affine kurve F.

(4) **Sætningen om implicit given funktion** (kendt fra Matematik 1) medfører, at en kurve i en omegn af et regulært punkt er givet som grafen af den ene variabel (dvs. x_1 eller x_2) som C^∞–funktion af den anden, og Regularitetssætningen (1) ovenfor viser, at kurvens (Matematik 3AG)–tangent i punktet er netop denne grafs (Matematik 1)–tangent i punktet.

(5) **Linier.** Ethvert punkt på en projektiv linie er regulært.

(1) **Kvadrikker.** For enhver *kvadrik* $K = (k)$ i $\mathbb{P}^2_{\mathbb{C}}$ (dvs. $\deg K = 2$) gælder:

$$K \text{ er reducibel} \iff \exists P \in \mathrm{W}(K)\colon P \text{ er ikke regulært på } K\,.$$

"$\Rightarrow$": Antag $k = \ell m$ med ℓ og m lineære. For $P \in \mathrm{W}(\ell) \cap \mathrm{W}(m)$, der ikke er tom, sml. evt. 1.2(3), er P ikke–regulært punkt på K ifølge 7(3).

"$\Leftarrow$": Bemærk først, at vi gerne kan antage, at O er et ikke–regulært punkt på K, og dermed $\operatorname{ord} k_* = \mathrm{m}_O(K) \geq 2$, dvs. $k_* = a_{20}x_1^2 + a_{11}x_1x_2 + a_{02}x_2^2$. Da således $k = k_*$ er et homogent polynomium af to variable, giver 3.3(5), at det er produkt af lineære polynomier og dermed reducibelt.

(2) **Eksempel.** Lad $p \in \mathbb{C}[x_1]$ være et polynomium (af én variabel) og grad 3, sæt $f \overset{\text{def}}{=\!=} x_2^2 - p \in \mathbb{C}[x_1, x_2]$, og betragt den affine kurve $F \overset{\text{def}}{=\!=} (f)$. Da $f_2' = 2x_2$, er alle $(a_1, a_2) \in \mathrm{V}(F)$ med $a_2 \neq 0$ regulære på F. For $P = (a, 0)$ gælder $P \in \mathrm{V}(F)$, netop hvis $p(a) = 0$; og da $f_1'(P) = -p'(a)$, er P regulært på F, netop hvis a ikke er multipel rod i p. Hvis således p er uden multiple rødder, da er alle punkter på kurven F regulære. I alle tilfælde har kurver af denne type højst ét ikke-regulært punkt.

(3) **Opgave.** Lad f være som i (2) ovenfor. Bevis, at punktet $(0:1:0)$ er regulært på den projektive kurve (f^*). (Udnyt f.eks. passende projektivt koordinatskift.)

(4) **Opgave.** Bestem samtlige ikke–regulære punkter på de projektive kurver (a^*), (b^*), (c^*), (d^*), (e^*) og (f^*) givet ved:

$$\begin{aligned} a &\overset{\text{def}}{=\!=} x_2^2 - (x_1+1)x_1(x_1-1)\,; & b &\overset{\text{def}}{=\!=} x_2^2 - (x_1+1)x_1^2\,; \\ c &\overset{\text{def}}{=\!=} x_1^3 + x_2^3\,; & d &\overset{\text{def}}{=\!=} x_2 - (x_1+1)x_1(x_1-1)\,; \\ e &\overset{\text{def}}{=\!=} (x_1+1)x_1(x_1-1)\,; & f &\overset{\text{def}}{=\!=} (x_1+1)x_2(x_1-1)\,. \end{aligned}$$

(Punkterne på $\mathcal{L}_\infty$ kræver speciel opmærksomhed!)

Mon en projektiv trediegradskurve kan have netop to ikke-regulære punkter?

(5) **Opgave.** Lad P være et punkt på en irreducibel projektiv trediegradskurve C. Bevis, at $\mathrm{m}_P(C) \leq 2$.

(6) **Stilopgave.** *Multiplicitetssætningen.*

(a) Formulér Multiplicitetssætningen.

(b) Bevis Multiplicitetssætningen. De enkelte trin i beviset bør fremstå klart. Hvis der undervejs udnyttes resultater, der har et specielt navn, da ønskes dette benyttet ved henvisning; resultater uden specielt navn kan blot udnyttes uden henvisning; de udnyttede resultater skal således ikke formuleres.

(7) **Stilopgave.** *DVR og regulære punkter.*

(a) Angiv definitionen af begrebet "DVR".

(b) Formulér et interessant resultat, der viser, at visse lokale ringe er DVR, og giv et bevis for dette resultat. Hvis Nakayama's Lemma udnyttes, ønskes det formuleret (men ikke bevist). De enkelte dele af beviset bør fremstå klart.

(c) Angiv definitionen af regularitet af et punkt på en kurve.

(d) Formulér og bevis Regularitetssætningen. Hvis der i beviset udnyttes et resultat om regulariteten af begyndelsespunktet, da ønskes dette resultat såvel formuleret som bevist. Hvis Nakayama's Korollar udnyttes, ønskes det formuleret (men ikke bevist). De enkelte dele af beviset bør fremstå klart.

7. SNITMULTIPLICITETER

(1) **Snitmultiplicitet.**

$\mathrm{m}_P(f \bullet g) \overset{\text{def}}{=\!=} \dim \mathcal{O}_P(f \bullet g)$ for $P \in \mathbb{A}^2_{\mathbb{C}}$ og $f, g \in \mathbb{C}[x_1, x_2]$ (sml. evt. ROM 5.1(4));
$\mathrm{m}_P(F \bullet G) \overset{\text{def}}{=\!=} \mathrm{m}_P(f \bullet g)$ for $P \in \mathbb{A}^2_{\mathbb{C}}$ og affine kurver $F = (f)$ og $G = (g)$; og
$\mathrm{m}_P(C \bullet D) \overset{\text{def}}{=\!=} \dim \mathcal{O}_P(C \bullet D)$ for $P \in \mathbb{P}^2_{\mathbb{C}}$ og projektive kurver C og D, idet
$\mathcal{O}_P(C \bullet D) \overset{\text{def}}{=\!=} \mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}}) / \big(\mathcal{I}_P(C) + \mathcal{I}_P(D)\big)$.

(2) **Benævnelser.** Det næste resultat indeholder vigtige egenskaber ved snitmultipliciteter. Disse egenskaber benævnes med udvalgte stikord, og der henvises ofte blot til stikordets begyndelsesbogstav (eller lignende) i parentes og uden sidetal, men skrevet med **fed** type.

(3) **Snitmultiplicitetssætningen.** *For $P \in \mathbb{P}^2_{\mathbb{C}}$ og projektive kurver C og D gælder* **(B)**, **(D)**, **(V)**, **(P)**, **(E)**, **(F)** *og* **(R)** *nedenfor.*

(B) Begyndelsespunkt. *Lad $\alpha \colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ være projektivt koordinatskift, f.eks. et, der fører punktet P over i begyndelsespunktet O. Der gælder da:*

$$\mathrm{m}_P(C \bullet D) = \mathrm{m}_{\alpha(P)}(C_\alpha \bullet D_\alpha)\,.$$

(D) Dehomogenisering. *For $P \in \mathbb{A}^2_{\mathbb{C}}$ gælder:*

$$\mathrm{m}_P(C \bullet D) = \mathrm{m}_P(C_* \bullet D_*)\,.$$

(V) Værdier.

$$0 \le \mathrm{m}_P(C \bullet D) \le \infty\,.$$

(P) Positivitet.

$$0 < \mathrm{m}_P(C \bullet D) \iff P \ \textit{ligger på både}\ C \ \textit{og}\ D\,.$$

(E) Endelighed.

$$\mathrm{m}_P(C \bullet D) < \infty \iff C \ \textit{og}\ D \ \textit{er uden fælles komponent gennem}\ P\,.$$

(F) Fælles tangent.

$$\mathrm{m}_P(C \bullet D) \ge \mathrm{m}_P(C)\,\mathrm{m}_P(D)\,;$$
$$\mathrm{m}_P(C \bullet D) = \mathrm{m}_P(C)\,\mathrm{m}_P(D) \iff C \ \textit{og}\ D \ \textit{er uden fælles tangent i}\ P\,.$$

(R) Regulære punkter.

$$\mathrm{m}_P(C \bullet D) = 1 \iff \begin{cases} P \ \textit{er regulært på både}\ C \ \textit{og}\ D\,,\ \textit{og} \\ C \ \textit{og}\ D \ \textit{er uden fælles tangent i}\ P\,. \end{cases}$$

For $P \in \mathbb{A}^2_{\mathbb{C}}$ og $f, g \in \mathbb{C}[x_1, x_2]$ gælder **(Q)**, **(I)**, **(S)**, **(M)**, **(K)**, **(A)** *og* **(O)** *nedenfor.*

(Q) Positivitet, affint tilfælde.

$$0 < \mathrm{m}_P(f \centerdot g) \quad \Longleftrightarrow \quad f(P) = 0 \quad \wedge \quad g(P) = 0 \,.$$

(I) Idealet. *Tallet $\mathrm{m}_P(f \centerdot g)$ afhænger kun af idealet $\mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})(f, g)$:*
Hvis $\mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})(f, g) = \mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})(h, k)$ med $h, k \in \mathbb{C}[x_1, x_2]$, da gælder:

$$\mathrm{m}_P(f \centerdot g) = \mathrm{m}_P(h \centerdot k) \,.$$

(S) Symmetri.

$$\mathrm{m}_P(f \centerdot g) = \mathrm{m}_P(g \centerdot f) \,.$$

(M) Modulo. *Tallet $\mathrm{m}_P(f \centerdot g)$ afhænger kun af restklassen $[f]_{(g)}$ af f modulo (g), henholdsvis restklassen $[g]_{(f)}$ af g modulo (f):*
For $h \in \mathbb{C}[x_1, x_2]$ gælder:

$$\mathrm{m}_P(f \centerdot g) = \mathrm{m}_P(f + hg \centerdot g) \,, \ \textit{henholdsvis} \ \ \mathrm{m}_P(f \centerdot g) = \mathrm{m}_P(f \centerdot g + hf) \,.$$

(K) Komponenter. *Tallet $\mathrm{m}_P(f \centerdot g)$ afhænger kun af komponenter gennem P:*
Hvis $f = ab$ og $g = cd$ med $a, b, c, d \in \mathbb{C}[x_1, x_2]$, $b(P) \neq 0$ og $d(P) \neq 0$, da gælder:

$$\mathrm{m}_P(f \centerdot g) = \mathrm{m}_P(a \centerdot c) \,.$$

(A) Additivitet. *For $h \in \mathbb{C}[x_1, x_2]$ gælder:*

$$\mathrm{m}_P(f \centerdot gh) = \mathrm{m}_P(f \centerdot g) + \mathrm{m}_P(f \centerdot h) \quad \textit{og} \quad \mathrm{m}_P(fh \centerdot g) = \mathrm{m}_P(f \centerdot g) + \mathrm{m}_P(h \centerdot g) \,.$$

(O) Orden. *For $u \in \mathbb{C}[x_1]$ og $w \in \mathbb{C}[x_2]$ gælder:*

$$\begin{aligned} \mathrm{m}_O(f \centerdot u) &= \big(\operatorname{ord} f(0, x_2)\big)\big(\operatorname{ord} u\big) \,, \quad & \mathrm{m}_O(f \centerdot w) &= \big(\operatorname{ord} f(x_1, 0)\big)\big(\operatorname{ord} w\big) \,, \\ \mathrm{m}_O(u \centerdot g) &= \big(\operatorname{ord} u\big)\big(\operatorname{ord} g(0, x_2)\big) \,, \quad & \mathrm{m}_O(w \centerdot g) &= \big(\operatorname{ord} w\big)\big(\operatorname{ord} g(x_1, 0)\big) \,. \end{aligned}$$

(1) **Kommentar.** Før beviset for Snitmultiplicitetssætningen bringes et resultat om udregning af snitmultipliciteter, et eksempel og to lemmaer.

(2) **Udregning.** Snitmultipliciteten $\mathrm{m}_P(C \centerdot D)$ kan altid udregnes:
Vælg først projektivt koordinatskift α med $\alpha(P) = O$, og udnyt (B).
Dehomogenisér dernæst, og udnyt (D).
Herefter er det $\mathrm{m}_O(f \centerdot g)$, der skal bestemmes for $f, g \in \mathbb{C}[x_1, x_2]$.
Hvis $f \in \mathbb{C}[x_1]$ (svarende til $\deg_2 f = 0$ – med notation fra 4.1(6) – eller $f = 0$), da kendes $\mathrm{m}_O(f \centerdot g)$ fra (O). Tilsvarende for $f \in \mathbb{C}[x_2]$, $g \in \mathbb{C}[x_1]$ eller $g \in \mathbb{C}[x_2]$.
Endelig kan x_2–graden (eller x_1–graden) af et af polynomierne f eller g reduceres:
Antag f.eks. $d \overset{\text{def}}{=\!=} \deg_2 f \geq e \overset{\text{def}}{=\!=} \deg_2 g$:

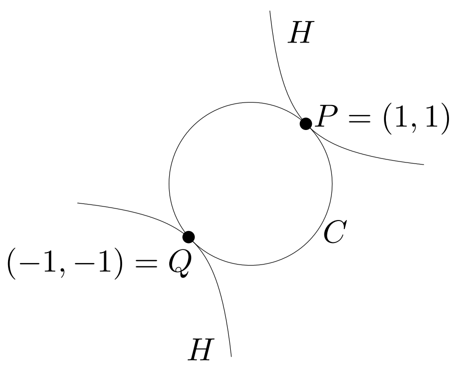
$$\begin{aligned} f &= a_d x_2^d + \cdots + a_1 x_2 + a_0 \quad \text{med} \quad a_d, \ldots, a_1, a_0 \in \mathbb{C}[x_1] \quad \text{og} \quad a_d \neq 0 \,; \\ g &= b_e x_2^e + \cdots + b_1 x_2 + b_0 \quad \text{med} \quad b_e, \ldots, b_1, b_0 \in \mathbb{C}[x_1] \quad \text{og} \quad b_e \neq 0 \,. \end{aligned}$$

Sæt $h \overset{\text{def}}{=\!=} b_e f - a_d x_2^{d-e} g$, og bemærk, at:

$$\begin{aligned} \mathrm{m}_O(f \bullet g) &\overset{\textbf{(A)}}{=\!=} \mathrm{m}_O(b_e f \bullet g) - \mathrm{m}_O(b_e \bullet g) \\ &\overset{\textbf{(M)}}{=\!=} \mathrm{m}_O(h \bullet g) - \mathrm{m}_O(b_e \bullet g) \\ &\overset{\textbf{(O)}}{=\!=} \mathrm{m}_O(h \bullet g) - \big(\operatorname{ord} b_e\big)\big(\operatorname{ord} g(0, x_2)\big) , \end{aligned}$$

samt at $\deg_2 h < d = \deg_2 f$.

(1) **Eksempel.** Betragt de affine punkter $P \overset{\text{def}}{=\!=} (1,1)$ og $Q \overset{\text{def}}{=\!=} (-1,-1) \in \mathbb{A}^2_{\mathbb{C}}$, der ligger på cirklen $C \overset{\text{def}}{=\!=} (x_1^2 + x_2^2 - 2x_3^2)$ og på hyperbelen $H \overset{\text{def}}{=\!=} (x_1 x_2 - x_3^2)$:



Vi udregner nu $\mathrm{m}_P(C \bullet H)$ med henvisninger til Snitmultiplicitetssætningen og udnyttelse af det projektive koordinatskift α givet ved $\alpha(x_1 : x_2 : x_3) \overset{\text{def}}{=\!=} (x_1 - x_3 : x_2 - x_3 : x_3)$, og som har $\alpha^{-1}(x_1 : x_2 : x_3) = (x_1 + x_3 : x_2 + x_3 : x_3)$.

$$\begin{aligned} \mathrm{m}_P(C \bullet H) &= \mathrm{m}_P((x_1^2 + x_2^2 - 2x_3^2) \bullet (x_1 x_2 - x_3^2)) \\ &\overset{\textbf{(B)}}{=\!=} \mathrm{m}_O\big(\big((x_1+x_3)^2 + (x_2+x_3)^2 - 2x_3^2\big) \bullet \big((x_1+x_3)(x_2+x_3) - x_3^2\big)\big) \\ &\overset{\textbf{(D)}}{=\!=} \mathrm{m}_O((x_1+1)^2 + (x_2+1)^2 - 2 \bullet (x_1+1)(x_2+1) - 1) \\ &= \mathrm{m}_O(x_1^2 + 2x_1 + x_2^2 + 2x_2 \bullet x_1 x_2 + x_1 + x_2) \\ &\overset{\textbf{(M)}}{=\!=} \mathrm{m}_O(x_1^2 + 2x_1 + x_2^2 + 2x_2 - 2(x_1 x_2 + x_1 + x_2) \bullet x_1 x_2 + x_1 + x_2) \\ &= \mathrm{m}_O((x_1 - x_2)^2 \bullet x_1 x_2 + x_1 + x_2) \\ &\overset{\textbf{(A)}}{=\!=} 2\,\mathrm{m}_O(x_1 - x_2 \bullet x_1 x_2 + x_1 + x_2) \\ &\overset{\textbf{(R)}}{=\!=} 2 \cdot 1 \\ &= 2 . \end{aligned}$$

Til næstsidste lighed blev brugt, at O er regulært på både (x_1-x_2) og $(x_1x_2+x_1+x_2)$ med tangent henholdsvis (x_1-x_2) og (x_1+x_2), og disse er forskellige. Den i 2(2) skitserede algoritme kunne også have været benyttet her. Hovedformålet med at præsentere denne algoritme er dog blot at vise, at udregning af snitmultipliciteter altid er mulig. Til praktiske formål er der ofte genveje – specielt ved udnyttelse af Bezout's Sætning i næste afsnit.

(1) **Lemma.** *Sæt* $G \overset{\text{def}}{=\!=} \mathbb{C}[x_1, x_2]$, *antag* $P \in \mathbb{A}^2_{\mathbb{C}}$ *og* $f \in \mathfrak{m}_P$ $(\in \operatorname{Max} G)$, *og sæt* $A \overset{\text{def}}{=\!=} G/G(f)$, $\mathfrak{m}_P{}' \overset{\text{def}}{=\!=} \mathfrak{m}_P/G(f)$ *og* $B \overset{\text{def}}{=\!=} \mathcal{O}_P(f)$. *For ethvert* $g \in G$ *er der da isomorfier af* $\mathbb{C}$*–vektorrum:*

$$\mathcal{O}_P(f \bullet g) \cong (A/gA)_{\mathfrak{m}_P{}'} \cong B/gB\,.$$

(Her er A og B også G–moduler, og $gA \overset{\text{def}}{=\!=} \{\, ga \mid a \in A \,\}$ og $gB \overset{\text{def}}{=\!=} \{\, gb \mid b \in B \,\}$ er idealer i henholdsvis A og B.)

(2) *Bevis.* Sæt $Q \overset{\text{def}}{=\!=} \mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}}) = G_{\mathfrak{m}_P}$, der er en G–modul, og bemærk, at $B = Q/Q(f) = Q/fQ$, samt at $gB = (fQ+gQ)/fQ$, som er et ideal i B. Vi har:

$$\begin{aligned}\mathcal{O}_P(f \bullet g) = Q/Q(f,g) \qquad\qquad & = Q/(fQ+gQ)\\ \cong \big(Q/fQ\big)/\big((fQ+gQ)/fQ\big) & = B/gB\\ \cong A_{\mathfrak{m}_P{}'}/gA_{\mathfrak{m}_P{}'} \qquad\qquad & \cong (A/gA)_{\mathfrak{m}_P{}'}\,.\end{aligned}$$

Her kommer første isomorfi fra Restklassemodullemmaet, den anden er induceret af isomorfien 6.2(2) $B \cong A_{\mathfrak{m}_P{}'}$, mens den sidste er fra Brøkmodullemmaet. □

(3) **Lemma.** *Hvis* $f, g \in G \overset{\text{def}}{=\!=} \mathbb{C}[x_1, x_2]$ *er primiske, dvs. uden fælles komponenter, da gælder der for alle* $h \in G$, *at:*

$$gh \in G(f) \quad \Rightarrow \quad h \in G(f)\,.$$

(4) *Bevis.* Antag, at $gh = kf$ for et $k \in G$. Da G er UFD, kan f og g skrives som produkt af primfaktorer: der findes $u, v \in \mathbb{N}_0$, $a_1, \ldots, a_u; b_1, \ldots, b_v \in \mathbb{N}$ og irreducible $p_1, \ldots, p_u; q_1, \ldots, q_v \in G$, så $f = p_1^{a_1} \cdots p_u^{a_u}$ og $g = q_1^{b_1} \cdots q_v^{b_v}$. Da f og g er uden fælles komponent, gælder $(p_i) \neq (q_j)$ for alle i og j. Ligningen $q_1^{b_1} \cdots q_v^{b_v} h = kp_1^{a_1} \cdots p_u^{a_u}$ giver (på grund af entydigheden af primfaktorfremstillinger), at primfaktorpotenserne i f går op i h, og dermed går f op i h – som ønsket. □

(5) *Bevis for Snitmultiplicitetssætningen* 1(3). Vælg $c, d \in \mathbb{C}[x_1, x_2, x_3]$ med $C = (c)$ og $D = (d)$.

(B): Isomorfien $\widetilde{\alpha}\colon \mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}}) \to \mathcal{O}_{\alpha(P)}(\mathbb{P}^2_{\mathbb{C}})$ fra 6.4(4) afbilder idealet $\mathcal{I}_P(C) + \mathcal{I}_P(D)$ på $\mathcal{I}_{\alpha(P)}(C_\alpha) + \mathcal{I}_{\alpha(P)}(D_\alpha)$ og inducerer derfor en isomorfi $\mathcal{O}_P(C \bullet D) \cong \mathcal{O}_{\alpha(P)}(C_\alpha \bullet D_\alpha)$, hvilket giver det ønskede.

(D): Isomorfien $\upsilon\colon \mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}}) \to \mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})$ fra 6.3(3) afbilder idealet $\mathcal{I}_P(C) + \mathcal{I}_P(D)$ på $\mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})(c_*, d_*)$ og inducerer derfor en isomorfi $\mathcal{O}_P(C \bullet D) \cong \mathcal{O}_P(c_* \bullet d_*)$, hvilket giver det ønskede.

(V) er oplagt ifølge definitionen.

(P) følger af **(B)**, **(D)** og **(Q)**.

(Q) følger af:

$$\mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})(f,g) \subseteq \mathcal{M}_P(\mathbb{A}^2_{\mathbb{C}}) \quad \Longleftrightarrow \quad f(P)=0 \ \ \wedge \ \ g(P)=0\,.$$

(E) "$\Rightarrow$": Vi kan gerne antage $P=O$. Antag, at $H=(h)$ er en fælles komponent for C og D gennem O, og vi kan gerne antage, at H er irreducibel, og dermed $G(h_*) \in \operatorname{Spec} G$ for $G \overset{\text{def}}{=\!=} \mathbb{C}[x_1,x_2]$. Da $\mathcal{I}_O(C)+\mathcal{I}_O(D) \subseteq \mathcal{I}_O(H)$, har vi surjektiv ringhomomorfi $\mathcal{O}_O(C \bullet D) \to \mathcal{O}_O(H)$, og dermed

$$\text{(1)} \qquad \mathrm{m}_O(C \bullet D) = \dim \mathcal{O}_O(C \bullet D) = \dim \mathcal{O}_O(H)\,.$$

Vi har også

$$\mathcal{O}_O(H) \cong \mathcal{O}_O(H_*) = \mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})/\mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})(h_*) \supseteq G/G(h_*)\,,$$

og dermed:

$$\text{(2)} \qquad \dim \mathcal{O}_O(H) \geq \dim \big(G/G(h_*)\big)\,.$$

For alle $P \in \mathrm{V}(h_*)$ har vi $G(h_*) \subseteq \mathfrak{m}_P \in \operatorname{Max} G$, og dermed $\mathfrak{m}_P/G(h_*) \in \operatorname{Max} G/G(h_*)$, som derfor er uendelig ifølge 4.1(4), så ROM 5.4(6) giver $\dim\big(G/G(h_*)\big)=\infty$. Sammenholdes dette med (2) og (1), fås det ønskede.

(F)'s bevis udskydes til senere.

(R) følger let af bl.a. **(F)**.

(I) er oplagt udfra definitionen.

(S) og **(M)** følger direkte af **(I)**.

(K): Ifølge **(S)** er nok at bevise $\mathcal{O}_P(ab \bullet g) \cong \mathcal{O}_P(a \bullet g)$, når $b(P) \neq 0$. Da b således er invertibel i $Q \overset{\text{def}}{=\!=} \mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})$, har vi:

$$B \overset{\text{def}}{=\!=} \mathcal{O}_P(ab) = Q/abQ = Q/aQ = \mathcal{O}_P(a)\,,$$

og to anvendelser af 4(1) giver:

$$\mathcal{O}_P(ab \bullet g) \cong B/gB \cong \mathcal{O}_P(a \bullet g)\,.$$

(A): Ifølge **(S)** er det tilstrækkeligt, at bevise formlen:

$$\text{(3)} \qquad \mathrm{m}_P(f \bullet gh) = \mathrm{m}_P(f \bullet g) + \mathrm{m}_P(f \bullet h)$$

for $f,g,h \in G \overset{\text{def}}{=\!=} \mathbb{C}[x_1,x_2]$.

Ifølge **(K)** kan vi gerne antage, at samtlige primfaktorer i f, i g og i h tilhører $\mathfrak{m}_P$.

Vi kan yderligere gerne antage, at f og g er uden fælles komponenter, thi en sådan ville gå gennem P, og **(E)** "$\Rightarrow$" ville derfor give:

$$\mathrm{m}_P(f \bullet gh) = \infty = \infty + \mathrm{m}_P(f \bullet h) = \mathrm{m}_P(f \bullet g) + \mathrm{m}_P(f \bullet h)\,,$$

dvs. lighed i (3) gælder.

Ifølge 4(1) gælder:

$$\begin{aligned} \mathrm{m}_P(f \bullet g) &= \dim(A/gA)_{\mathfrak{m}_{P'}} \\ \mathrm{m}_P(f \bullet h) &= \dim(A/hA)_{\mathfrak{m}_{P'}} \\ \mathrm{m}_P(f \bullet gh) &= \dim(A/ghA)_{\mathfrak{m}_{P'}} \end{aligned}$$

med betegnelser fra 4(1). Ifølge Den udvidede Dimensionssætning ROM 2.5(3) er det derfor nok at bevise, at der er en exakt følge:

$$0 \to (A/hA)_{\mathfrak{m}_{P'}} \to (A/ghA)_{\mathfrak{m}_{P'}} \to (A/gA)_{\mathfrak{m}_{P'}} \to 0\,,$$

og dette gøres ved at udnytte ROM 3.4(5) og konstruere en exakt følge:

(1) $$0 \to A/hA \xrightarrow{\gamma} A/ghA \xrightarrow{\pi} A/gA \to 0\,.$$

γ gives ved $\gamma\big([a]_{hA}\big) \overset{\text{def}}{=\!=} [ga]_{ghA}$. Da der gælder $a \in hA \;\Rightarrow\; ga \in ghA$, er γ korrekt defineret. For at indse, at γ er injektiv, antag at $\gamma\big([a]_{hA}\big) = 0$, dvs. $ga \in ghA$, og dermed $ga = ghu$ for et $u \in A$. Vælg $p, q \in G$ med $a = [p]_{fG}$ og $u = [q]_{fG}$. Da $[gp]_{fG} = [ghq]_{fG}$, har vi $g(p - hq) \in fG$ $(= G(f)\,)$, og dermed $p - hq \in fG$ ifølge 4(3). Heraf følger $a = [p]_{fG} = [hq]_{fG} = hu \in hA$, og dermed $[a]_{hA} = 0$ som ønsket. Direkte af definitionen følger $\operatorname{Im}\gamma = gA/ghA$.

π gives ved $\pi\big([a]_{ghA}\big) \overset{\text{def}}{=\!=} [a]_{gA}$, og er korrekt defineret herved, da $ghA \subseteq gA$. Det er oplagt, at π er surjektiv med $\operatorname{Ker}\pi = gA/ghA$.

Den exakte følge (1) er nu etableret, og **(A)** er bevist.

(E) "$\Leftarrow$": Antag, at C og D er uden fælles komponent gennem P. Da $\mathrm{m}_P(C \bullet D)$ ifølge **(K)** ikke afhænger af komponenter, der ikke går gennem P, kan vi gerne antage, at C og D er helt uden fælles komponenter. Det ønskede følger nu af Bezout's sætning 8.1(6) i næste afsnit, og i beviset for denne benyttes ikke resultater, der hviler på **(E)**"$\Leftarrow$".

(O): Det er nok at bevise f.eks. $\mathrm{m}_O(f \bullet u) = mn$, når $m \overset{\text{def}}{=\!=} \operatorname{ord} f(0, x_2)$ og $n \overset{\text{def}}{=\!=} \operatorname{ord} u$. Bemærk, at $f - f(0, x_2) \in x_1 G$, vælg $v \in \mathbb{C}[x_2]$ og $w \in \mathbb{C}[x_1]$ med $f(0, x_2) = x_2^m v$ og $u = x_1^n w$, og bemærk $v(O) \neq 0$ og $w(O) \neq 0$. Vi har:

$$\begin{aligned} \mathrm{m}_O(f \bullet u) &\overset{\textbf{(K)}}{=\!=} \mathrm{m}_O(f \bullet x_1^n) \overset{\textbf{(A)}}{=\!=} n\,\mathrm{m}_O(f \bullet x_1) \overset{\textbf{(M)}}{=\!=} n\,\mathrm{m}_O(f(0, x_2) \bullet x_1) \\ &\overset{\textbf{(K)}}{=\!=} n\,\mathrm{m}_O(x_2^m \bullet x_1) \overset{\textbf{(F)}}{=\!=} n(m \cdot 1) = mn\,. \quad \square \end{aligned}$$

(2) **Opgave.** Bestem multipliciteterne $\mathrm{m}_{(0,0)}(f \bullet g)$, $\mathrm{m}_{(1,1)}(f \bullet g)$ og $\mathrm{m}_{(0:1:0)}((f^*) \bullet (g^*))$ for $f \overset{\text{def}}{=\!=} x_1^2 - x_2$ og $g \overset{\text{def}}{=\!=} x_1^3 - x_2^2$.

(3) **Opgave.** (Hører egentlig hjemme i PAK 5.) Bestem $\mathrm{m}_{(1,1)}(F)$ for kurven $F \overset{\text{def}}{=\!=} (1 - 4x_1 + x_2 + 3x_1^2 + x_1x_2 - x_2^2 - x_1^3)$. Bestem samtlige tangenter til kurven i dette punkt.

(4) **Opgave.** Bevis, at linien L er tangent til den projektive kurve C i punktet P, netop hvis $\mathrm{m}_P(L \bullet C) > \mathrm{m}_P(C)$.

(1) **Opgave.** Bestem multipliciteterne $\mathrm{m}_O(F)$, $\mathrm{m}_O(G)$ og $\mathrm{m}_O(F \bullet G)$ for kurverne $F \stackrel{\text{def}}{=\!=} (x_2^3 - x_1^4)$ og $G \stackrel{\text{def}}{=\!=} (x_2^2 - x_1^3)$.

(2) **Stilopgave.** *Snitmultipliciteter.*

(a) Angiv definitionerne af snitmultipliciteten i et affint punkt for to polynomier og af snitmultipliciteten i et projektivt punkt for to projektive kurver.

(b) Angiv de vigtige egenskaber ved snitmultipliciteter.

(c) Bevis additivitetsegenskaben ved snitmultipliciteter. Hvis der udnyttes en isomorfi, der medfører, at snitmultipliciteter kan udtrykkes som dimensioner af passende ringe, da ønskes denne isomorfi angivet (men ikke bevist). Hvis der udnyttes et lemma om primiske elementer i $\mathbb{C}[x_1, x_2]$, da ønskes dette formuleret (men ikke bevist). De enkelte dele af beviset bør fremstå klart.

8. BEZOUT'S SÆTNING

(1) **Bemærkning.** Hvis $c \in \mathbb{C}[x_1, x_2, x_3]$ er homogent, da findes $r \in \mathbb{N}_0$, så $c = x_3^r d$, og så x_3 ikke er divisor i d, og dermed $c = x_3^r (c_*)^*$ ifølge 3.4(2).

(2) **Lemma.** *Lad $C = (c)$ være en projektiv kurve. Da er fællesmængden $\mathrm{W}(C) \cap \mathcal{L}_\infty$ ikke tom, og den er endelig, hvis yderligere $\mathcal{L}_\infty$ ikke er komponent i C.*

(3) *Bevis.* Når $\mathcal{L}_\infty$ er komponent i C, har vi $\mathrm{W}(C) \cap \mathcal{L}_\infty = \mathcal{L}_\infty \neq \varnothing$. Når $\mathcal{L}_\infty$ ikke er komponent i C, er x_3 ikke divisor i c, så vi har $c = (c_*)^*$, og dermed $\mathrm{W}(C) \cap \mathcal{L}_\infty = \mathrm{W}\big((c_*)^*\big) \cap \mathcal{L}_\infty$, som er ikke–tom og endelig ifølge 4.4(1). $\square$

(4) **Lemma.** *Til punkter $P_1, \dots, P_n \in \mathbb{P}^2_{\mathbb{C}}$ findes linie L, som ikke går gennem noget P_i.*

(5) *Bevis.* Da $\mathbb{P}^2_{\mathbb{C}}$ er uendelig, kan $Q \in \mathbb{P}^2_{\mathbb{C}}$ vælges, så $Q \neq P_i$ for alle i. Lad L_i være den projektive linie gennem Q og P_i. Da der (f.eks. ifølge Dualitetsprincippet) findes uendelig mange projektive linier gennem Q, kan projektiv linie L gennem Q vælges, så $L \neq L_i$ for alle i. $\square$

(6) **Bezout's Sætning.** *Hvis C og D er projektive kurver uden fælles komponent, da gælder:*

$$\sum_{P \in \mathbb{P}^2_{\mathbb{C}}} \mathrm{m}_P(C \bullet D) = (\deg C)(\deg D)\,.$$

(7) *Bevis.* Da $\mathcal{L}_\infty$ ikke er komponent i både C og D, er $\mathrm{W}(C) \cap \mathcal{L}_\infty$ eller $\mathrm{W}(D) \cap \mathcal{L}_\infty$ endelig ifølge (2), og dermed er mængden $U \stackrel{\text{def}}{=} \mathrm{W}(C) \cap \mathrm{W}(D) \cap \mathcal{L}_\infty$ endelig.

Vælg $c, d \in \mathbb{C}[x_1, x_2, x_3]$, så $C = (c)$ og $D = (d)$, og sæt $A \stackrel{\text{def}}{=} \mathrm{W}(C) \cap \mathrm{W}(D) \cap \mathbb{A}^2_{\mathbb{C}}$, som ifølge 4.6(5) er lig med $\mathrm{V}(c_*) \cap \mathrm{V}(d_*)$. Polynomierne c_* og d_* har ikke fælles komponent (thi var p en sådan, da ville p^* være divisor i $(c_*)^*$ og $(d_*)^*$ og dermed i c og d ifølge (1)). Derfor giver Endelighedslemmaet, se ROM 5.1(7), at $\mathrm{V}(c_*) \cap \mathrm{V}(d_*)$ er endelig; mængden A er altså endelig.

Da vi nu har, at $\mathrm{W}(C) \cap \mathrm{W}(D) = U \cup A$ er endelig, kan vi ifølge (4) vælge en linie L, så $\mathrm{W}(C) \cap \mathrm{W}(D) \cap L = \varnothing$.

Vælg nu projektivt koordinatskift $\alpha \colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ med $\alpha(L) = \mathcal{L}_\infty$ og isomorfi $\underline{\varphi} \colon \mathbb{C}^3 \to \mathbb{C}^3$ med $\alpha = \underline{\underline{\varphi}}$. Den inverse afbildningen $\alpha^{-1} \colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ er også et projektivt koordinatskift, nemlig $\alpha^{-1} = \underline{\underline{\varphi}^{-1}}$. Vi har:

$$\alpha^{-1}\big(\mathrm{W}(C_\alpha) \cap \mathrm{W}(D_\alpha) \cap \mathcal{L}_\infty\big) \subseteq \alpha^{-1}\big(\mathrm{W}(C_\alpha)\big) \cap \alpha^{-1}\big(\mathrm{W}(D_\alpha)\big) \cap \alpha^{-1}\big(\mathcal{L}_\infty\big)\,,$$

som ifølge 4.5(2) er lig med $\mathrm{W}(C) \cap \mathrm{W}(D) \cap L = \varnothing$. Heraf følger, at:

$$\mathrm{W}(C_\alpha) \cap \mathrm{W}(D_\alpha) \cap \mathcal{L}_\infty = \varnothing\,.$$

Da $\mathrm{W}(C_\alpha) \cap \mathcal{L}_\infty \neq \varnothing$ og $\mathrm{W}(D_\alpha) \cap \mathcal{L}_\infty \neq \varnothing$ ifølge (2), kan $\mathcal{L}_\infty$ ikke være indeholdt i $\mathrm{W}(C_\alpha)$ eller i $\mathrm{W}(D_\alpha)$, dvs. x_3 kan ikke være divisor i de tilsvarende polynomier $c \circ \underline{\varphi}^{-1}$ og $d \circ \underline{\varphi}^{-1}$. For polynomierne $f \stackrel{\text{def}}{=} (c \circ \underline{\varphi}^{-1})_*$ og $g \stackrel{\text{def}}{=} (d \circ \underline{\varphi}^{-1})_*$ gælder derfor, at $f^* = c \circ \underline{\varphi}^{-1}$ og $g^* = d \circ \underline{\varphi}^{-1}$, og at f og g er uden fælles komponent (thi var p en sådan, da ville p^* være divisor i $c \circ \underline{\varphi}^{-1}$ og $d \circ \underline{\varphi}^{-1}$, og dermed ville $p^* \circ \underline{\varphi}$ være divisor i c og d). Endvidere har vi $\mathrm{W}(f^*) \cap \mathrm{W}(g^*) \cap \mathcal{L}_\infty = \mathrm{W}(C_\alpha) \cap \mathrm{W}(D_\alpha) \cap \mathcal{L}_\infty = \varnothing$. Vælg indbyrdes forskellige $P_1, \dots, P_n \in \mathbb{A}^2_{\mathbb{C}}$, så $\mathrm{V}(f) \cap \mathrm{V}(g) = \{P_1, \dots, P_n\}$. Endelighedslemmaet, se ROM 5.1(10),(8), giver nu:

$$\sum_{i=1}^{n} \dim \mathcal{O}_{P_i}(f \bullet g) = (\deg f)(\deg g)\,. \tag{1}$$

Idet

$$\mathrm{W}(C_\alpha) \cap \mathrm{W}(D_\alpha) = \mathrm{W}(C_\alpha) \cap \mathrm{W}(D_\alpha) \cap \mathbb{A}^2_{\mathbb{C}} = \mathrm{V}(f) \cap \mathrm{V}(g) = \{P_1, \dots, P_n\}$$

har vi med henvisning til Snitmultiplicitetssætningen 7.1(3) og (1) ovenfor, at:

$$\begin{aligned}
\sum_{P \in \mathbb{P}^2_{\mathbb{C}}} \mathrm{m}_P(C \bullet D) &\overset{\textbf{(B)}}{=} \sum_{P \in \mathbb{P}^2_{\mathbb{C}}} \mathrm{m}_{\alpha(P)}(C_\alpha \bullet D_\alpha) = \sum_{P \in \mathbb{P}^2_{\mathbb{C}}} \mathrm{m}_P(C_\alpha \bullet D_\alpha) \\
&\overset{\textbf{(P)}}{=} \sum_{i=1}^{n} \mathrm{m}_{P_i}(C_\alpha \bullet D_\alpha) \quad \overset{\textbf{(D)}}{=} \sum_{i=1}^{n} \mathrm{m}_{P_i}(f \bullet g) \\
&\overset{\text{per}}{\underset{\text{def}}{=}} \sum_{i=1}^{n} \dim \mathcal{O}_{P_i}(f \bullet g) \quad \overset{(1)}{=} (\deg f)(\deg g) \\
&= (\deg C_\alpha)(\deg D_\alpha) \quad = (\deg C)(\deg D)\,. \quad \square
\end{aligned}$$

(2) **Eksempel.** For kvadrikkerne C og H fra 7.3(1) har vi – uden udregning – at:

$$4 = 2 \cdot 2 \overset{\text{Be–}}{\underset{\text{zout}}{=}} \sum_{P \in \mathbb{P}^2_{\mathbb{C}}} \mathrm{m}_P(C \bullet H) \overset{\textbf{(V)}}{\geq} \mathrm{m}_P(C \bullet H) + \mathrm{m}_Q(C \bullet H) \overset{\textbf{(F)}}{\geq} 2 + 2 = 4\,,$$

hvoraf $\mathrm{m}_P(C \bullet H) = 2$ og $\mathrm{m}_Q(C \bullet H) = 2$.

(3) **Opgave.** Tegn kurverne $C = (f^*)$ og $D = (g^*)$, hvor $f \overset{\text{def}}{=} x_1^2 + x_2^2 - 1$ og $g \overset{\text{def}}{=} x_1^2 + 4x_2^2 - 4$, bestem $\mathrm{W}(C) \cap \mathrm{W}(D)$, og udnyt Bezout til at bestemme snitmultipliciteten $\mathrm{m}_P(C \bullet D)$ i ethvert $P \in \mathrm{W}(C) \cap \mathrm{W}(D)$.

(4) **Opgave.** Tegn kurverne $C = (f^*)$ og $D = (g^*)$, hvor $f \overset{\text{def}}{=} x_1^2 + (x_2 - 1)^2 - 4$ og $g \overset{\text{def}}{=} x_1^2 + 4x_2^2 - 4$, bestem $\mathrm{W}(C) \cap \mathrm{W}(D)$, og udnyt Bezout til at bestemme snitmultipliciteten $\mathrm{m}_P(C \bullet D)$ i ethvert $P \in \mathrm{W}(C) \cap \mathrm{W}(D)$.

(5) **Kubiske kurver.** En projektiv kurve af grad 3 kaldes en *kubisk kurve.* Lad C være en kubisk kurve. Der følgende muligheder:

/ $C = (\ell^3)$, hvor $L = (\ell)$ er en linie: $\mathrm{W}(C) = \mathrm{W}(L)$, og der er ingen regulære punkter på C.

$\nmid$ $C = (\ell^2 m)$, hvor $L = (\ell)$ og $M = (m)$ er to forskellige linier: $\mathrm{W}(C) = \mathrm{W}(L) \cup \mathrm{W}(M)$, og punkterne på L er ikke–regulære punkter på C, mens ethvert $P \in \mathrm{W}(M) \setminus \mathrm{W}(L)$ er regulært på C.

 $C = (\ell m n)$, hvor $L = (\ell)$, $M = (m)$ og $N = (n)$ er tre indbyrdes forskellige linier, der alle går gennem punktet P: $\mathrm{W}(C) = \mathrm{W}(L) \cup \mathrm{W}(M) \cup \mathrm{W}(N)$, og der er netop ét ikke–regulært punkt på C, nemlig P.

 $C = (\ell m n)$, hvor $L = (\ell)$, $M = (m)$ og $N = (n)$ er tre indbyrdes forskellige linier, der ikke har fælles punkt: $\mathrm{W}(C) = \mathrm{W}(L) \cup \mathrm{W}(M) \cup \mathrm{W}(N)$, og der er netop tre ikke–regulære punkter på C, nemlig de tre skæringspunkter mellem to af linierne.

 $C = (k\ell)$, hvor $K = (k)$ er en irreducibel kvadrik, sml. 6.9(1), og hvor $L = (\ell)$ er tangenten til K i et punkt P: $\mathrm{W}(C) = \mathrm{W}(K) \cup \mathrm{W}(L)$, og der er netop ét ikke–regulært punkt på C, nemlig P. Ifølge **(F)** er $\mathrm{m}_P(K \bullet L) > 1$, så Bezout giver, at der ikke er andre skæringspunkter mellem K og L.

 $C = (k\ell)$, hvor (k) er en irreducibel kvadrik, og hvor (ℓ) er en linie, der ikke er tangent til (k): $\mathrm{W}(C) = \mathrm{W}(k) \cup \mathrm{W}(\ell)$, og der er netop to ikke–regulære punkter på C, nemlig de to skæringspunkter mellem K og L, som Bezout giver. Sml. nu med spørgsmålet i 6.9(4).

$\sim$ C er irreducibel: Se næste resultat.

(1) **Sætning.** *Hvis C er en irreducibel kubisk kurve, da er der højst ét ikke–regulært punkt på C.*

(2) *Bevis.* Antag, at Q er et ikke-regulært punkt på C, dvs. $\mathrm{m}_Q(C) \geq 2$, og at R er et punkt i $\mathbb{P}^2_{\mathbb{C}}$ forskelligt fra Q. Lad L være linien gennem Q og R. Vi har:

$$\begin{aligned} 3 = 3 \cdot 1 &\overset{\text{Be–}}{\underset{\text{zout}}{=\!=}} \sum_{P \in \mathbb{P}^2_{\mathbb{C}}} \mathrm{m}_P(C \bullet L) \\ &\overset{\textbf{(V)}}{\geq} \mathrm{m}_Q(C \bullet L) + \mathrm{m}_R(C \bullet L) \\ &\overset{\textbf{(F)}}{\geq} \mathrm{m}_Q(C) \cdot 1 + \mathrm{m}_R(C) \cdot 1 \\ &\geq 2 + \mathrm{m}_R(C)\,, \end{aligned}$$

hvoraf følger, at $\mathrm{m}_R(C) \leq 1$, hvilket medfører at R ikke er ikke–regulært på C. $\square$

(3) **Opgave.** Antag, at P er et dobbeltpunkt på kurven $F = (f)$ (dvs. $\mathrm{m}_P(F) = 2$), og at L er dobbelttangent til F i P (for $P = O$ betyder dette, at L^2 er det homogene led af laveste grad i F). Bevis, at $\mathrm{m}_P(L \bullet F) \geq 3$. Man siger, at F har en *cusp* i P, netop når $\mathrm{m}_P(L \bullet F) = 3$. Bevis, at hvis $L = (x_2)$, da er O en cusp på F, netop når der for den tredie afledede af f mht. x_1 gælder $f_1'''(O) \neq 0$. Bevis, at hvis P er en cusp på F, da har F kun én komponent gennem P. Angiv en kurve af grad 3 med en cusp i O og tegn den.

(4) **Opgave.** Betragt kurverne $F \overset{\text{def}}{=\!=} (4x_1^2x_2^2 - (x_1^2 + x_2^2)^3)$ og $G \overset{\text{def}}{=\!=} (x_1^2 - x_2^2)$. Angiv kurvernes multiplicitet i begyndelsespunktet O, bestem deres tangenter i dette punkt, og bestem snitmultipliciteten $\mathrm{m}_O(F \bullet G)$. Bestem dernæst snitmultipliciteten $\mathrm{m}_P(F \bullet G)$ for ethvert punkt P på begge kurver. (Benyt Bezout.)

(1) **Opgave.** Betragt kurverne $C \stackrel{\text{def}}{=\!=} (x_2^2x_3 - x_1^3)$ og $D \stackrel{\text{def}}{=\!=} (x_1^2x_3 - x_2^3)$. Bestem multipliciteterne $\mathrm{m}_O(C)$ og $\mathrm{m}_O(D)$ samt snitmultipliciteten $\mathrm{m}_O(C \bullet D)$. Bestem snitmultipliciteten $\mathrm{m}_P(C \bullet D)$ for alle $P \in \mathbb{P}^2_{\mathbb{C}}$. (Benyt Bezout.)

(2) **Opgave.** Antag $F \stackrel{\text{def}}{=\!=} \big(x_2^2 - x_1^2(x_1+1)\big)$. Bestem $\mathrm{m}_O(F)$. Lad P være et regulært punkt på F. Bevis, at tangenten til F i P ikke kan gå igennem O. (Benyt Bezout.)

(3) **Opgave.** Betragt de affine kurver:

$$F \stackrel{\text{def}}{=\!=} \big((x_1+1)^2 + x_2^2 - 1\big) \;\text{ og }\; G \stackrel{\text{def}}{=\!=} \big((x_1+2)^2 + 4x_2^2 - 4\big)\,.$$

Bestem kurvernes multiplicitet i begyndelsespunktet O.
Bestem kurvernes tangenter i O.
Angiv to andre punkter i nulpunktsfællesmængden $\mathrm{V}(F) \cap \mathrm{V}(G)$.
Bestem snitcyklen $F^* \bullet G^*$ for de tilsvarende projektive kurver.

9. Max Noether's Sætning.

(1) **Cykler.** Mængden af heltalsfunktioner $n\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{Z}$ betegnes $\mathbb{Z}^{\mathbb{P}^2_{\mathbb{C}}}$ og er en kommutativ gruppe med additionen $(n, n') \mapsto n + n'\colon \mathbb{P}^2_{\mathbb{C}} \to \mathbb{Z}$, hvor summen $n + n'$ er defineret ved $(n+n')(P) \overset{\text{def}}{=} n(P)+n'(P) \in \mathbb{Z}$ for $P \in \mathbb{P}^2_{\mathbb{C}}$. En funktion $n \in \mathbb{Z}^{\mathbb{P}^2_{\mathbb{C}}}$ siges at være en *cykel*, netop hvis mængden $\{\, P \in \mathbb{P}^2_{\mathbb{C}} \mid n(P) \neq 0 \,\}$ er endelig, og mængden af cykler betegnes $\mathbb{Z}^{(\mathbb{P}^2_{\mathbb{C}})}$ og er en undergruppe af $\mathbb{Z}^{\mathbb{P}^2_{\mathbb{C}}}$. Når n er en cykel, altså $n \in \mathbb{Z}^{(\mathbb{P}^2_{\mathbb{C}})}$, skrives n ofte som en *formel* sum:

$$n = \sum_{P \in \mathbb{P}^2_{\mathbb{C}}} n(P)P = n(P_1)P_1 + \cdots + n(P_m)P_m\,,$$

hvor $P_1, \ldots, P_m \in \mathbb{P}^2_{\mathbb{C}}$ i det sidste udtryk er indbyrdes forskellige og valgt, så $n(P) \neq 0$, kun når $P \in \{P_1, \ldots, P_m\}$. En cykel n er altså en (endelig) *formel* heltalslinearkombination $n_1P_1 + \cdots + n_mP_m$ af punkter i $\mathbb{P}^2_{\mathbb{C}}$.

Graden af en cykel n er givet ved $\deg n \overset{\text{def}}{=} \sum_{P \in \mathbb{P}^2_{\mathbb{C}}} n(P)$, og denne sum har mening og tilhører $\mathbb{Z}$, da $n(P) \neq 0$ kun for endelig mange $P \in \mathbb{P}^2_{\mathbb{C}}$. Altså: $\deg(n_1P_1+\cdots+n_mP_m) = n_1 + \cdots + n_m \in \mathbb{Z}$. Gruppen af cykler *ordnes* (partielt) ved:

$$n \preceq n' \quad \overset{\text{def}}{\iff} \quad \forall\, P \in \mathbb{P}^2_{\mathbb{C}}\colon n(P) \leq n'(P)\,,$$

og vi definerer også:

$$n \prec n' \quad \overset{\text{def}}{\iff} \quad n \preceq n' \;\;\wedge\;\; n \neq n'\,.$$

(2) **Eksempel og advarsel.** Cyklen $n \overset{\text{def}}{=} 1(6\!:\!4\!:\!2) + 2(0\!:\!0\!:\!1) + 0(1\!:\!2\!:\!3)$ kan (med sædvanlige regler for projektive koordinatsæt og for 1 og 0 som koefficienter) skrives $n = (3\!:\!2\!:\!1) + 2(0\!:\!0\!:\!1)$, og den er forskellig fra cyklen $n' \overset{\text{def}}{=} (3\!:\!2\!:\!1)$.

Advarsel: Her, hvor alle de nævnte punkter tilhører $\mathbb{A}^2_{\mathbb{C}}$, kan disse repræsenteres som talpar, og når man gør det, fås $n = (3,2)+2(0,0)$ og $n' = (3,2)$: *Disse er ikke ens cykler!* Undgå derfor at repræsentere punkter, der indgår i cykler, som talpar.

Der gælder $n' \prec n$ samt $\deg n' = 1$ og $\deg n = 3$. For $n'' \overset{\text{def}}{=} (3\!:\!2\!:\!1)+9(1\!:\!0\!:\!0)$ gælder $n' \prec n''$ og $\deg n'' = 10$, men $n \not\preceq n''$ og $n'' \not\preceq n$; det er således ikke alle cykler, der kan sammenlignes ved $\preceq$, så ordningen er ikke total – kun partiel.

(3) **Snitcykler.** Lad C og D være to projektive kurver uden fælles komponent. Vi ved, f.eks. fra Bezout, at $\mathrm{m}_P(C\,\bullet\,D) \neq 0$ kun for endelig mange $P \in \mathbb{P}^2_{\mathbb{C}}$, og *snitcyklen* for C og D defineres ved:

$$C\,\bullet\,D \overset{\text{def}}{=} \sum_{P \in \mathbb{P}^2_{\mathbb{C}}} \mathrm{m}_P(C\,\bullet\,D)P\,.$$

Bezout giver:

$$\text{(4)} \qquad \deg(C\,\bullet\,D) = (\deg C)(\deg D)\,.$$

Snitmultiplicitetsegenskaberne **(A)**, **(B)** og **(D)** giver:

$$\text{(5)} \qquad C\,\bullet\,DE = C\,\bullet\,D + C\,\bullet\,E\,,$$

når E også er en projektiv kurve uden fælles komponemt med C, og $DE \overset{\text{def}}{=} (hk)$, idet $D = (h)$ og $E = (k)$ med homogene $h, k \in \mathbb{C}[x_1, x_2, x_3]$.

(1) **Eksempel.** I eksempel 7.3(1), se også 8.2(2), har vi $C \bullet H = 2P + 2Q$.

(2) **Opgave.** Betragt de affine kurver $F \overset{\text{def}}{=} \big((x_1^2 - x_2^2)^2 - (x_1^2 + x_2^2)^3\big)$ og $G \overset{\text{def}}{=} (x_1 x_2)$. Angiv kurvernes multiplicitet i begyndelsespunktet O, bestem deres tangenter i dette punkt, og bestem snitmultipliciteten $\mathrm{m}_O(F \bullet G)$. Angiv yderligere 4 punkter i nulpunktsfællesmængden $\mathrm{V}(F) \cap \mathrm{V}(G)$. Benyt Bezout til at bestemme nulpunktsfællesmængden $\mathrm{W}(F^*) \cap \mathrm{W}(G^*)$ for de tilsvarende projektive kurver, og bestem snitcyklen $F^* \bullet G^*$.

(3) **Opgave.** Betragt den affine kurve $F = (f)$ med $f \overset{\text{def}}{=} (1 - 2x_1^2 + x_1^4 - x_2^2)$. Bestem samtlige ikke-regulære punkter på F samt multipliciteten i hvert af disse. Bemærk, at $f = \big(x_2 - (x_1^2 - 1)\big)\big(x_2 + (x_1^2 - 1)\big)$. Tegn. Bestem snitcyklen $F^* \bullet G^*$, idet $G \overset{\text{def}}{=} \big(x_2(2x_1 - 2 - x_2)\big)$.

(4) **Max Noether's Sætning.** *Lad C, D og E være projektive kurver, så ingen komponent i C er komponent i D eller E. Antag, at:*

$$C \bullet D \prec C \bullet E \quad \textit{og} \quad \forall\, P \in \mathrm{W}(C) \cap \mathrm{W}(D) \colon P \ \textit{regulært på}\ C\,.$$

Da findes projektiv kurve F uden fælles komponenter med C og af grad $\deg E - \deg D$, *så*

$$(*) \qquad C \bullet F = C \bullet E - C \bullet D\,.$$

(5) *Bevis.* At F findes, så $(*)$, bevises senere. Af $(*)$ og 1(5) følger $C \bullet FD = C \bullet E$, og formlen $\deg F = \deg E - \deg D$ følger af 1(4). $\square$

(6) **Pascal's Sætning.** *Skæringspunkterne for de modstående sider i en sekskant, der er indskrevet i en irreducibel kvadrik, ligger på linie.*

(7) **Kommentar.** Mere udførligt siger Pascal's Sætning:

Lad D være en irreducibel kvadrik, og lad $P_1, \ldots, P_6$ være 6 indbyrdes forskellige punkter på D. For $i \in \{1, \ldots, 6\}$ betegner L_i linien gennem P_i og P_{i+1} (idet indekser regnes modulo seks[4]). For $j \in \{1, 2, 3\}$ betegner Q_j skæringspunktet[5] mellem L_j og L_{j+3}. Da ligger Q_1, Q_2, Q_3 på linie. Se illustration 3(1).

(8) *Bevis for Pascal.* Vi benytter betegnelser fra (7). Betragt de projektive kurver $C \overset{\text{def}}{=} L_1 L_3 L_5$ og $E \overset{\text{def}}{=} L_2 L_4 L_6$, der begge er af grad 3. Vi har:

$$\begin{aligned} C \bullet E &= P_1 + \cdots + P_6 + Q_1 + Q_2 + Q_3 \\ C \bullet D &= P_1 + \cdots + P_6 \end{aligned}$$

så ethvert fællespunkt for C og D er regulært på C, og Max Noether giver:

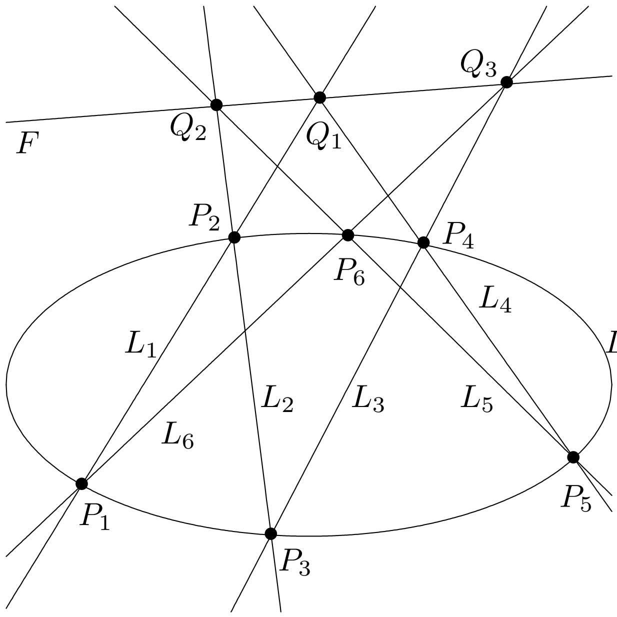
$$C \bullet F = \qquad\qquad Q_1 + Q_2 + Q_3$$

for projektiv kurve F med $\deg F = \deg E - \deg D = 3 - 2 = 1$. Specielt er F en linie gennem Q_1, Q_2 og Q_3. $\square$

[4] Altså $P_7 \overset{\text{def}}{=} P_1$.

[5] Linierne er indbyrdes forskellige, da hver linie har netop to punkter på kvadikken ifølge Bezout.

(1) **Pascal illustreret** (med betegnelser fra 2(7)):



(2) **Kommentar.** En nær slægtning til Pascal's Sætning er Pappos' Sætning 1.3(7), hvori kvadrikken D blot ikke er irreducibel, men består af to forskellige linier.

(3) **Tredie skæringspunkt på kubiske kurver.** Lad C være en irreducibel kubisk kurve, sml. 8.2(5), og lad C° betegne mængden af regulære punkter på C. Husk, at der er højst ét ikke–regulært punkt på C ifølge 8.3(1); altså enten $C^\circ = C$, hvis C er uden ikke–regulære punkter, eller $C^\circ = C \setminus \{U\}$, hvis U er ikke–regulært punkt på C.

For punkter $P, Q \in C^\circ$ sættes:

$$\mathrm{T}_{PQ} \stackrel{\text{def}}{=\!=} \begin{cases} \text{linien gennem } \ P \ \text{ og } \ Q\,, \text{ hvis } \ P \neq Q \\ \text{tangenten til } \ C \ \text{ i } \ P\,, \text{ hvis } \ P = Q\,. \end{cases}$$

I begge tilfælde giver Bezout, at der findes R på C, så $C \bullet \mathrm{T}_{PQ} = P + Q + R$. Der gælder $R \in C^\circ$, hvilket jo er oplagt, når $R = P$ eller $R = Q$, og ellers, dvs. $\mathrm{m}_R(C \bullet \mathrm{T}_{PQ}) = 1$, har vi $R \in C^\circ$ ifølge **(R)**. Punktet R betegnes $P{\wedge}Q$, som udtales "P *hak* Q".

Der findes altså en komposition $\wedge\colon C^\circ \times C^\circ \longrightarrow C^\circ$, $(P, Q) \mapsto P{\wedge}Q$ med:

(4) $$C \bullet \mathrm{T}_{PQ} = P + Q + P{\wedge}Q\,.$$

Kompositionen $\wedge$ er kommutativ, men ikke associativ.

For alle $P, Q, S \in C^\circ$ gælder:

(1) $$\big(\exists L \text{ linie: } C \bullet L = P + Q + S\big) \quad \Rightarrow \quad S = P \wedge Q\,.$$

Hvis nemlig $P \neq Q$, da er L linien gennem P og Q, og hvis $P = Q$, da er L ifølge 7.6(4) tangenten til C i P; i begge tilfælde er $L = \mathrm{T}_{PQ}$, og dermed $S = P \wedge Q$.

(2) **Opgave.** Lad der være givet en irreducibel kubisk kurve C, og lad L være en linie, som skærer C i tre forskellige punkter P_1, P_2 og P_3. Begrund, at disse punkter er regulære på C. For hvert i sættes $T_i \overset{\text{def}}{=\!=} \mathrm{T}_{P_iP_i}$, tangenten til C i P_i, og $Q_i \overset{\text{def}}{=\!=} P_i \wedge P_i$, det tredie skæringspunkt mellem denne tangent og C. Bestem snitcyklerne $C \bullet T_1T_2T_3$ og $C \bullet L^2$. Bevis, at Q_1, Q_2 og Q_3 ligger på en ret linie. (Benyt Max Noether.)

(3) **Opgave.** Lad der være givet en irreducibel kubisk kurve C. Et regulært punkt P på C siges at være en *flex* (på C), netop hvis det tredie skæringspunkt på tangenten T_{PP} til C i P er P selv. Begrund, at dette betyder, at $C \bullet \mathrm{T}_{PP} = 3P$. Lad P og Q være to forskellige flexer på C. Bevis, at $P \wedge Q$ også er en flex.

(4) **Addition på kubiske kurver.** *Fra nu af er N et fast punkt i C°.*

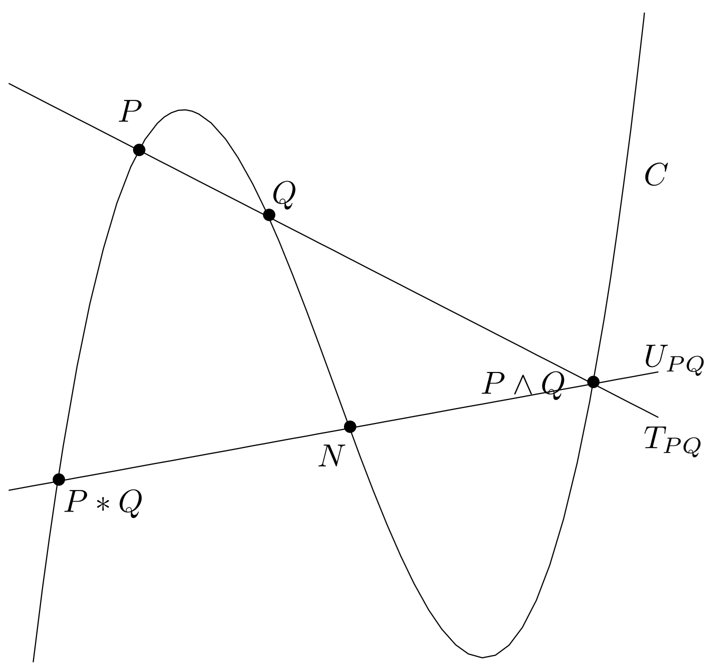
Kompositionen $*\colon C^\circ \times C^\circ \to C^\circ$ defineres ved:

$$P * Q \overset{\text{def}}{=\!=} (P \wedge Q) \wedge N\,.$$

Idet vi sætter $\mathrm{U}_{PQ} \overset{\text{def}}{=\!=} \mathrm{T}_{(P\wedge Q)N}$, gælder der altså:

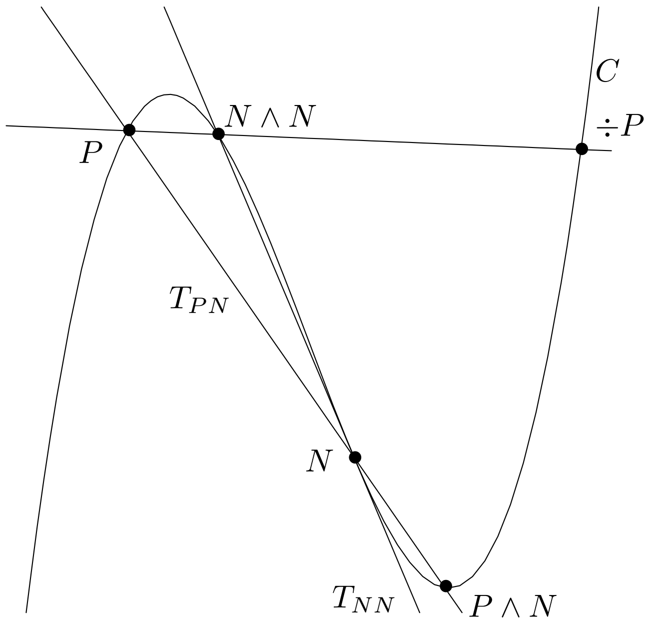
(5) $$C \bullet \mathrm{U}_{PQ} = P \wedge Q + N + P * Q\,.$$

(Bemærk, at man i 3(4) og i (5) ovenfor ikke sætter parenteser om $P \wedge Q$ og $P * Q$.)



For $P \in C^\circ$ defineres:

$$\div P \stackrel{\text{def}}{=} P\wedge(N\wedge N) \ (\in C^\circ)\,.$$



(1) **Sætning.** *Kompositionen $*$ gør C° til en kommutativ gruppe med N som nul-element og $\div P$ som modsat element til P.*

(2) *Bevis.* Kompositionen $*$ er kommutativ, da $\wedge$ er det.

For $P \in C^\circ$ har vi $C_{\bullet}\,\mathrm{T}_{PN} = P + N + P\wedge N = P\wedge N + N + P$, som ifølge 4(1) medfører $P = (P\wedge N)\wedge N$, dvs. $P = P * N$. Punktet N er således neutralt ved $*$.

Ifølge definitionen af $\div P$ har vi $C_{\bullet}\,\mathrm{T}_{P(N\wedge N)} = P + N\wedge N + (\div P) = P + (\div P) + N\wedge N$, som ifølge 4(1) medfører:

$$N\wedge N = P\wedge(\div P)\,.$$

I alt har vi:

$$P * (\div P) = \big(P\wedge(\div P)\big)\wedge N = (N\wedge N)\wedge N = N * N = N\,.$$

Nu skal associativiteten bevises. For $P, Q, S \in C^\circ$ betragtes de projektive kurver $E \stackrel{\text{def}}{=} \mathrm{T}_{PQ}\,\mathrm{T}_{(P*Q)S}\,\mathrm{U}_{QS}$ og $D \stackrel{\text{def}}{=} \mathrm{U}_{PQ}\,\mathrm{T}_{QS}$ af grader henholdsvis 3 og 2. Vi har:

$$\begin{aligned} C_{\bullet}\,E &= P + Q + P\wedge Q + P*Q + S + (P*Q)\wedge S + Q\wedge S + N + Q*S \\ C_{\bullet}\,D &= \phantom{P+{}} Q + P\wedge Q + P*Q + S \phantom{{}+(P*Q)\wedge S} + Q\wedge S + N \end{aligned}$$

så ethvert fællespunkt for C og D er regulært på C, og Max Noether giver:

$$C_{\bullet}\,F = P \qquad + (P*Q)\wedge S \qquad + Q*S$$

for projektiv kurve F med $\deg F = \deg E - \deg D = 3 - 2 = 1$.

Der findes altså linie F med $C \bullet F = P + Q * S + (P * Q)\wedge S$, så 4(1) giver $(P * Q)\wedge S = P\wedge(Q * S)$, og dermed:

$$(P * Q) * S = \big((P * Q)\wedge S\big)\wedge N = \big(P\wedge(Q * S)\big)\wedge N = P * (Q * S)\,. \quad \square$$

(1) **Opgave.** Lad der være givet en irreducibel kubisk kurve C, og lad N være en flex på C, sml. 4(3). Betragt additionen på C med N som neutralt punkt. Begrund, at $N = N\wedge N$, samt at $\div P = P\wedge N$ for alle $P \in C^\circ$. Bevis, at der for regulære punkter P, Q og R på C gælder: $P * Q * R = N$, hvis og kun hvis R ligger på linien T_{PQ} .

(2) **Opgave.** Lad C være en irreducibel kubisk kurve, og lad D være en kvadrik. Antag, at disse to kurver skærer i seks forskellige punkter $P_1, \dots, P_6$. For $i \in \{2, 4, 6\}$ betragtes linien $L_i \overset{\text{def}}{=\!=} \mathrm{T}_{P_{i-1}P_i}$ gennem P_{i-1} og P_i og det tredie skæringspunkt $Q_i \overset{\text{def}}{=\!=} P_{i-1}\wedge P_i$ med C. Bevis, at Q_2, Q_4 og Q_6 ligger på linie. Betragt en addition på C, hvori det neutrale punkt N er en flex på C, sml. 4(3). Bevis, at $P_1 * \cdots * P_6 = N$.

(3) **Opgave.** Lad P være et regulært punkt på en irreducibel kubisk kurve C, lad L være tangenten til C i P, lad R være det tredie skæringspunkt, lad M være tangenten til C i R, lad S være det tredie skæringspunkt, lad N være linien gennem S og P, og lad endelig Q være det tredie skæringspunkt. Tegn. Angiv $C \bullet L^2N$. Bevis, at der findes kvadrik D, så $C \bullet D = 5P + Q$. Bevis, at det herved bestemte punkt Q er entydigt bestemt (altså at hvis D' er en kvadrik med $C \bullet D' = 5P + Q'$, da er $Q' = Q$).

(4) **Opgave.** Antag, at C er en irreducibel kubisk kurve, og at N er en flex på C, sml. 4(3). Betragt additionen $*$ på C° med N som nul-element. Hvad er $N\wedge N$ i dette tilfælde? For et punkt P i C° betegner P' det tredie skæringspunkt mellem tangenten T_{PP} og C. Beskriv P' vha. P, $*$ og $\div$. Beskriv Q i opgave (3) ovenfor vha. P, $*$ og $\div$.

(5) **Opgave.** Antag, at C er en irreducibel kubisk kurve, at D er kubisk kurve, der snitter C i 9 forskellige punkter $P_1, \dots, P_9$, der er regulære på C. Antag yderligere, at P_1, P_2 og P_3 ligger på en linie. Bevis, at de resterende 6 punkter $P_4, \dots, P_9$ ligger på en kvadrik.

(6) **Opgave.** Antag, at P og Q er regulære punkter på en irreducibel kubisk kurve C, at E er en kubisk kurve med $C \bullet E = 8P+Q$, at D er en kvadrik med $C \bullet D = 5P+Q$. Bevis, at P er en flex på C, sml. 4(3), ved at bevise, at der findes en linie T, så $C \bullet T = 3P$, og begrund, at T er tangenten til C i P.

(7) **Opgave.** Antag, at $P_1, \dots, P_6$, P'_5 og P'_6 er 8 regulære punkter på en irreducibel kubisk kurve C, at D og D' er kvadrikker med henholdsvis $C \bullet D = P_1 + \cdots + P_6$ og $C \bullet D' = P_1 + \cdots + P_4 + P'_5 + P'_6$.

Antag, at P_5, P'_5 og P'_6 ligger på en linie L. Udregn snitcyklen $C \bullet DL$. Bevis, at tangenten til C i P_5 går gennem P_6.

Antag nu, at $P_5 = P'_5$. Bevis, at $P_6 = P'_6$. (Antag f.eks., at $P_6 \neq P'_6$, lad M være linien gennem P_6 og P'_6, lad Q være dennes linies tredie skæringspunkt med C, udregn $C \bullet DM$, og udled en modstrid.)

(1) **Opgave.** Antag, at P og Q er regulære punkter på en irreducibel kubisk kurve C, at L er linien T_{PQ} gennem P og Q, at R er denne linies tredie skæringspunkt $P{\wedge}Q$ med C, at M er tangenten T_{RR} til C i R, at S er dennes tredie skæringspunkt $R{\wedge}R$ med C, at N er linien T_{PS} gennem P og S, og at U er dennes tredie skæringspunkt $P{\wedge}S$ med C.

Bestem snitcyklerne $C \bullet L^2N$ og $C \bullet M$.

Bevis, at der findes en kvadrik D, så $C \bullet D = 3P + 2Q + U$.

Bevis, hvis D' er en kvadrik med $C \bullet D' = 3P + 2Q + U'$, da er $U' = U$.

(2) **Opgave.** Bestem snitcyklen $C \bullet D$ for C og D som i 8.2(3), og dernæst som i 8.4(1).

(3) **Opgave.** Lad $F = (f)$ være en affin kurve, og betragt den tilsvarende projektive kurve $F^* = (f^*)$. Beskriv snitcyklen $F^* \bullet \mathcal{L}_\infty$ i lyset af 4.4(1).

(4) **Opgave.** Bestem snitcyklen $C \bullet D$ for de projektive kurver $C \overset{\text{def}}{=\!=} (x_1^2 - x_2^2 + x_1^3)^*$ og $D \overset{\text{def}}{=\!=} (x_1 + x_1^2 + x_2^2)^*$. Tegn.

1. Algebraiske strukturer

(1) **Kommentar.** Vi starter med at genopfriske nogle algebraiske grundbegreber.

(2) **Kommutative grupper.** Lad G være en mængde udstyret med

- en afbildning $+\colon G \times G \to G$, der til ethvert $(g, g') \in G \times G$ tilordner netop ét element $g + g' \in G$;
- en afbildning $-\colon G \to G$, der til ethvert $g \in G$ tilordner netop ét element $-g \in G$;
- et element $0 \in G$.

Mængden G siges at være en *gruppe*, hvis der gælder

(G1) $(g + g') + g'' = g + (g' + g'')$ for alle $g, g', g'' \in G$;
(G2) $g + 0 = g$ og $0 + g = g$ for alle $g \in G$; og
(G3) $g + (-g) = 0$ og $(-g) + g = 0$ for alle $g \in G$.

Her er (G1) associativiteten af $+$, (G2) viser, at 0 er et neutralt element, og (G3) udtrykker, at $-g$ er inverst element til g. Man taler også om gruppen $(G, +)$ eller blot om gruppen G. Brugen af symbolerne $+$, $-$ og 0 omtales som additiv skrivemåde.

Lad $(G, +)$ være en gruppe. Den kaldes *kommutativ* (eller abelsk), netop hvis

(G4) $g + g' = g' + g$ for alle $g, g' \in G$.

I så fald kaldes $+$ *additionen*, 0 omtales som *nul-elementet*, og $-g$ er det *modsatte element*.

Mængden $\{n\}$ bestående af netop ét element n er en kommutativ gruppe: $n + n = n$, $0 = n$ og $-n = n$; den kaldes *nul-gruppen* og betegnes O; altså $O = \{0\}$.

(3) **Kommutative ringe.** Lad $(R, +)$ være en kommutativ gruppe. Den kaldes en *ring*, hvis den (udover $+$, $-$ og 0) er udstyret med

- en (såkaldt) *multiplikation*, dvs. en afbildning: $R \times R \to R$, der til ethvert $(r, r') \in R \times R$ tilordner netop ét element $rr' \in R$; og
- et (såkaldt) *et-element* $1 \in R$,

således at der gælder

(R1) $(rr')r'' = r(r'r'')$ for alle $r, r', r'' \in R$ (associativitet);
(R2) $r(r'+r'') = rr'+rr''$ og $(r+r')r'' = rr''+r'r''$ for alle $r, r', r'' \in R$ (distributivitet);
(R3) $r1 = r$ og $1r = r$ for alle $r \in R$.

Ringen R kaldes *kommutativ*, netop hvis

(R4) $rr' = r'r$ for alle $r, r' \in R$.

Eksempler på kommutative ringe er de hele tal $\mathbb{Z}$, de komplekse tal $\mathbb{C}$ og polynomiumsringene $\mathbb{C}[x_1]$, $\mathbb{C}[x_1, x_2]$ og $\mathbb{C}[x_1, x_2, x_3]$. Ringen $\mathbb{C}^3_3$ af 3×3–matricer er ikke kommutativ.

Ringen R siges at være *ikke–triviel*, netop hvis $R \neq \{0\}$; altså

$$R \text{ ikke–triviel} \quad \Longleftrightarrow \quad 1 \neq 0\,.$$

(til "$\Rightarrow$" vælg $r \in R \setminus \{0\}$, og bemærk, at der gælder $1r = r \neq 0 = 0r$ og dermed $1 \neq 0$.)

(4) **Konvention.** I ROM–delen af disse noter gælder **altid:**

$$\boxed{\boxed{R \ \textbf{er en ikke–triviel kommutativ ring.}}}$$

(1) **Specielle ringelementer.** For $r \in R$ har vi følgende definitioner:

$$\begin{aligned} r \text{ er } \textit{invertibelt} \quad &\Longleftrightarrow \quad \exists\, r^{-1} \in R\colon\ rr^{-1} = 1\,; \\ r \text{ er } \textit{nuldivisor} \quad &\Longleftrightarrow \quad \exists\, a \in R\colon\ ra = 0 \ \wedge\ a \neq 0\,; \\ r \text{ er } \textit{ikke–nuldivisor} \quad &\Longleftrightarrow \quad \forall\, a \in R\colon\ ra = 0 \ \Rightarrow\ a = 0\,. \end{aligned}$$

Et andet ord for et invertibelt element er en *enhed*, og en ikke–nuldivisorer betegnes ofte som et *regulært* element.

(2) **Specielle ringe.** Vi har følgende to definitioner og en observation.

$$\begin{aligned} R \text{ er et } \textit{legeme} \quad &\Longleftrightarrow \quad \forall\, r \in R \setminus \{0\}\colon\ r \ \text{ er invertibelt; og} \\ R \text{ er et } \textit{integritetsområde} \quad &\Longleftrightarrow \quad \forall\, r \in R \setminus \{0\}\colon\ r \ \text{ er en ikke–nuldivisor} \\ &\Longleftrightarrow \quad \forall\, r, r' \in R\colon\ rr' = 0 \ \Rightarrow\ r = 0 \ \vee\ r' = 0\,. \end{aligned}$$

Det sidste udsagn kaldes ofte *nulreglen.* Ethvert legeme er et integritetsområde. De komplekse tal $\mathbb{C}$ er et legeme, mens polynomiumsringene $\mathbb{C}[x_1]$, $\mathbb{C}[x_1, x_2]$ og $\mathbb{C}[x_1, x_2, x_3]$ er integritetsområder, der ikke er legemer (da f.eks. x_1 ikke er invertibelt). Ringen $\mathbb{Z}/(4)$ af restklasser modulo 4, altså $\mathbb{Z}/(4) = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$, er ikke et integritetsområde (da $\overline{2}\,\overline{2} = \overline{0}$, som er nulelementet).

(3) **Idealer.** Et *ideal* $\mathcal{I}$ i R er en delmængde $\mathcal{I} \subseteq R$, der opfylder

(I1) $0 \in \mathcal{I}$;
(I2) $a + a' \in \mathcal{I}$ for alle $a, a' \in \mathcal{I}$; og
(I3) $ra \in \mathcal{I}$ for alle $r \in R$ og $a \in \mathcal{I}$.

Det kaldes *ægte*, netop hvis $\mathcal{I} \neq R$; ægte idealer indeholder ikke invertible elementer (hvis nemlig $u \in \mathcal{I}$ er invertibel, og $r \in R$ er vilkårligt, da gælder $r = r1 = r(uu^{-1}) = r(u^{-1}u) = (ru^{-1})u \in \mathcal{I}$).

Delmængderne $\{0\}$ og R er idealer i R og kaldes de *trivielle idealer*; $\{0\}$ benævnes ofte *nulidealet.*

For $a \in R$ er Ra notationen for *hovedidealet frembragt af* a, og det betegnes ofte (a) (når det af den øvrige sammenhæng fremgår i hvilken ring, vi arbejder); altså

$$(a) = Ra = \{\, ra \mid r \in R \,\}\,.$$

De trivielle idealer er hovedidealer: $\{0\} = (0)$ og $R = (1)$. Fra Mat 2AL vides, at integritetsområderne $\mathbb{Z}$ og $\mathbb{C}[x_1]$ er hovedidealområder: alle idealer i dem er hovedidealer.

(4) **Opgave.** Bevis, at for ethvert $n \in \mathbb{N}_0$ er $\mathcal{M}^n = \{\, f \in \mathbb{C}[x_1, x_2] \mid \operatorname{ord} f \geq n \,\}$ et ideal i $\mathbb{C}[x_1, x_2]$. Hvilke af dem er hovedidealer?

(5) **Moduler.** Lad $(M, +)$ være en kommutativ gruppe. Den kaldes en *modul over* R eller blot en *R–modul*, hvis den (udover $+$, $-$ og 0) er udstyret med

- en (såkaldt) *R–multiplikation*, dvs. en afbildning $R \times M \longrightarrow M$, der til ethvert $(r, m) \in R \times M$ tilordner netop ét element $rm \in M$,

så der gælder

(M1) $(rr')m = r(r'm)$ for alle $r, r' \in R$ og $m \in M$ (associativitet);
(M2) $(r + r')m = rm + r'm$ og $r(m + m') = rm + rm'$ for alle $r, r' \in R$ og $m, m' \in M$ (distributivitet); og
(M3) $1m = m$ for alle $m \in M$ (etreglen).

Ringen R er selv en R–modul med R–multiplikationen lig med ringmultiplikationen.

Nul-gruppen $O = \{0\}$ er altid en R–modul med R–multiplikationen $r0 = 0$.

Hvis R er et legeme, da er M en R–modul, netop hvis M er et vektorrum over R.

Enhver kommutativ gruppe G er en $\mathbb{Z}$–modul med $\mathbb{Z}$–multiplikationen defineret for $r \in \mathbb{Z}$ og $g \in G$ ved $rg = 0$ for $r = 0$, ved $rg = g + \cdots + g$ med r led for $r > 0$ og for $r < 0$ ved $rg = -(-r)g$ (som allerede er defineret, da $-r > 0$). Det følger ved gentagen anvendelse af modulregel (M2), at dette er en $\mathbb{Z}$–multiplikation på gruppen M, og at det er den eneste mulige. På den anden side er enhver modul – og dermed specielt enhver $\mathbb{Z}$–modul – per definition også en kommutativ gruppe. Begrebet "$\mathbb{Z}$–modul" er altså det samme som "kommutativ gruppe".

For ethvert element m i en R–modul M gælder

(1) $$0m = 0 \quad \text{og} \quad (-1)m = -m\,.$$

I første lighed er nullet til venstre for lighedstegnet nul-elementet i R, mens nullet til højre er nul-elementet i M; og i den anden er $-1 \in R$ og $-m \in M$. Første lighed indses således: $0m = (0+0)m = 0m + 0m$ og dermed $0m = 0m - 0m = 0$; og den anden således: $0 = 0m = (1 + (-1))m = 1m + (-1)m = m + (-1)m$.

(2) **Undermoduler.** En *undermodul* N af en R–modul M er en delmængde $N \subseteq M$, der opfylder

(U1) $0 \in N$;
(U2) $n + n' \in N$ for alle $n, n' \in N$; og
(U3) $rn \in N$ for alle $r \in R$ og $n \in N$.

Enhver undermodul er selv en R–modul med restriktionerne af addition og multiplikation. Den kaldes *ægte*, netop hvis $N \neq M$. Hele M er en undermodul af M, og det er $O = \{0\}$ også; dette er de *trivielle undermoduler*.

Undermoduler af R–modulen R er netop idealerne i R.

Hvis R er et legeme, og V er en R–modul, altså et vektorrum over R, da er undermodulerne af V netop underrummene af V.

Lad N og P være undermoduler af M. Fællesmængden $N \cap P$ er da igen en undermodul af M, idet (U1)–(U3) er opfyldt. Summen defineres ved

$$N + P = \{\, n + p \mid n \in N \ \wedge \ p \in P \,\}$$

og er igen en undermodul af M; nemlig:

(U1) $0 = 0 + 0 \in N + P$;
(U2) $(n + p) + (n' + p') = (n + n') + (p + p') \in N + P$ for $n, n' \in N$ og $p, p' \in P$; og
(U3) $r(n + p) = rn + rp \in N + P$ for $n \in N$ og $p \in P$.

Lad nu $N_1, \ldots, N_v$ være undermoduler af R–modul M. Fællesmængden $N_1 \cap \cdots \cap N_v$ er en undermodul af M. For $v > 1$ kan summen defineres rekursivt ved

$$N_1 + \cdots + N_v = (N_1 + \cdots + N_{v-1}) + N_v\,,$$

og dens elementer har formen $n_1 + \cdots + n_v$ med $n_i \in N_i$ for alle i. Ved induktion efter v ses, at $N_1 + \cdots + N_v$ er en undermodul af M.

(1) **Opgave.** Lad N være en delmængde af en R–modul M. Bevis, at N er en undermodul af M, hvis og kun hvis der gælder:

$$N \neq \varnothing \quad \text{og} \quad rn + n' \in N \quad \text{for alle} \quad r \in R \quad \text{og} \quad n, n' \in N\,.$$

(2) **Undermoduler frembragt af delmængde.** Lad M være en R–modul, og lad W være en delmængde af mængden M. Vi sætter $\operatorname{span}_R W$ lig med mængden af *linearkombinationer* af elementer fra W; altså

$$\operatorname{span}_R W = \{\, r_1 w_1 + \cdots + r_n w_n \mid n \in \mathbb{N} \;\wedge\; r_1, \ldots, r_n \in R \;\wedge\; w_1, \ldots, w_n \in W \,\}\,,$$

og $\operatorname{span}_R \varnothing = O$, nulundermodulen af M.

For alle $W \subseteq M$ er $\operatorname{span}_R W$ en undermodul af M: for $W = \varnothing$ er det oplagt (per definition), og for $W \neq \varnothing$ har vi:

- (U1) $0 = 0w \in \operatorname{span}_R W$ for $w \in W$;
- (U2) summen af to linearkombinationer af elementer fra W er igen en linearkombination af elementer fra W; og
- (U3) $r(r_1 w_1 + \cdots + r_n w_n) = (rr_1)w_1 + \cdots + (rr_n)w_n$ ifølge (M1)&(M2).

(Hvis man tillader tomme linearkombinationer og lader sådanne være 0, da bliver den tomme mængdes særstilling overflødig ovenfor.)

Man siger, at *span*$_R W$ er *undermodulen frembragt af* W. Bemærk, at $W \subseteq \operatorname{span}_R W$, og at der gælder lighedstegn her, netop hvis W er en undermodul af M.

(3) **Opgave.** Lad M være en R–modul, lad N være en undermodul af M, og lad W være en delmængde af M. Bevis, at der gælder:

$$W \subseteq N \quad \Rightarrow \quad \operatorname{span}_R W \subseteq N\,.$$

(4) **Endeligt frembragte moduler.** R–modulen M siges at være *endeligt frembragt*, netop hvis der findes en *endelig* delmængde W, så $M = \operatorname{span}_R W$; altså netop hvis der findes $n \in \mathbb{N}_0$ og $m_1, \ldots, m_n \in M$, så ethvert element m i M er en linearkombination af $m_1, \ldots, m_n \in M$, dvs. der findes $r_1, \ldots, r_n \in R$, så $m = r_1 m_1 + \cdots + r_n m_n$.

Nulmodulen O er endeligt frembragt; den kan frembringes af 0 elementer.

R–modulen R er endeligt frembragt; den kan frembriges af det ene element 1. Ethvert hovedideal (a) i R er en endeligt frembragt modul, nemlig frembragt af a.

Idealet $\mathcal{M} = \{\, f \in \mathbb{C}[x_1, x_2] \mid \operatorname{ord} f > 0 \,\}$ i $\mathbb{C}[x_1, x_2]$ er en endeligt frembragt $\mathbb{C}[x_1, x_2]$–modul: den består netop af de polynomier, der ikke har noget konstantled:

$$\sum_{i+j>0} a_{ij} x_1^i x_2^j = \Big(\sum_{i>0} a_{ij} x_1^{i-1} x_2^j\Big) x_1 + \Big(\sum_{j>0} a_{0j} x_2^{j-1}\Big) x_2\,,$$

så den er frembragt af x_1, x_2.

(5) **Opgave.** Bevis, at idealet $\mathcal{M}^n$ fra opgave 2(4) er en endeligt frembragt modul.

(6) **Cykliske moduler.** En R–modul M er *cyklisk*, netop hvis den er frembragt af et element: $M = \operatorname{span}_R\{m\}$ for et $m \in M$. Nulmodulen er cyklisk: $O = \operatorname{span}_R\{0\}$. Ringen R er selv en cyklisk modul: $R = \operatorname{span}_R\{1\}$. Et ideal er en cyklisk modul, netop hvis det er et hovedideal. Vi sætter $Rm = \operatorname{span}_R\{m\}$.

(1) **Opgave.** Lad M være en R–modul, og lad $m_1, \dots, m_n$ tilhøre M. Bevis, at

$$\operatorname{span}_R\{m_1, \dots, m_n\} = Rm_1 + \cdots + Rm_n\,.$$

(2) **Produkt af ideal og undermodul.** Lad M være en R–modul, lad P være en undermodul af M, og lad $\mathcal{I}$ være et ideal i R. *Produktet* af $\mathcal{I}$ og P er undermodulen af M defineret ved:

$$\mathcal{I}P = \operatorname{span}_R\{\, ip \mid i \in \mathcal{I} \ \wedge\ p \in P\,\}\,.$$

Undermodulen $\mathcal{I}P$ består netop af linearkombinationer af elementer fra P med koefficienter fra $\mathcal{I}$; altså:

(3) $$\mathcal{I}P = \{\, i_1p_1 + \cdots + i_np_n \mid n \in \mathbb{N} \ \wedge\ i_1, \dots, i_n \in \mathcal{I} \ \wedge\ p_1, \dots, p_n \in P\,\}\,.$$

Her følger inklusionen $\supseteq$ af, at $\mathcal{I}P$ opfylder (U2). Definitionen af undermodulen $\mathcal{I}P$ viser, at dens elementer har formen $r_1(i_1p_1) + \cdots + r_n(i_np_n)$ med $r_1, \dots, r_n \in R$, $i_1, \dots, i_n \in \mathcal{I}$, og $p_1, \dots, p_n \in P$, altså ifølge modulregel (M1) af formen $(r_1i_1)p_1 + \cdots + (r_ni_n)p_n$, som tilhører højresiden i (3), da $r_1i_1, \dots, r_ni_n \in \mathcal{I}$, og nu er inklusionen $\subseteq$ bevist.

Hvis $\mathcal{I}$ er endeligt frembragt af $a_1, \dots, a_k$, altså $\mathcal{I} = \operatorname{span}_R\{a_1, \dots, a_k\}$, da gælder:

(4) $$\mathcal{I}P = \{\, a_1p_1 + \cdots + a_kp_k \mid p_1, \dots, p_k \in P\,\}\,.$$

Her er inklusionen $\supseteq$ oplagt. Betragt nu et element fra venstresiden:

$$w = i_1y_1 + \cdots + i_ny_n = \sum_{u=1}^{n} i_uy_u \in \mathcal{I}P$$

med $i_1, \dots, i_n \in \mathcal{I}$ og $y_1, \dots, y_n \in P$. Til hvert $i_u \in \mathcal{I} = \operatorname{span}_R\{a_1, \dots, a_k\}$ findes $r_{u1}, \dots, r_{uk} \in R$, så $i_u = \sum_{v=1}^{k} r_{uv}a_v$, og dermed

$$w = \sum_{u=1}^{n} i_uy_u = \sum_{u=1}^{n} \Big(\sum_{v=1}^{k} r_{uv}a_v\Big)y_u = \sum_{v=1}^{k} a_v\Big(\sum_{u=1}^{n} r_{uv}y_u\Big)\,,$$

som er af den ønskede form $\sum_{v=1}^{k} a_vp_v$ med $p_v = \sum_{u=1}^{n} r_{uv}y_u$.

Helt tilsvarende bevises det næste udsagn.

(5) $$P = \operatorname{span}_R\{y_1, \dots, y_\ell\} \quad \Rightarrow \quad \mathcal{I}P = \{\, i_1y_1 + \cdots + i_\ell y_\ell \mid i_1, \dots, i_\ell \in \mathcal{I}\,\}\,.$$

(6) **Opgave.** Bevis det næste udsagn (for $\mathcal{I}$ og P som ovenfor).

(7) $$\begin{gathered}\mathcal{I} = \operatorname{span}_R\{a_1, \dots, a_k\} \ \wedge\ P = \operatorname{span}_R\{y_1, \dots, y_\ell\} \quad \Rightarrow \\ \mathcal{I}P = \operatorname{span}_R\{\, a_uy_v \mid 1 \le u \le k \ \wedge\ 1 \le v \le \ell\,\}\,.\end{gathered}$$

(1) **Produkt af idealer.** Lad $\mathcal{I}$ og $\mathcal{J}$ være idealer i R. Da er

$$\mathcal{I}\mathcal{J} = \operatorname{span}_R\{\, ij \mid i \in \mathcal{I} \;\wedge\; j \in \mathcal{J}\,\}$$

et ideal i R, nemlig produktet af idealet $\mathcal{I}$ og modulen $\mathcal{J}$. For $n \in \mathbb{N}_0$ defineres $\mathcal{I}^n$ rekursivt ved $\mathcal{I}^0 = R$ og $\mathcal{I}^n = \mathcal{I}(\mathcal{I}^{n-1})$ for $n > 0$.

(2) **Opgave.** Betragt idealet $\mathcal{M} = \{\, f \in \mathbb{C}[x_1, x_2] \mid \operatorname{ord} f > 0\,\}$ i $\mathbb{C}[x_1, x_2]$ som i 4(4). Forklar notationen i 2(4) i lys af (1).

(3) **Homomorfier.** Lad M og N være R–moduler, og lad $\varphi\colon M \longrightarrow N$ være en afbildning. Da siges φ at være en *R–homomorfi* – eller blot en homomorfi, netop hvis den opfylder:

(H1) $\varphi(m + m') = \varphi(m) + \varphi(m')$ for alle $m, m' \in M$; og
(H2) $\varphi(rm) = r\varphi(m)$ for alle $r \in R$ og $m \in M$.

Udtrykket *R–lineær afbildning* bruges også for sådanne afbildninger.

Når man taler om en R–homomorfi $\varphi\colon M \longrightarrow N$, underforstås altid, at M og N er R–moduler, M kaldes *kilden* (på engelsk: source) og N *målet* (target) for φ.

Hvis R er et legeme, da er φ en R–homomorfi, netop hvis den er en lineær afbildning $M \longrightarrow N$ af vektorrum over R.

Endvidere er φ en $\mathbb{Z}$–homomorfi, netop hvis den blot opfylder homomorfiregel (H1), dvs. netop hvis den er en homomorfi $M \longrightarrow N$ af kommutative grupper.

Hvis N er en undermodul af en R–modul M, da er *inklusionsafbildningen* $\iota\colon N \longrightarrow M$ en R–homomorfi, der ofte betegnes som $N \hookrightarrow M$. For $N = M$ er det identiteten $\mathrm{id}_M\colon M \longrightarrow M$.

For $a \in R$ og en R–modul M defineres afbildning $a_M\colon M \longrightarrow M$ ved $a_M(m) = am$ for $m \in M$. Denne afbildning er en R–homomorfi, som kaldes *multiplikation med a*. Specielt er $1_M = \mathrm{id}_M$.

Hvis $\varphi\colon M \longrightarrow N$ er en *bijektiv* R–homomorfi, da er $\varphi^{-1}\colon N \longrightarrow M$ også en R–homomorfi, φ siges at være en *R–isomorfi*, og man skriver $\varphi\colon M \xrightarrow{\cong} N$. Identiteten $\mathrm{id}_M\colon M \longrightarrow M$ er en isomorfi. Notationen $M \cong N$ betyder, at der findes en R–isomorfi $M \xrightarrow{\cong} N$, og M og N siges at være *isomorfe*.

Nulhomomorfien $o\colon M \longrightarrow N$ er givet ved $o(m) = 0$ for alle $m \in M$ altså $o = 0_M$.

Der findes netop én R–homomorfi $M \longrightarrow O$, nemlig nulhomomorfien.

Hvis $\varphi\colon M \longrightarrow N$ er en R–homomorfi, da gælder:

$$\varphi(0) = 0 \;\text{ og }\; \varphi(-m) = -\varphi(m) \;\text{ for }\; m \in M\,. \tag{4}$$

Dette følger af regel (H2): $\varphi(0) = \varphi(0m) = 0\varphi(m) = 0$ og $\varphi(-m) = \varphi((-1)m) = (-1)\varphi(m) = -\varphi(m)$. Der findes netop én R–homomorfi $O \longrightarrow N$, nemlig nulhomomorfien.

(5) **Opgave.** Bevis, at (4) også følger af homomorfiregel (H1).

(6) **Opgave.** Bevis, at a_M er en isomorfi for ethvert invertibelt $a \in R$.

(7) **Kerne og billede.** For R–homomorfi $\varphi\colon M \longrightarrow N$ defineres *kernen* (på engelsk: kernel) og *billedet* (på engelsk: image) ved

$$\begin{aligned}\operatorname{Ker}\varphi &\overset{\text{def}}{=\!=} \varphi^{-1}(O) \overset{\text{def}}{=\!=} \{\, m \in M \mid \varphi(m) = 0\,\}\,;\ \text{og}\\ \operatorname{Im}\varphi &\overset{\text{def}}{=\!=} \varphi(M) \quad\overset{\text{def}}{=\!=} \{\, \varphi(m) \mid m \in M\,\}\,,\end{aligned}$$

og der gælder

(1)
$$\begin{aligned} &\operatorname{Ker}\varphi \ \text{ er en undermodul af } \ M\,;\ \text{og}\\ &\operatorname{Im}\varphi \ \text{ er en undermodul af } \ N\,. \end{aligned}$$

For $m, m' \in \operatorname{Ker}\varphi$ og $r \in R$ har vi nemlig:

$$\varphi(0) = 0\,,\ \varphi(m + m') = \varphi(m) + \varphi(m') = 0 + 0 = 0 \ \text{ og } \ \varphi(rm) = r\varphi(m) = r0 = 0\,,$$

og dermed $0, m + m', rm \in \operatorname{Ker}\varphi$. Til $y, y' \in \operatorname{Im}\varphi$ vælges $m, m' \in M$, så $\varphi(m) = y$ og $\varphi(m') = y'$, og for $r \in R$ har vi:

$$\begin{gathered} 0 = \varphi(0) \in \operatorname{Im}\varphi\,,\ y + y' = \varphi(m) + \varphi(m') = \varphi(m + m') \in \operatorname{Im}\varphi \ \text{ og}\\ ry = r\varphi(m) = \varphi(rm) \in \operatorname{Im}\varphi\,. \end{gathered}$$

For enhver R–homomorfi $\varphi\colon M \to N$ gælder:

(2)
$$\varphi \ \text{ er injektiv } \iff \operatorname{Ker}\varphi = O$$

(3)
$$\varphi \ \text{ er surjektiv } \iff \operatorname{Im}\varphi = N\,.$$

Her følger (3) direkte af definitionen af surjektivitet. For at indse (2) antag først, at φ er injektiv, og at m tilhører $\operatorname{Ker}\varphi$. Da $\varphi(m) = 0 = \varphi(0)$, giver injektiviteten, at $m = 0$. Nu er "$\Rightarrow$" i (2) bevist. Antag omvendt, at $\operatorname{Ker}\varphi = O$, og at $m, m' \in M$ har $\varphi(m) = \varphi(m')$. Vi har

$$\varphi(m - m') = \varphi(m + (-m')) = \varphi(m) + \varphi(-m') = \varphi(m) + (-\varphi(m')) = \varphi(m) - \varphi(m') = 0\,,$$

og dermed $m - m' \in \operatorname{Ker}\varphi$, dvs. $m = m'$. Nu er injektiviteten af φ bevist.

(4) **Opgave.** Lad $\varphi\colon M \to N$ være R–homomorfi, og lad M' og N' være undermoduler af henholdsvis M og N. Bevis, at

(5)
$$\varphi(M') \stackrel{\text{def}}{=\!=} \{\, \varphi(m') \mid m' \in M' \,\} \ \text{ er en undermodul af } \ N\,;$$

(6)
$$\varphi^{-1}(N') \stackrel{\text{def}}{=\!=} \{\, m \in M \mid \varphi(m) \in N' \,\} \ \text{ er en undermodul af } \ M\,.$$

Begrund, at (1) er specialtilfælde heraf.

(7) **Direkte sum.** Lad N og P være R–moduler. Når produktmængden $N \times P$ udstyres med additionen $(n, p) + (n', p') = (n + n', p + p')$ for $(n, p), (n', p') \in N \times P$, bliver den til en kommutativ gruppe med $-(n, p) = (-n, -p)$ som modsat element og $(0, 0)$ som nulelement. R–multiplikationen $r(n, p) = (rn, rp)$ for $r \in R$ og $(n, p) \in N \times P$ gør $N \times P$ til en R–modul, der oftest betegnes $N \oplus P$ og kaldes den *(ydre) direkte sum* af N og P, men betegnelsen $N \times P$ bruges også – specielt for ringe, og i så fald taler man om det *direkte produkt.*

Lad N og N' være undermoduler af R–modul M. Afbildningen $\nu_{NN'}\colon N \oplus N' \to M$ defineret ved $\nu_{NN'}(n, n') = n + n'$ for $(n, n') \in N \oplus N'$ er en R–homomorfi med $\operatorname{Im} \nu_{NN'} = N + N'$. Undermodulerne N og N' siges at *danne (indre) direkte sum*, netop hvis $N \cap N' = O$; og i bekræftende fald er $\nu_{NN'}$ en isomorfi: $N \oplus N' \cong N + N'$.

For R–moduler $M_1, \ldots, M_v$ med $v > 1$ defineres den direkte sum rekursivt:

$$M_1 \oplus \cdots \oplus M_v = (M_1 \oplus \cdots \oplus M_{v-1}) \oplus M_v\,,$$

og dette er en R–modul med elementer $(m_1, \ldots, m_v)$, hvor $m_1 \in M_1, \ldots, m_v \in M_v$.

Antag $u \in \mathbb{N}$ og $1 \leq u \leq v$.

Inklusionen $\iota_u\colon M_u \to M_1 \oplus \cdots \oplus M_v$ er givet ved $\iota_u(x) = (0, \ldots, 0, x, 0, \ldots, 0)$ med x på plads u (og 0 på de andre) for $x \in M_u$, og den er en R–homomorfi.

Projektionen $\pi_u\colon M_1 \oplus \cdots \oplus M_v \to M_u$ er givet ved $\pi_u(m_1, \ldots, m_v) = m_u$ for $(m_1, \ldots, m_v) \in M_1 \oplus \cdots \oplus M_v$, og den er en R–homomorfi. Der gælder $\pi_u \circ \iota_u = \mathrm{id}_{M_u}$.

2. Restklassemoduler

$\boxed{\boxed{R \text{ er en ikke–triviel kommutativ ring.}}}$

(1) **Restklasser.** Lad M være en R–modul, og lad H være en undermodul af M. For $m \in M$ er *restklassen* $[m]_H$ *af* m *modulo* H defineret ved:

$$[m]_H = \{\, m + h \mid h \in H \,\}\,,$$

som er en delmængde af M. (På engelsk kaldes dette ofte "coset" og betegnes $m+H$ (da additiv skrivemåde benyttes.) Bemærk i øvrigt, at da M er kommutativ som gruppe, er H en normal undergruppe af M.)

For $m, m' \in M$ gælder:

$$[m]_H = [m']_H \quad \Longleftrightarrow \quad m - m' \in H\,.$$

Med M/H betegnes *mængden af restklasser modulo* H; altså:

$$M/H = \{\ [m]_H \mid m \in M\,\}\,.$$

Når undermodulen H fremgår af den øvrige sammenhæng skrives $\overline{M} = M/H$ og $\overline{m} = [m]_H$, og dermed $\overline{M} = \{\,\overline{m} \mid m \in M\,\}$.

Der defineres en addition i $\overline{M}$ ved $\overline{m_1} + \overline{m_2} = \overline{m_1 + m_2}$ for $m_1, m_2 \in M$. For at indse, at dette er en korrekt definition (dvs. at $+$ herved er "veldefineret"), antag, at $\overline{m_1} = \overline{m_1'}$ og $\overline{m_2} = \overline{m_2'}$, og bemærk, at $(m_1+m_2)-(m_1'+m_2') = (m_1-m_1')+(m_2-m_2') \in H$, hvoraf følger $\overline{m_1 + m_2} = \overline{m_1' + m_2'}$ som ønsket. Herved bliver $(\overline{M}, +)$ en kommutativ gruppe.

Ved $r\overline{m} = \overline{rm}$ gives en korrekt definition af en R–multiplikation. Hvis nemlig $\overline{m} = \overline{m'}$, da er $rm - rm' = r(m - m') \in H$, og dermed $\overline{rm} = \overline{rm'}$. Med $\overline{0}$ som nulelement og $-\overline{m} = \overline{-m}$ modsat element bliver modulreglerne er opfyldt, så $\overline{M}$ en R–modul:

$$M/H \ \text{ er en } R\text{–modul med } \ [m]_H + [m']_H = [m + m']_H\,,$$
$$\text{nulelement } \ [0]_H\,, \quad -[m]_H = [-m]_H \ \text{ og } \ r[m]_H = [rm]_H$$

for $r \in R$ og $m, m' \in M$. I R–modulen M/H gælder for $m \in M$, at

$$[m]_H = 0 \quad \Longleftrightarrow \quad m \in H\,.$$

Man kalder M/H *restklassemodulen* M *modulo* H. (Andre navne er kvotientmodulen og faktormodulen.) Afbildningen

$$\pi_H \colon M \to M/H \ \text{ givet ved } \ \pi_H(m) = [m]_H$$

er en R–homomorfi, der kaldes *restklassehomomorfien*, og den betegnes ofte $M \twoheadrightarrow M/H$. Den har $\operatorname{Ker} \pi_H = H$ og er surjektiv: $\operatorname{Im} \pi_H = M/H$.

For nulundermodulen O af M og $m \in M$ gælder $[m]_O = \{m\}$, $[m]_O + [m']_O = \{m+m'\}$ og $r[m]_O = \{rm\}$, så derfor identificeres M/O altid med M; altså $M/O = M$.

For undermodulen M af M og $m \in M$ gælder $[m]_M = M$, så modulen M/M har netop ét element, dvs. $M/M = O$, nulmodulen.

(2) **Undermoduler af restklassemoduler.** Lad M være en R–modul, og lad H være en undermodul af M.

Hvis K også er en undermodul af M, og $K \supseteq H$, da er H en undermodul af R–modulen K, og $K/H = \{\ [k]_H \mid k \in K\,\}$ $(\subseteq M/H)$ opfylder undermodulbetingelserne, og derfor er K/H en undermodul af M/H. Hvis omvendt W er en undermodul af R–modulen M/H, og K sættes lig med originalmængden $\pi_H^{-1}(W) = \{\, m \in M \mid [m]_H \in W\,\}$, da er K en undermodul af M, og $W = K/H$.

(1) **Homomorfisætningen.** *Hvis $\varphi\colon M \to P$ er en R–homomorfi, og H er en undermodul af M indeholdt i $\operatorname{Ker}\varphi$, da induceres en R–homomorfi:*

$$\widetilde{\varphi}\colon M/H \to P \quad \textit{med} \quad \widetilde{\varphi}([m]_H) = \varphi(m)\,, \quad \operatorname{Ker}\widetilde{\varphi} = \operatorname{Ker}\varphi/H \quad \textit{og} \quad \operatorname{Im}\widetilde{\varphi} = \operatorname{Im}\varphi\,.$$

(2) *Bevis.* Hvis $m, m' \in M$ har $[m]_H = [m']_H$, da gælder $m - m' \in H \subseteq \operatorname{Ker}\varphi$, så $\varphi(m) - \varphi(m') = \varphi(m - m') = 0$, dvs. $\varphi(m) = \varphi(m')$. Dette viser, at definitionen $\widetilde{\varphi}([m]_H) = \varphi(m)$ er korrekt. At $\widetilde{\varphi}$ opfylder (H1) og (H2) ses ved inspektion, og det samme gælder påstandene om $\operatorname{Ker}\widetilde{\varphi}$ og $\operatorname{Im}\widetilde{\varphi}$. $\square$

(3) **Isomorfisætningen.** *Enhver R–homomorfi $\varphi\colon M \to P$ inducerer en R–isomorfi:*

$$\widetilde{\varphi}\colon M/\operatorname{Ker}\varphi \xrightarrow{\cong} \operatorname{Im}\varphi \quad \textit{med} \quad \widetilde{\varphi}([m]_{\operatorname{Ker}\varphi}) = \varphi(m)\,.$$

(4) *Bevis.* Dette følger direkte af Homomorfisætningen med $H = \operatorname{Ker}\varphi$. $\square$

(5) **Restklassemodullemmaet.** *Lad M være en R–modul, og lad H være en undermodul af M. Undermodulerne af restklassemodulen M/H er da netop delmængderne K/H, hvor K er en undermodul af M indeholdende H, og for sådanne er der en isomorfi*

(6)
$$\begin{aligned} (M/H)/(K/H) &\xrightarrow{\cong} M/K \\ \big[\,[m]_H\big]_{K/H} &\longmapsto [m]_K\,. \end{aligned}$$

(7) *Bevis.* At undermodulerne netop er de beskrevne fremgår af 1(2). At give afbildningen

$$\pi_{HK}\colon M/H \to M/K \quad \text{ved} \quad [m]_H \mapsto [m]_K$$

er en korrekt definition, da $H \subseteq K$. Endvidere er π_{HK} en R–homomorfi med $\operatorname{Ker}\pi_{HK} = K/H$ og $\operatorname{Im}\pi_{HK} = M/K$. Isomorfisætningen giver derfor den ønskede isomorfi. $\square$

(8) **Kommentar.** Restklassemodullemmaet kaldes ofte *Noether's anden Isomorfisætning* (men her ønsker jeg at tydeliggøre en analogi med et senere resultat).

(9) **Noether's første Isomorfisætning.** *Lad M være en R–modul, og lad H og K være undermoduler af M. Der er da en R–isomorfi:*

$$\begin{aligned} H/H\cap K &\xrightarrow{\cong} (H+K)/K \\ [h]_{H\cap K} &\longmapsto [h]_K\,. \end{aligned}$$

(10) *Bevis.* Sammensætningen $H \hookrightarrow H+K \twoheadrightarrow (H+K)/K$ (af inklusionen og restklassehomomorfien) er en R–homomorfi $\varphi\colon H \to (H+K)/K$ givet ved $\varphi(h) = [h]_K$ og med $\operatorname{Ker}\varphi = H \cap K$. Den er surjektiv: for et vilkårligt element $[h+k]_K \in (H+K)/K$ gælder (da $(h+k) - h = k \in K$), at $[h+k]_K = [h]_K = \varphi(h)$. Isomorfisætningen giver nu den ønskede isomorfi. $\square$

(1) **Annullatorer.** Lad M være en R–modul, og lad m være et element i M. Vi definerer *annullatoren* $\operatorname{Ann}_R M$ af modulen M og *annullatoren* $\operatorname{Ann}_R(m)$ af elementet m ved henholdsvis:

$$\begin{aligned}\operatorname{Ann}_R M &= \{\, r \in R \mid \forall\, m \in M\colon\ rm = 0 \,\} \quad \text{og} \\ \operatorname{Ann}_R(m) &= \{\, r \in R \mid rm = 0 \,\}\,.\end{aligned}$$

Disse annulatorer er idealer i R, da det eftervises direkte at idealbetingelserne (I1)–(I3) er opfyldt. Det nedre indeks $_R$ udelades, når ringens navn er oplagt. Der gælder $\operatorname{Ann} Rm = \operatorname{Ann}(m)$, idet inklusionen $\subseteq$ følger af $m \in Rm$; og for $a \in \operatorname{Ann}(m)$ og $rm \in Rm$ har vi $a(rm) = (ar)m = (ra)m = r(am) = r0 = 0$, hvilket viser den anden inklusion.

(2) **Sætning om cykliske moduler.** *For enhver R–modul M er følgende ensbetydende.*

(*i*) *M er cyklisk;*
(*ii*) *$M \cong R/\operatorname{Ann} M$;*
(*iii*) *der findes ideal $\mathcal{I}$, så $R/\mathcal{I} \cong M$;*
(*iv*) *der findes surjektiv R–homomorfi $\psi\colon R \longrightarrow M$.*

(3) *Bevis.* (*i*) $\Rightarrow$ (*ii*): Antag $M = Rm$, og lad afbildningen $\varphi\colon R \longrightarrow M$ være defineret ved $\varphi(r) = rm$. Da φ er en R–homomorfi med $\operatorname{Ker}\varphi = \operatorname{Ann}(m) = \operatorname{Ann} Rm = \operatorname{Ann} M$ og $\operatorname{Im}\varphi = Rm = M$ følger det ønskede af Isomorfisætningen.

(*ii*) $\Rightarrow$ (*iii*) er oplagt.

(*iii*) $\Rightarrow$ (*iv*): Sammensætningen $R \twoheadrightarrow R/\mathcal{I} \xrightarrow{\cong} M$ af restklasseafbildningen og isomorfien er en surjektiv R–homomorfi.

(*iv*) $\Rightarrow$ (*i*): Sæt $m = \psi(1)$, og vi vil bevise $M = Rm$. Til vilkårligt $y \in M$ findes (da ψ er surjektiv) $r \in R$, så $y = \psi(r)$. Der gælder $y = \psi(r1) = r\psi(1) = rm \in Rm$ som ønsket. $\square$

(4) **Opgave.** Bevis, at der gælder $\operatorname{Ann}(H + K) = (\operatorname{Ann} H) \cap (\operatorname{Ann} K)$ for undermoduler H og K af en modul M. Bevis, at hvis M er frembragt af $m_1, \dots, m_v$, da er $\operatorname{Ann} M = \operatorname{Ann}(m_1) \cap \cdots \cap \operatorname{Ann}(m_v)$.

(5) **Sætning.** *For enhver undermodul H af R–modulen M gælder:*

(6) $$M = \operatorname{span}\{y_1, \dots, y_v\} \quad \Rightarrow \quad M/H = \operatorname{span}\{[y_1]_H, \dots, [y_v]_H\}\,;$$

(7) $$\begin{gathered} H = \operatorname{span}\{x_1, \dots, x_u\} \ \wedge\ M/H = \operatorname{span}\{[z_1]_H, \dots, [z_w]_H\} \quad \Rightarrow \\ M = \operatorname{span}\{x_1, \dots, x_u; z_1, \dots, z_w\}\,. \end{gathered}$$

(8) *Bevis.* (6): Elementerne i M/H har formen $[m]_H$ med $m \in M$, og der findes $r_1, \dots, r_v$ i R, så $m = r_1y_1 + \cdots + r_vy_v$, og dermed $[m]_H = [r_1y_1 + \cdots + r_vy_v]_H = r_1[y_1]_H + \cdots + r_v[y_v]_H$ som ønsket.

(7): For $m \in M$ betragtes $[m]_H \in M/H$, og der vælges $s_1, \dots, s_w \in R$, så $[m]_H = s_1[z_1]_H + \cdots + s_w[z_w]_H$, og dermed $[m]_H = [s_1z_1 + \cdots + s_wz_w]_H$, hvilket medfører, at elementet $m - (s_1z_1 + \cdots + s_wz_w)$ tilhører H. Kald dette element h, og vælg $q_1, \dots, q_u \in R$, så $h = q_1x_1 \cdots + q_ux_u$. Vi har $m = s_1z_1 + \cdots + s_wz_w + q_1x_1 \cdots + q_ux_u$ som ønsket. $\square$

Vi benytter ofte 3(6) og 3(7) på følgende korte form:

(1) M endeligt frembragt $\Rightarrow$ M/H endeligt frembragt; og

(2) H og M/H endeligt frembragte $\Rightarrow$ M endeligt frembragt.

(3) **Exakte følger.** En følge $K \xrightarrow{\kappa} L \xrightarrow{\lambda} M$ af R–homomorfier siges at være *exakt i* L, netop hvis $\operatorname{Im}\kappa = \operatorname{Ker}\lambda$. En følge

$$\mathbb{L} \quad = \quad L^0 \xrightarrow{\psi^0} L^1 \to \cdots \to L^{i-1} \xrightarrow{\psi^{i-1}} L^i \xrightarrow{\psi^i} L^{i+1} \to \cdots \to L^{m-1} \xrightarrow{\psi^{m-1}} L^m$$

af m R–homomorfier siges at være *exakt*, netop hvis den er exakt i enhver L^i med $0 < i < m$, dvs. $\operatorname{Im}\psi^{i-1} = \operatorname{Ker}\psi^i$ for alle i med $0 < i < m$. Bemærk i øvrigt, at her har homomorfien $\psi^i \colon L^i \to L^{i+1}$ samme indeks som sin kilde.

(4) **Opgave.** Betragt følgen $\mathbb{L} = 0 \to L^1 \to 0$ (altså $m = 2$, $L^0 = 0$ og $L^2 = 0$ i notationen ovenfor). Bevis, at denne følge er exakt, netop hvis $L^1 = 0$.

(5) **Opgave.** Bevis, at $\mathbb{L} = 0 \to L^1 \xrightarrow{\psi^1} L^2 \to 0$ er exakt, netop hvis ψ^1 er en isomorfi.

(6) **Opgave.** Antag, at H er en undermodul af R–modulen M. Begrund, at der er en exakt følge $0 \to H \hookrightarrow M \twoheadrightarrow M/H \to 0$.

(7) **Opgave.** Bevis, at $\mathbb{L} = 0 \to L^1 \xrightarrow{\psi^1} L^2 \xrightarrow{\psi^2} L^3 \to 0$ er exakt, netop hvis

$$\psi^1 \text{ er injektiv,} \quad \operatorname{Im}\psi^1 = \operatorname{Ker}\psi^2 \quad \text{og} \quad \psi^2 \text{ er surjektiv.}$$

Bevis, at når $\mathbb{L}$ er exakt, da gælder

(8) $$L^1 \cong \operatorname{Ker}\psi^2 \quad \text{og} \quad L^3 \cong L^2/\operatorname{Ker}\psi^2\,.$$

(9) $\mathbb{C}$–**algebraer.** Antag, at ringen R er en $\mathbb{C}$–*algebra*, dvs. at der findes $\delta\colon \mathbb{C} \to R$, som er en *ringhomomorfi*; for alle $a, a' \in \mathbb{C}$ har vi altså

$$\delta(a + a') = \delta(a) + \delta(a')\,, \quad \delta(aa') = \delta(a)\delta(a') \quad \text{og} \quad \delta(1) = 1\,.$$

Her er det første 1 tallet $1 \in \mathbb{C}$ (dvs. etelementet i ringen $\mathbb{C}$), og det andet 1 er etelementet i ringen R.

Enhver R–modul M bliver en $\mathbb{C}$–modul (altså et vektorrum over $\mathbb{C}$) ved $\mathbb{C}$–multiplikationen $\mathbb{C} \times M \to M$ givet ved $(c, m) \mapsto \delta(c)m$; altså $cm = \delta(c)m$. Dimensionen af M som vektorrum over $\mathbb{C}$ betegnes $\dim M$ (og denne dimension kan selvfølgelig godt være uendelig).

(10) **Dimensionssætningen.** *Antag, at* R *er en* $\mathbb{C}$*–algebra, og at* H *er undermodul af* R*–modulen* M*. Hvis* $\dim H$ *og* $\dim(M/H)$ *begge er endelige, da er* $\dim M$ *endelig, og*

$$\dim M = \dim H + \dim(M/H)\,.$$

(1) *Bevis.* Sæt $u = \dim H$ og $w = \dim \overline{M}$, idet $\overline{M} = M/H$, og vælg baser $(x_1, \ldots, x_u)$ og $(\overline{z_1}, \ldots, \overline{z_w})$ for vektorrummene henholdsvis H og $\overline{M}$. Da $x_1, \ldots, x_u$ og $\overline{z_1}, \ldots, \overline{z_w}$ frembringer henholdsvis H og $\overline{M}$ som $\mathbb{C}$–moduler, giver 3(7) (anvendt over ringen $\mathbb{C}$), at $\mathbb{C}$–modulen (dvs. vektorrummet) M er frembragt af $x_1, \ldots, x_u; z_1, \ldots, z_w$. Nu mangler vi blot at bevise, at disse $u + w$ vektorer udgør et lineært uafhængigt sæt. Betragt derfor en lineær relation

$$a_1x_1 + \cdots + a_ux_u + c_1z_1 + \cdots + c_wz_w = 0 \tag{2}$$

med $a_1, \ldots, a_u; c_1, \ldots, c_w \in \mathbb{C}$. I restklassemodulen $\overline{M}$ fås

$$c_1\overline{z_1} + \cdots + c_w\overline{z_w} = \overline{c_1z_1 + \cdots + c_wz_w} = -\overline{a_1x_1 + \cdots + a_ux_u} = 0\,,$$

hvilket – da sættet $(\overline{z_1}, \ldots, \overline{z_w})$ er lineært uafhægigt – giver $c_1 = \cdots = c_w = 0$. Herefter er relationen (2) reduceret til $a_1x_1 + \cdots + a_ux_u = 0$, som – da sættet $(x_1, \ldots, x_u)$ er lineært uafhægigt – giver $a_1 = \cdots = a_u = 0$. Det ønskede er nu bevist: relationen (2) er triviel. □

(3) **Den udvidede Dimensionssætning.** *Lad R være en $\mathbb{C}$–algebra, og betragt følgen*

$$\mathbb{M} \quad = \quad 0 \longrightarrow M^0 \xrightarrow{\varphi^0} M^1 \xrightarrow{\varphi^1} \cdots \xrightarrow{\varphi^{n-2}} M^{n-1} \xrightarrow{\varphi^{n-1}} M^n \longrightarrow 0$$

af $n+2$ R–homomorfier (startende og sluttende med nul). Hvis $\mathbb{M}$ er exakt, og $\dim M^i$ *er endelig for alle i, da gælder*

$$\sum_{i=0}^{n} (-1)^i \dim M^i = 0\,.$$

Konklusionen kan også skrives

$$\dim M^0 - \dim M^1 + \cdots + (-1)^{n-1} \dim M^{n-1} + (-1)^n \dim M^n = 0\,. \tag{†}$$

(4) *Bevis.* Først behandles to specialtilfælde.
<u>$n = 0$</u>, dvs. $\mathbb{M} = 0 \longrightarrow M^0 \longrightarrow 0$: Ifølge opgave 4(4) har vi $M^0 = 0$, og dermed

$$\sum_{i=0}^{0} (-1)^i \dim M^i = \dim M^0 = 0\,.$$

<u>$n = 1$</u>, dvs. $\mathbb{M} = 0 \longrightarrow M^0 \xrightarrow{\varphi^0} M^1 \longrightarrow 0$: Ifølge opgave 4(5) har vi $M^0 \cong M^1$ som R–moduler – og dermed også som vektorrum, og vi får

$$\sum_{i=0}^{1} (-1)^i \dim M^i = \dim M^0 - \dim M^1 = 0\,.$$

Nu er påstanden bevist for $n = 0$ og for $n = 1$. Generelt bevises den ved induktion efter n startende for $n = 2$.

$\underline{n=2}$, dvs. $\mathbb{M} = 0 \longrightarrow M^0 \xrightarrow{\varphi^0} M^1 \xrightarrow{\varphi^1} M^2 \longrightarrow 0$: Ifølge opgave 4(7) har vi

$$M^0 \cong \operatorname{Ker}\varphi^1 \quad \text{og} \quad M^2 \cong M^1/\operatorname{Ker}\varphi^1 .$$

Dette giver første lighedstegn i den næste kæde, hvori det andet følger af Dimensionssætningen 4(10).

$$\begin{aligned}\sum_{i=0}^{2}(-1)^i \dim M^i &= \dim \operatorname{Ker}\varphi^1 - \dim M^1 + \dim(M^1/\operatorname{Ker}\varphi^1) \\ &= \dim \operatorname{Ker}\varphi^1 - \dim M^1 + \dim M^1 - \dim \operatorname{Ker}\varphi^1 = 0 .\end{aligned}$$

$\underline{n>2}$ (induktionstrinnet): Sæt $W = \operatorname{Ker}\varphi^{n-1} = \operatorname{Im}\varphi^{n-2}$ ($\subseteq M^{n-1}$), og betragt følgen

$$\mathbb{M}' \quad = \quad 0 \longrightarrow M^0 \xrightarrow{\varphi^0} M^1 \xrightarrow{\varphi^1} \cdots \longrightarrow M^{n-3} \xrightarrow{\varphi^{n-3}} M^{n-2} \xrightarrow{\widetilde{\varphi}^{n-2}} W \longrightarrow 0 ,$$

hvor $\widetilde{\varphi}^{n-2}(x) = \varphi^{n-2}(x)$ for $x \in M^{n-2}$. Følgen $\mathbb{M}'$ er exakt i M^i for $0 \le i \le n-3$, da den oprindelige følge $\mathbb{M}$ er det. Følgen $\mathbb{M}'$ er også exakt i M^{n-2}, da

$$\operatorname{Im}\varphi^{n-3} = \operatorname{Ker}\varphi^{n-2} = \operatorname{Ker}\widetilde{\varphi}^{n-2} .$$

Endelig er $\mathbb{M}'$ exakt i W, da $\operatorname{Im}\widetilde{\varphi}^{n-2} = W = \operatorname{Ker}(W \longrightarrow 0)$.

Da følgen $\mathbb{M}'$ således er (overalt) exakt, giver induktionsantagelsen

$$(\ddagger) \qquad \dim M^0 - \dim M^1 + \cdots + (-1)^{n-2}\dim M^{n-2} + (-1)^{n-1}\dim W = 0 .$$

På den anden side er følgen

$$0 \longrightarrow W \hookrightarrow M^{n-1} \xrightarrow{\varphi^{n-1}} M^n \longrightarrow 0$$

exakt, så tilfældet $n = 2$ giver $\dim W - \dim M^{n-1} + \dim M^n = 0$, dvs. $\dim W = \dim M^{n-1} - \dim M^n$, der indsat i ($\ddagger$) giver den ønskede ($\dagger$). $\square$

(1) **Restklasseringe.** Lad $\mathcal{I}$ være et ideal i R, dvs. en undermodul af R–modulen R. I restklassemodulen $R/\mathcal{I}$ defineres et produkt $(R/\mathcal{I}) \times (R/\mathcal{I}) \longrightarrow R/\mathcal{I}$ korrekt ved $([r]_\mathcal{I}, [r']_\mathcal{I}) \mapsto [rr']_\mathcal{I}$, og dette gør $R/\mathcal{I}$ til en kommutativ ring, der kaldes *restklasseringen R modulo $\mathcal{I}$*. Ringen $R/\mathcal{I}$ er ikke–triviel, netop hvis idealet $\mathcal{I}$ er ægte.

Enhver $R/\mathcal{I}$–modul W er også en R–modul med multiplikationen $R \times W \longrightarrow W$ defineret ved $(r, w) \mapsto [r]_\mathcal{I} w$; altså $rw = [r]_\mathcal{I} w$. Der gælder $\operatorname{Ann}_R W \supseteq \mathcal{I}$, da $iw = [i]_\mathcal{I} w = 0w = 0$ for $i \in \mathcal{I}$ og $w \in W$.

På den anden side er enhver R–modul M med $\operatorname{Ann}_R M \supseteq \mathcal{I}$ også en $R/\mathcal{I}$–modul med multiplikationen $(R/\mathcal{I}) \times M \longrightarrow M$ korrekt defineret ved $([r]_\mathcal{I}, m) \mapsto rm$; altså $[r]_\mathcal{I} m = rm$.

(2) **Opgave.** Lad $\mathcal{I}$ være et ideal i R, og lad M være en R–modul. Giv $M/\mathcal{I}M$ en struktur som $R/\mathcal{I}$–modul. Bevis, at hvis $y_1, \ldots, y_u$ frembringer M som R–modul, da frembringer restklasserne $[y_1]_{\mathcal{I}M}, \ldots, [y_u]_{\mathcal{I}M}$ restklassemodulen $M/\mathcal{I}M$ som $R/\mathcal{I}$–modul.

(1) **Primidealer.** En delmængde $\mathcal{P} \subseteq R$ siges at være et *primideal* i R, netop hvis

$$(*) \qquad \mathcal{P} \text{ er et \textit{ægte} ideal i } R \quad \text{og} \quad \forall\, r, r' \in R\colon \quad rr' \in \mathcal{P} \quad \Rightarrow \quad r \in \mathcal{P} \ \vee \ r' \in \mathcal{P}\,.$$

Mængden af primidealer i R betegnes $\operatorname{Spec} R$; altså:

$$\operatorname{Spec} R = \{\, \mathcal{P} \subset R \mid \mathcal{P} \text{ er et primideal} \,\}\,.$$

I restklasseringen $R/\mathcal{P}$ bliver sidste del af udsagnet $(*)$ ovenfor til:

$$\forall\, r, r' \in R\colon \quad [rr']_{\mathcal{P}} = 0 \quad \Rightarrow \quad [r]_{\mathcal{P}} = 0 \ \vee \ [r']_{\mathcal{P}} = 0\,,$$

og dette viser, at vi har:

$$\mathcal{P} \in \operatorname{Spec} R \quad \iff \quad R/\mathcal{P} \text{ er et integritetsområde.}$$

Specielt er R et integritetsområde, netop hvis nulidealet O tilhører $\operatorname{Spec} R$.

(2) **Maksimalidealer.** En delmængde $\mathcal{M} \subseteq R$ siges at være et *maksimalideal* i R, netop hvis det er maksimalt blandt *ægte* idealer, dvs. netop hvis

$$\mathcal{M} \text{ er et \textit{ægte} ideal i } R \quad \text{og} \quad \forall\, \mathcal{I} \text{ \textit{ægte} ideal i } R\colon \quad \mathcal{M} \subseteq \mathcal{I} \quad \Rightarrow \quad \mathcal{M} = \mathcal{I}\,;$$

altså netop hvis der netop er *to* idealer, der indeholder $\mathcal{M}$ (nemlig $\mathcal{M}$ og R). Mængden af maksimalidealer i R betegnes $\operatorname{Max} R$; altså:

$$\operatorname{Max} R = \{\, \mathcal{M} \subset R \mid \mathcal{M} \text{ er et maksimalideal} \,\}\,.$$

Da idealerne i restklasseringen $R/\mathcal{M}$ netop er af formen $\mathcal{I}/\mathcal{M}$, hvor $\mathcal{I}$ er et ideal i R med $\mathcal{I} \supseteq \mathcal{M}$, og da en kommutativ ring er et legeme, netop hvis den har netop *to* idealer, har vi, at der gælder:

$$\mathcal{M} \in \operatorname{Max} R \quad \iff \quad R/\mathcal{M} \text{ er et legeme.}$$

Da ethvert legeme er et integritesområde, har vi:

$$\operatorname{Max} R \quad \subseteq \quad \operatorname{Spec} R\,.$$

(3) **Eksempler.** Hvis L er et legeme, da er $\operatorname{Spec} L = \operatorname{Max} L = \{O\}$.
Da $\mathbb{Z}$ og $\mathbb{C}[x_1]$ er hovedidealområder, har vi

$$\begin{aligned} \operatorname{Max} \mathbb{Z} &= \{\, (p) \mid p \text{ primtal} \,\} &\quad&\text{og}\quad \operatorname{Spec} \mathbb{Z} &&= \{O\} \cup \operatorname{Max} \mathbb{Z}\,;\\ \operatorname{Max} \mathbb{C}[x_1] &= \{\, (p) \mid p \text{ irreducibelt} \,\} &&\text{og}\quad \operatorname{Spec} \mathbb{C}[x_1] &&= \{O\} \cup \operatorname{Max} \mathbb{C}[x_1]\,. \end{aligned}$$

Af diskussionen ovenfor og Restklassemodullemmaet 2(5) følger det næste resultat.

(4) **Restklasseringlemmaet.** *Lad $\mathcal{I}$ være et ideal i R. Idealerne i restklasseringen $R/\mathcal{I}$ er da netop delmængderne $\mathcal{J}/\mathcal{I}$, hvor $\mathcal{J}$ er et ideal i R indeholdende $\mathcal{I}$, og for sådanne er der en isomorfi*

$$(5) \qquad \begin{aligned} (R/\mathcal{I})/(\mathcal{J}/\mathcal{I}) &\xrightarrow{\cong} R/\mathcal{J}\\ \big[\, [r]_{\mathcal{I}} \big]_{\mathcal{J}/\mathcal{I}} &\longmapsto [r]_{\mathcal{J}}\,. \end{aligned}$$

Endvidere gælder:

$$(6) \qquad \begin{aligned} \operatorname{Spec}(R/\mathcal{I}) &= \{\, \mathcal{P}/\mathcal{I} \mid \mathcal{P} \in \operatorname{Spec} R \ \wedge \ \mathcal{P} \supseteq \mathcal{I} \,\}\\ \operatorname{Max}(R/\mathcal{I}) &= \{\, \mathcal{M}/\mathcal{I} \mid \mathcal{M} \in \operatorname{Max} R \ \wedge \ \mathcal{M} \supseteq \mathcal{I} \,\}\,. \quad \square \end{aligned}$$

3. Brøkmoduler

R er en ikke–triviel kommutativ ring.

(1) **Multiplikativt system.** En delmængde $S \subseteq R$ siges at være et *multiplikativt system*, netop hvis der gælder:

$$1 \in S \quad \text{og} \quad \forall\, s, s' \in S\colon\; ss' \in S\,.$$

(2) **Eksempler** på delmængder af R, der er multiplikative systemer.
$\{1\}$.
$U = \{\, u \in R \mid u \text{ er invertibelt} \,\}$.
$V = \{\, v \in R \mid v \text{ er ikke–nuldivisor} \,\}$, sml. 1.2(1).
$X = \{\, x^n \mid n \in \mathbb{N}_0 \,\}$ for $x \in R$ (idet $x^0 = 1$ per definition).
$R \setminus \mathcal{P}$, når $\mathcal{P}$ er et primideal i R.

(3) **Brøkmodul.** Lad S være et multiplikativt system i R, lad M være en R–modul, og betragt produktmængden $M \times S = \{\, (m, s) \mid m \in M \;\wedge\; s \in S \,\}$.

Der defineres en addition $(M \times S) \times (M \times S) \longrightarrow M \times S$ ved $\big((m, s), (m_1, s_1)\big) \mapsto (s_1 m + s m_1, s s_1)$. Denne addition er associativ og kommutativ, $(0, 1)$ er neutralt element, men alle elementer har ikke nødvendigvis et inverst element; additionen opfylder altså gruppebetingelserne (G1), (G2) og (G4), men (G3) mangler.

Ved $\big(r, (m, s)\big) \mapsto (rm, s)$ defineres en R–multiplikation $R \times (M \times S) \longrightarrow M \times S$, som opfylder modulbetingelserne (M1), (M3) samt anden lighed i (M2), mens første lighed i (M2) normalt ikke er opfyldt.

Nu indføres der en relation i mængden $M \times S$ ved

$$(m, s) \sim (m', s') \quad \iff \quad \exists\, u \in S\colon us'm = usm'\,.$$

Dette er en ækvivalensrelation, da den er *refleksiv*, *symmetrisk* og *transitiv:* for alle elementer (m, s), (m', s') og (m'', s'') i $M \times S$ gælder henholdsvis:

(r) $(m, s) \sim (m, s)$;
(s) $(m, s) \sim (m', s') \;\;\Rightarrow\;\; (m', s') \sim (m, s)$;
(t) $(m, s) \sim (m', s') \;\wedge\; (m', s') \sim (m'', s'') \;\;\Rightarrow\;\; (m, s) \sim (m'', s'')$.

Ad (t) bemærkes, at når $us'm = usm'$ og $u's''m' = u's'm''$ med $u, u' \in S$, da har vi:

$$(uu's')s''m = (u's'')(us'm) = (u's'')(usm') = (us)(u's''m') = (us)(u's'm'') = (uu's')sm''$$

og $uu's' \in S$. Endvidere harmonerer ækvivalensrelationen med additionen og R–multiplikationen: for alle $(m, s), (m', s'), (m_1, s_1), (m'_1, s'_1) \in M \times S$ og $r \in R$ gælder:

$$\begin{aligned} (m, s) \sim (m', s') \;\wedge\; (m_1, s_1) \sim (m'_1, s'_1) \quad &\Rightarrow \quad (s_1 m + s m_1, s s_1) \sim (s'_1 m' + s' m'_1, s' s'_1) \\ (m, s) \sim (m', s') \quad &\Rightarrow \quad (rm, s) \sim (rm', s')\,. \end{aligned}$$

(4) **Opgave.** Bevis de to udsagn ovenfor.

Ækvivalensklassen repræsenteret ved (m, s) betegnes m/s, og for $(m, s), (m', s') \in M \times S$ gælder derfor:

$$m/s = m'/s' \iff (m, s) \sim (m', s') \iff \exists\, u \in S \colon us'm = usm'\,;$$

specielt gælder

$$(tm)/(ts) = m/s$$

for $t \in S$ og $(m, s) \in M \times S$. Elementet m/s kaldes en *brøk* med *tæller* m og *nævner* s; brøken kan også skrives med vandret brøkstreg: $\frac{m}{s} = m/s$. Den skrå brøkstreg / må ikke forveksles med modulostregen i udtrykket M/H, når H er en undermodul af M; i disse noter skrives modulostregen aldrig vandret.

Mængden af ækvivalensklasser betegnes $S^{-1}M$; altså:

$$S^{-1}M = \{\, m/s \mid m \in M \;\wedge\; s \in S \,\}\,.$$

Additionen på $M \times S$ inducerer en addition $+\colon S^{-1}M \times S^{-1}M \to S^{-1}M$ givet ved

$$\big(m/s, m_1/s_1\big) \mapsto (m/s) + (m_1/s_1) = (s_1 m + s m_1)/(s s_1)\,,$$

og dette er en korrekt definition, da $\sim$ harmonerer med additionen på $M \times S$. Mængden $S^{-1}M$ opfylder med denne $+$ gruppebetingelserne (G1), (G2) og (G4), da disse allerede er opfyldt for additionen på $M \times S$, og også (G3) ses at være opfyldt:

$$(m/s) + ((-m)/s) = (sm + s(-m))/(ss) = 0/(ss) = 0/1\,.$$

Nu er $(S^{-1}M, +)$ udstyret med struktur som kommutativ gruppe.

R–multiplikationen på $M \times S$ giver en R–multiplikation $R \times S^{-1}M \to S^{-1}M$ ved

$$(r, m/s) \mapsto r(m/s) = (rm)/s\,,$$

og dette er en korrekt definition, da $\sim$ harmonerer med R–multiplikationen på $M \times S$. Modulbetingelserne (M1), (M3) samt anden lighed i (M2) overføres til $S^{-1}M$, og også første lighed i (M2) gælder:

$$\begin{aligned}(r + r')(m/s) &= ((r + r')m)/s = (s(rm) + s(r'm))/(ss) = (rm)/s + (r'm)/s \\ &= r(m/s) + r'(m/s)\,.\end{aligned}$$

Nu er $S^{-1}M$ udstyret med en R–modulstruktur. Afbildningen

$$\rho^S_M \colon M \to S^{-1}M \quad \text{defineret ved} \quad \rho^S_M(m) = m/1 \quad \text{for} \quad m \in M$$

er en R–homomorfi. Når S fremgår af den øvrige sammenhæng, skrives blot ρ_M.

Multiplikationen $S^{-1}R \times S^{-1}R \to S^{-1}R$ givet ved

$$\big((r/s), (r'/s')\big) \mapsto (r/s)(r'/s') = (rr')/(ss')$$

er korrekt defineret og gør den kommutative gruppe $(S^{-1}R, +)$ til en kommutativ ring med $1/1$ som et-element. Ringen $S^{-1}R$ kaldes *brøkringen for* R (og S kaldes nævnermængden).

R–homomorfien $\rho_R\colon R \to S^{-1}R$ er også en ringhomomorfi: $\rho_R(1) = 1/1$ og $\rho_R(rr') = \rho_R(r)\rho_R(r')$ for $r, r' \in R$.

$S^{-1}R$–multiplikationen $S^{-1}R \times S^{-1}M \to S^{-1}M$ givet ved

$$\bigl((r/s), (m/s')\bigr) \mapsto (r/s)(m/s') = (rm)/(ss')$$

er korrekt defineret og gør R–modulen $S^{-1}M$ til en $S^{-1}R$–modul, som kaldes *brøkmodulen for M*.

Bemærk, at $0/1$ er nulelementet i $S^{-1}M$, og at der for $m/s \in S^{-1}M$ gælder:

(1) $$m/s = 0/1 \iff \exists\, u \in S\colon um = 0\,.$$

Endvidere gælder der for nulmodulen O, at brøkmodulen $S^{-1}O$ også er nulmodulen: $S^{-1}O = O$. Også brøkmoduler af ikke–trivielle moduler kan være nul: Betragt ringen $R = \mathbb{Z}$, modulen $M = \mathbb{Z}/(2) = \{\overline{0}, \overline{1}\}$ og det multiplikative system $S = \mathbb{Z} \setminus \{0\}$. Her er $S^{-1}M = O$, da $\overline{1}/v = (2\overline{1})/(2v) = \overline{2}/(2v) = 0/(2v) = 0/1$.

(2) **Opgave.** Lad M være en R–modul, og lad S være et multiplikativt system i R. Bevis:

$$S^{-1}M = O \iff \forall\, m \in M\colon\ \mathrm{Ann}_R(m) \cap S \neq \varnothing\,.$$

(3) **Opgave.** Betragt de to multiplikative systemer:

$$U = \{\, u \in R \mid u \text{ er invertibelt} \,\} \ \text{ og}$$
$$V = \{\, v \in R \mid v \text{ er ikke–nuldivisor} \,\}\,.$$

Bevis, at $\rho_R^U\colon R \to U^{-1}R$ er en isomorfi, og at $\rho_R^V\colon R \to V^{-1}R$ er injektiv.

(4) **Brøklegeme.** Lad R være et integritetsområde, og sæt $V = R\setminus\{0\}$, der jo er et multiplikativt system. Brøkringen $V^{-1}R$ er et legeme (med $(r/v)^{-1} = v/r$ for $r/v \in V^{-1}R$ og $r/v \neq 0/1$), nemlig *brøklegemet* for R, og $\rho_R^V\colon R \to V^{-1}R$ er indlejringen.

Antag nu yderligere, at S er et multiplikativt system i R med $0 \notin S$. Da $S \subseteq V$, er $S^{-1}R$ en delring af brøklegemet $V^{-1}R$, og dermed er $S^{-1}R$ et integritetsområde.

(5) **Induceret homomorfi.** Lad $\varphi\colon M \to N$ være en R–homomorfi. At sætte

$$S^{-1}\varphi\bigl(m/s\bigr) = \varphi(m)/s \ (\in S^{-1}N) \ \text{ for } \ m/s \in S^{-1}M$$

er en korrekt definition af en afbildning $S^{-1}\varphi\colon S^{-1}M \to S^{-1}N$, og denne er en $S^{-1}R$–homomorfi: f.eks. har vi for $r/t \in S^{-1}R$ og $m/s \in S^{-1}M$:

$$\begin{aligned} S^{-1}\varphi\bigl((r/t)(m/s)\bigr) &= S^{-1}\varphi\bigl((rm)/(ts)\bigr) = \varphi(rm)/(ts) = (r\varphi(m))/(ts) = (r/t)(\varphi(m)/s) \\ &= (r/t)S^{-1}\varphi\bigl(m/s\bigr)\,. \end{aligned}$$

(1) **Brøkmodullemmaet.** *Lad M være en R–modul, og lad S være et multiplikativt system i R. Undermodulerne af brøkmodulen $S^{-1}M$ er da netop delmængderne $S^{-1}H$, hvor H er en undermodul af M, og for sådanne er der en $S^{-1}R$–isomorfi:*

(2)
$$\begin{aligned} S^{-1}M/S^{-1}H &\xrightarrow{\cong} S^{-1}(M/H) \\ \big[\,m/s\,\big]_{S^{-1}H} &\longmapsto \big([m]_H\big)/s\,. \end{aligned}$$

Skrevet med vandret brøkstreg bliver definitionen af isomorfien følgende:

$$\Big[\,\frac{m}{s}\,\Big]_{S^{-1}H} \longmapsto \frac{[m]_H}{s}\,.$$

(3) *Bevis.* Hvis H er en undermodul af M, da er delmængden

$$S^{-1}H = \{\, h/s \mid h \in H \;\wedge\; s \in S \,\}$$

en undermodul af $S^{-1}R$–modulen $S^{-1}M$, da undermodulbetingelserne (U1) – (U3) er opfyldt.

Hvis omvendt W er en undermodul af $S^{-1}R$–modulen $S^{-1}M$, og H sættes lig med originalmængden $\rho_M^{-1}(W) = \{\, m \in M \mid m/1 \in W\,\}$, da er H en undermodul af M ifølge 1.7(6). Endvidere gælder $W = S^{-1}H$: for $m/s \in W$ har vi $m \in H$ (da $m/1 = (s/1)(m/s) \in W$), og dermed $m/s \in S^{-1}H$; på den anden side har vi $h/s = (1/s)(h/1) \in W$, når $h \in H$ (thi i så fald gælder $h/1 \in W$).

Restklassehomomorfien $\pi_H\colon M \longrightarrow M/H$ inducerer $S^{-1}\pi_H\colon S^{-1}M \longrightarrow S^{-1}(M/H)$, der er en $S^{-1}R$–homomorfi givet ved $S^{-1}\pi_H\big(m/s\big) = \big([m]_H\big)/s$, og (4) nedenfor giver:

$$\begin{aligned} \operatorname{Ker} S^{-1}\pi_H &= S^{-1}\operatorname{Ker}\pi_H = S^{-1}H\,; \\ \operatorname{Im} S^{-1}\pi_H &= S^{-1}\operatorname{Im}\pi_H \;\; = S^{-1}(M/H)\,. \end{aligned}$$

Isomorfisætningen giver derfor den ønskede isomorfi. $\square$

(4) **Opgave.** Lad S være et multiplikativt system i R, og lad $\varphi\colon M \longrightarrow N$ være en R–homomorfi. Bevis:

$$\operatorname{Ker} S^{-1}\varphi = S^{-1}\operatorname{Ker}\varphi \quad\text{og}\quad \operatorname{Im} S^{-1}\varphi = S^{-1}\operatorname{Im}\varphi\,.$$

(5) **Opgave.** Lad S være et multiplikativt system i R, og lad $M \xrightarrow{\varphi} N \xrightarrow{\psi} P$ være en exakt følge af R–homomorfier. Bevis, at de inducerede $S^{-1}R$–homomorfier $S^{-1}M \xrightarrow{S^{-1}\varphi} S^{-1}N \xrightarrow{S^{-1}\psi} S^{-1}P$ danner en exakt følge.

(6) **Opgave.** Lad $\mathcal{I}$ og $\mathcal{I}'$ være idealer i R, og lad $n \in \mathbb{N}_0$. Bevis de næste to formler.

(7)
$$(S^{-1}\mathcal{I})(S^{-1}\mathcal{I}') = S^{-1}(\mathcal{I}\mathcal{I}')\,;$$

(8)
$$(S^{-1}\mathcal{I})^n = S^{-1}(\mathcal{I}^n)\,.$$

Antag, at $\mathcal{J}$ er yderligere et ideal i R, og at det er indeholdt i både $\mathcal{I}$ og $\mathcal{I}'$. Bevis også de næste formler.

(9)
$$(\mathcal{I}/\mathcal{J})(\mathcal{I}'/\mathcal{J}) = (\mathcal{I}\mathcal{I}' + \mathcal{J})/\mathcal{J}\,;$$

(10)
$$(\mathcal{I}/\mathcal{J})^n = (\mathcal{I}^n + \mathcal{J})/\mathcal{J}\,.$$

(1) **Brøkringlemmaet.** *Lad S være et multiplikativt system i R. Idealerne i brøkringen $S^{-1}R$ er da netop delmængderne $S^{-1}\mathcal{I}$, hvor $\mathcal{I}$ er et ideal i R. Lad nu $\mathcal{I}$ være et ideal i R, og sæt $\widetilde{S} \overset{\text{def}}{=\!=} \{\, [s]_{\mathcal{I}} \mid s \in S \,\}$. Da er $\widetilde{S}$ et multiplikativt system i restklasseringen $R/\mathcal{I}$, og der er en $S^{-1}R$–isomorfi og en ringisomorfi henholdsvis:*

(2)
$$\begin{array}{ccc} S^{-1}R/S^{-1}\mathcal{I} \xrightarrow{\;\cong\;} S^{-1}(R/\mathcal{I}) & \qquad & S^{-1}R/S^{-1}\mathcal{I} \xrightarrow{\;\cong\;} \widetilde{S}^{-1}(R/\mathcal{I}) \\ \big[r/s\big]_{S^{-1}\mathcal{I}} \longmapsto [r]_{\mathcal{I}}/s\,; & & \big[r/s\big]_{S^{-1}\mathcal{I}} \longmapsto [r]_{\mathcal{I}}/[s]_{\mathcal{I}}\,. \end{array}$$

Endvidere gælder:

(3)
$$\operatorname{Spec} S^{-1}R = \{\, S^{-1}\mathcal{P} \mid \mathcal{P} \in \operatorname{Spec} R \;\wedge\; \mathcal{P} \cap S = \varnothing \,\}\,.$$

(4) *Bevis.* Den første påstand (om idealerne i $S^{-1}R$) og den første isomorfi i (2) følger direkte af Brøkmodullemmaet 4(1).

Det er oplagt, at $\widetilde{S}$ er et multiplikativt system i $R/\mathcal{I}$. Tilordningen $r/s \mapsto [r]_{\mathcal{I}}/[s]_{\mathcal{I}}$ giver en korrekt definition af en surjektiv ringhomomorfi $S^{-1}R \to \widetilde{S}^{-1}(R/\mathcal{I})$ med kerne $S^{-1}\mathcal{I}$, så Isomorfisætningen (for ringe) giver den anden isomorfi i (2).

Hvis $\mathcal{P}$ er et primideal i R med $\mathcal{P} \cap S$ tom, da er $\widetilde{S}^{-1}(R/\mathcal{P})$ et integritetsområde ifølge 3(4), så anden isomorfi i (2) giver, at $S^{-1}\mathcal{P}$ er et primideal i $S^{-1}R$.

Hvis omvendt $\mathcal{Q}$ er et primideal i $S^{-1}R$, da har vi for $\mathcal{P} = \rho_R^{-1}(\mathcal{Q})$, som let bevises at være et primideal i R, at $S^{-1}\mathcal{P} = \mathcal{Q}$. $\square$

(5) **Opgave.** Lad S være et multiplikativt system i R, og lad M være en R–modul. For $s \in R$ betragtes multiplikationshomomorfien $s_M \colon M \to M$ (defineret i 1.6(3) ved $s_M(x) = sx$). Endvidere betragtes homomorfien $\rho^S_M \colon M \to S^{-1}M$, $x \mapsto x/1$. Bevis de næste to påstande.

(i) Hvis s_M er injektiv for alle $s \in S$, da er ρ^S_M injektiv.
(s) Hvis s_M er surjektiv for alle $s \in S$, da er ρ^S_M surjektiv.

(6) **Maksimalidealsætningen**[6]**.** *Ringen*[7] *R har (mindst) et maksimalideal; det vil sige, mængden $\operatorname{Max} R$ er ikke tom.*

(7) *Bevis.* (Ikke pensum.) Lad $\mathbb{I}$ betegne mængden af *ægte* idealer i R. Da ringen R er forudsat at være ikke–triviel, er $\mathbb{I}$ ikke den tomme mængde. Vi vil anvende Zorn's Lemma[8] på $\mathbb{I}$ ordnet ved inklusion $\subseteq$, så vi ønsker at vise, at $\mathbb{I}$ herved er *induktivt ordnet*; altså at enhver delmængde $\mathbb{Y} \subseteq \mathbb{I}$, der er *totalt ordnet*[9], har en *majorant*[10]. Lad derfor $\mathbb{Y} \subseteq \mathbb{I}$ være totalt ordnet, og sæt $W \overset{\text{def}}{=\!=} \bigcup_{Y \in \mathbb{Y}}$, som er et ideal, da idealbetingelserne (I1)–(I3) fra 1.2(3) er opfyldt. For f.eks. at indse (I2) antager man $a, a' \in W$, dvs. $a \in Y \in \mathbb{Y}$ og $a' \in Y' \in \mathbb{Y}$, og da $\mathbb{Y}$ er totalt ordnet kan man gerne antage $Y \subseteq Y'$; man har nu $a + a' \in Y' \subseteq W$ som ønsket. Endvidere er W et ægte ideal, thi ellers ville 1 tilhøre det og dermed også et Y fra $\mathbb{Y} \subseteq \mathbb{I}$ i modstrid med definitionen af $\mathbb{I}$. Man har således, at $W \in \mathbb{I}$ er en majorant for $\mathbb{Y}$. Nu da det er bevist, at $\mathbb{I}$ er induktivt ordnet ved $\subseteq$, giver Zorn's Lemma et maksimalt element $\mathcal{M}$ i $\mathbb{I}$, og dette er netop et maksimalideal. $\square$

[6] der kunne have været bragt i ROM 2.
[7] som er **ikke-triviel** ifl. 1.1(4).
[8] *Enhver induktivt ordnet ikke–tom mængde har et maksimalt element.*
[9] dvs. for alle $Y, Y' \in \mathbb{Y}$ gælder $Y \subseteq Y'$ eller $Y' \subseteq Y$.
[10] dvs. en $W \in \mathbb{I}$, så $Y \subseteq W$ for alle $Y \in \mathbb{Y}$.

(1) **Maksimalidealkorollaret.** *Ethvert ægte ideal $\mathcal{I}$ i R er indeholdt i et maksimalideal.*

(2) *Bevis.* Da $\mathcal{I}$ er et ægte ideal, er ringen $R/\mathcal{I}$ ikke triviel, og Maksimalidealsætningen giver et maksimalideal $\mathcal{M}'$ i $R/\mathcal{I}$. Ifølge Restklasseringlemmaet, se 2.7(6), findes $\mathcal{M} \in \operatorname{Max} R$, så $\mathcal{I} \subseteq \mathcal{M}$ og $\mathcal{M}' = \mathcal{M}/\mathcal{I}$. $\square$

(3) **Lokal ring.** Ringen R siges at være *lokal*, netop hvis R har netop ét maksimalideal. Når man vil gøre opmærksom på, at maksimalideal*et* betegnes $\mathcal{M}$, siger man: $(R, \mathcal{M})$ *er lokal.*

$\big(\mathbb{Z}/(4), (2)/(4)\big)$ er lokal.

$\mathbb{Z}/(6)$ er ikke lokal, da både $(2)/(6)$ og $(3)/(6)$ er maksimalidealer.

Hvis $(R, \mathcal{M})$ er lokal, da gælder for ethvert ideal $\mathcal{I}$ i R og ethvert $r \in R$, at:

(4) $$\mathcal{I} \ \text{ er et ægte ideal} \quad \Rightarrow \quad \mathcal{I} \subseteq \mathcal{M}$$

(5) $$r \ \text{ er ikke invertibelt} \quad \Rightarrow \quad r \in \mathcal{M}\,.$$

(6) **Lemma.** *Idet $U = \{\, u \in R \mid u \text{ er invertibelt}\}$, gælder:*

$$R \ \text{ er lokal} \quad \Longleftrightarrow \quad R \setminus U \ \text{ er et ideal.}$$

I bekræftende fald er $R \setminus U$ maksimalidealet i R.

(7) *Bevis.* Først bemærkes, at der gælder:

(8) $$\mathcal{I} \ \text{ er et ægte ideal} \quad \Rightarrow \quad \mathcal{I} \cap U = \varnothing\,.$$

For at bevise "$\Leftarrow$" antages, at $\mathcal{M} \overset{\text{def}}{=} R \setminus U$ er et ideal. Det er da et maksimalideal, thi hvis $\mathcal{I}$ er et ægte ideal, da er $\mathcal{I} \cap U = \varnothing$ ifølge (8), og dermed $\mathcal{I} \subseteq R \setminus U = \mathcal{M}$.

Omvendt, når $(R, \mathcal{M})$ er lokal, da er $R \setminus U = \mathcal{M}$, idet inklusionen $\subseteq$ er (5), og $\supseteq$ er (8); og $R \setminus U$ er derfor et ideal.

Biimplikationen er nu bevist, og det blev den sidste påstand også undervejs. $\square$

(9) **Opgave.** Afgør, om $\mathbb{C}[x_1, x_2]$ er en lokal ring (sml. f.eks. PAK 6.1(4)). Er $\mathbb{C}[x_1]$ lokal? Er $\mathbb{C}[x_1, x_2, x_3]$?

(10) **Lokalisation.** Lad $\mathcal{P}$ være et primideal i R, dvs. $\mathcal{P} \in \operatorname{Spec} R$, og lad M være en R–modul. Mængden $R \setminus \mathcal{P}$ er da et multiplikativt system, og man sætter:

$$M_{\mathcal{P}} \overset{\text{def}}{=} (R \setminus \mathcal{P})^{-1} M\,.$$

Specielt betegner $R_{\mathcal{P}}$ brøkringen $(R \setminus \mathcal{P})^{-1} R$, som er en lokal ring ifølge (1) nedenfor; den kaldes R *lokaliseret i* $\mathcal{P}$, og $R_{\mathcal{P}}$–modulen $M_{\mathcal{P}}$ kaldes M *lokaliseret i* $\mathcal{P}$.

(11) **Lemma.** *For $\mathcal{P} \in \operatorname{Spec} R$ og $r/s \in R_{\mathcal{P}}$ med $r \in R, s \in R \setminus \mathcal{P}$ gælder:*

$$r/s \ \text{ er invertibelt i } \ R_{\mathcal{P}} \quad \Longleftrightarrow \quad r \notin \mathcal{P}\,.$$

(12) *Bevis.* Implikationen "$\Leftarrow$" er oplagt: for $r \notin \mathcal{P}$ har vi $s/r \in R_{\mathcal{P}}$ og $(s/r)(r/s) = (rs)/(rs) = 1/1$, som er et-elementet i $R_{\mathcal{P}}$.

Antag omvendt, at $a/t \in R_{\mathcal{P}}$ med $a \in R,\ t \notin \mathcal{P}$ og $(a/t)(r/s) = 1/1$. Det sidste giver $u \notin \mathcal{P}$, så $uar = uts$. Da $u, t, s \notin \mathcal{P}$ og $\mathcal{P} \in \operatorname{Spec} R$, har vi $uts \notin \mathcal{P}$, og dermed specielt $r \notin \mathcal{P}$. $\square$

(1) **Lemma.** *Brøkringen $R_{\mathcal{P}}$ er lokal med maksimalidealet*

$$\mathcal{P}_{\mathcal{P}} = \{\, a/s \mid a \in \mathcal{P} \;\wedge\; s \notin \mathcal{P} \,\}\,.$$

(2) *Bevis.* Sammenhold 6(11) med 6(6). □

(3) **Opgave.** Lad S være et multiplikativt system i R, og lad $\mathcal{P} \in \operatorname{Spec} R$ være så $\mathcal{P} \cap S = \varnothing$. Bevis, at der for $r/s \in S^{-1}R$ med $r \in R,\ s \in S$ gælder:

$$r/s \in S^{-1}\mathcal{P} \quad\Longleftrightarrow\quad r \in \mathcal{P}\,. \tag{4}$$

Etablér en isomorfi:

$$(S^{-1}R)_{S^{-1}\mathcal{P}} \xrightarrow{\cong} R_{\mathcal{P}}\,. \tag{5}$$

(6) **Lemma.** *Lad X være en R–modul, så der findes $\mathcal{M} \in \operatorname{Max} R$ med $\mathcal{M} \subseteq \operatorname{Ann} X$. Der er da en R–isomorfi:*

$$\rho_X \colon X \xrightarrow{\cong} X_{\mathcal{M}}\,.$$

(7) *Bevis.* Ifølge opgave 5(5) er det nok at bevise, at s_X er en isomorfi for alle $s \in R\setminus\mathcal{M}$. For sådant s er maksimalidealet $\mathcal{M}$ en ægte delmængde af idealet $\mathcal{M}+(s)$, og sidstnævnte ideal er derfor ikke ægte; altså $\mathcal{M} + (s) = R$. Vælg $r \in R$ og $m \in \mathcal{M}$, så $rs + m = 1$. Heraf følger, at homomorfierne r_X og s_X er hinandens inverse, idet vi for $x \in X$ har:

$$r_X(s_X(x)) = rsx = (rs + m)x = 1x = x \quad\text{og}\quad s_X(r_X(x)) = srx = rsx = x\,,$$

hvor anden lighed skyldes, at $m \in \operatorname{Ann}(x)$. □

(8) **Opgave.** Lad X være en R–modul, så der findes $\mathcal{M} \in \operatorname{Max} R$ og $n \in \mathbb{N}$ med $\mathcal{M}^n$ indeholdt i $\operatorname{Ann} X$. Bevis, at der er en R–isomorfi $\rho_X \colon X \xrightarrow{\cong} X_{\mathcal{M}}$. (Gå frem som i beviset (7). Binomialformlen giver: $1 = 1^n = (rs + m)^n = \sum_{i=0}^{n} \binom{n}{i} (rs)^i m^{n-i} = as + m^n$ for $a \overset{\text{def}}{=} \sum_{i=1}^{n} \binom{n}{i} r^i s^{i-1} m^{n-i}$. Slut heraf, at homomorfierne a_X og s_X er hinandens inverse.)

(9) **Opgave.** Bevis, at $S^{-1}(\mathcal{I}+\mathcal{J}) = (S^{-1}\mathcal{I})+(S^{-1}\mathcal{J})$ og $S^{-1}(\mathcal{I}\cap\mathcal{J}) = (S^{-1}\mathcal{I})\cap(S^{-1}\mathcal{J})$, når $\mathcal{I}$ og $\mathcal{J}$ er idealer og S er et multiplikativt system i R.

(10) **Opgave.** Bevis, at en R–modulen M er triviel, hvis $M_{\mathcal{M}} = 0$ for alle $\mathcal{M} \in \operatorname{Max} R$.
Bevis, at hvis $\mathcal{I}$ og $\mathcal{J}$ er idealer i R med $\mathcal{I}_{\mathcal{M}} = \mathcal{J}_{\mathcal{M}}$ for alle $\mathcal{M} \in \operatorname{Max} R$, da er $\mathcal{I} = \mathcal{J}$ (Betragt f.eks. R–modulen $(\mathcal{I} + \mathcal{J})/\mathcal{I}$).

(11) **Opgave.** Lad $\varphi\colon V \to H$ være en R–homomorfi, og betragt den inducerede $R_{\mathcal{M}}$–homomorfi $\varphi_{\mathcal{M}}\colon V_{\mathcal{M}} \to H_{\mathcal{M}}$ for $\mathcal{M} \in \operatorname{Max} R$. Bevis (ved også at benytte 4(4)):

$$\varphi \text{ injektiv} \quad\Longleftrightarrow\quad \forall\, \mathcal{M} \in \operatorname{Max} R\colon \varphi_{\mathcal{M}} \text{ injektiv}; \tag{12}$$

$$\varphi \text{ surjektiv} \quad\Longleftrightarrow\quad \forall\, \mathcal{M} \in \operatorname{Max} R\colon \varphi_{\mathcal{M}} \text{ surjektiv}. \tag{13}$$

(14) **Opgave.** Formulér og bevis: $S^{-1}(M_1 \oplus \cdots \oplus M_n) \cong (S^{-1}M_1) \oplus \cdots \oplus (S^{-1}M_n)\,.$

(1) **Opgave.** Bestem for undermoduler H og K af R–modul M tre homomorfier ι, φ og π, så der er en exakt følge:

$$0 \longrightarrow H \xrightarrow{\iota} H + K \xrightarrow{\varphi} M/H \cap K \xrightarrow{\pi} M/K \longrightarrow 0\,.$$

(2) **Opgave.** Bestem for undermoduler H og K af R–modul M tre homomorfier ι, φ og π, så der er en exakt følge:

$$0 \longrightarrow H \cap K \xrightarrow{\iota} H \xrightarrow{\varphi} M/K \xrightarrow{\pi} M/(H + K) \longrightarrow 0\,.$$

(3) **Opgave.** Lad a være et element i ringen R, og betragt for R–modul M undermodulen $\underline{M} = \{\, m \in M \mid am = 0\,\}$. [At dette er en undermodul af M ønskes ikke uddybet.]

(a) Begrund, at der for enhver homomorfi $\varphi\colon M \longrightarrow N$ gælder $\varphi(\underline{M}) \subseteq \underline{N}$.

Lad $\underline{\varphi}\colon \underline{M} \longrightarrow \underline{N}$ betegne restriktionen.

(b) Bevis, at enhver exakt følge $0 \longrightarrow K \xrightarrow{\kappa} L \xrightarrow{\lambda} P$ af R–moduler inducerer en exakt følge $0 \longrightarrow \underline{K} \xrightarrow{\underline{\kappa}} \underline{L} \xrightarrow{\underline{\lambda}} \underline{P}\,$.

4. Noetherske ringe

$\boxed{R \text{ er en ikke–triviel kommutativ ring.}}$

(1) **Emmy Noether** (1882–1935), tysk, fra 1933 bosat i USA, datter af Max Noether, som optræder i PAK 9. Emmy Noether var en foregangsperson inden for abstrakt ringteori.

(2) **Noetherske ringe.** Man siger, at ringen R er *noethersk*, netop hvis ethvert ideal i R er endeligt frembragt.

Alle legemer er noetherske. Ringene $\mathbb{Z}$ og $\mathbb{C}[x_1]$ er noetherske; alle PID (dvs. hovedidealområder) er noetherske. Senere skal vi i 3(2) se, at (f.eks.) $\mathbb{C}[x_1, x_2]$ og $\mathbb{C}[x_1, x_2, x_3]$ er noetherske, og i 3(3)&(5) at den lokale ring $\mathcal{O}_P(G)$ i et punkt på en (affin eller projektiv) kurve G er noethersk.

(3) **Sætning.** *For ringen R er følgende udsagn ensbetydende.*

(*i*) *R er noethersk.*

(*ii*) *Enhver stigende kæde $\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \cdots \subseteq \mathcal{I}_m \subseteq \mathcal{I}_{m+1} \subseteq \cdots$ af idealer i R er sluttelig stationær, dvs. der findes $m_0 \in \mathbb{N}$, så $\mathcal{I}_{m_0} = \mathcal{I}_{m_0+i}$ for alle $i \in \mathbb{N}_0$.*

(*iii*) *Enhver ikke–tom delmængde $\mathbb{I}$ af idealer i R har et maksimalt element $\mathcal{I}_0$, dvs. for alle $\mathcal{I} \in \mathbb{I}$ med $\mathcal{I}_0 \subseteq \mathcal{I}$ gælder $\mathcal{I}_0 = \mathcal{I}$.*

(4) *Bevis.* "(*i*) $\Rightarrow$ (*ii*)": Lad $\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \cdots \subseteq \mathcal{I}_m \subseteq \mathcal{I}_{m+1} \subseteq \cdots$ være en stigende kæde af idealer i R, og sæt $\mathcal{I} \overset{\text{def}}{=} \cup_{m\in\mathbb{N}} \mathcal{I}_m$, som let ses at opfylde idealbetingelserne (I1) – (I3) i 1.2(3) og derfor er et ideal i R. Forudsætningen giver, at $\mathcal{I}$ er endeligt frembragt: $\mathcal{I} = (a_1, \ldots, a_n)$ med $a_1, \ldots, a_n \in \mathcal{I}$. Til hvert a_i findes et $m_i \in \mathbb{N}$ med $a_i \in \mathcal{I}_{m_i}$. Lad m_0 være det største blandt $m_1, \ldots, m_n$, og bemærk $a_1, \ldots, a_n \in \mathcal{I}_{m_0}$ og dermed $\mathcal{I} = (a_1, \ldots, a_n) \subseteq \mathcal{I}_{m_0} \subseteq \mathcal{I}$. Heraf følger $\mathcal{I}_{m_0} = \mathcal{I}$, og derfor giver $\mathcal{I}_{m_0} \subseteq \mathcal{I}_{m_0+i} \subseteq \mathcal{I}$ for $i \in \mathbb{N}_0$, at $\mathcal{I}_{m_0} = \mathcal{I}_{m_0+i}$ for alle $i \in \mathbb{N}_0$.

"(*ii*) $\Rightarrow$ (*iii*)": Antag, at $\mathbb{I}$ er en ikke-tom mængde af idealer i R, og at $\mathbb{I}$ *ikke har maksimalt element.* Enhver endelig strengt[11] stigende kæde $\mathcal{I}_1 \subset \cdots \subset \mathcal{I}_m$ af elementer fra $\mathbb{I}$ kan – da $\mathcal{I}_m$ ikke er maksimalt i $\mathbb{I}$ – udvides til kæde $\mathcal{I}_1 \subset \cdots \subset \mathcal{I}_m \subset \mathcal{I}_{m+1}$ med også $\mathcal{I}_{m+1}$ i $\mathbb{I}$. Dette viser, at der findes en uendelig strengt stigende kæde $\mathcal{I}_1 \subset \cdots \subset \mathcal{I}_m \subset \mathcal{I}_{m+1} \subset \cdots$ i modstrid med (*ii*).

"(*iii*) $\Rightarrow$ (*i*)": Antag, at $\mathcal{I}$ er et ideal, der *ikke er endeligt frembragt* (og dermed specielt $\mathcal{I} \neq 0$). Vi kan derfor vælge $a_1, a_2, \ldots, a_m, \ldots$ i $\mathcal{I}$, så $a_{m+1} \notin (a_1, \ldots, a_m)$ for alle $m \in \mathbb{N}_0$ (idet $(a_1, \ldots, a_m) \overset{\text{def}}{=} 0$ for $m = 0$). Mængden $\mathbb{I} \overset{\text{def}}{=} \{(a_1), (a_1, a_2), \ldots, (a_1, \ldots, a_m), \ldots\}$ af idealer i R er ikke-tom og har ikke et maksimalt element i modstrid med (*iii*). $\square$

(5) **Opgave.** Begrund, at mængden $R \overset{\text{def}}{=} \{\, f \in \mathbb{C}[x_1] \mid f(o) \in \mathbb{Z}\,\}$ af polynomier $f \in \mathbb{C}[x_1]$ med helt konstantled er en delring af $\mathbb{C}[x_1]$. Konstruér i R et ideal $\mathcal{I}$, der ikke er endeligt frembragt og en uendelig strengt stigende kæde af idealer.

(6) **Opgave.** Lad X være en ikke–tom mængde, og lad $\mathbb{C}^X$ være mængden af funktioner $f\colon X \to \mathbb{C}$. Begrund, at $\mathbb{C}^X$ er en ring: for $f, g \in \mathbb{C}^X$ defineres $f+g, fg \in \mathbb{C}^X$ ved henholdsvis $(f+g)(x) = f(x) + g(x)$ og $(fg)(x) = f(x)g(x)$ for $x \in X$. Bevis for delmængde $Y \subseteq X$, at $\mathcal{I}_Y \overset{\text{def}}{=} \{\, f \in \mathbb{C}^X \mid \forall y \in Y : f(y) = 0\,\}$ er et ideal, og at $\mathcal{I}_Y \subset \mathcal{I}_{Y'}$, når $Y \supset Y'$. Bevis, at $\mathbb{C}^X$ ikke er noethersk, når mængden X er uendelig.

[11] I disse noter betegner $\subset$ *streng* inklusion; altså: $X \subset Y \iff X \subseteq Y \wedge X \neq Y$.

(1) **Sætning.** *Hvis R er noethersk, og $\mathcal{I}$ er et ideal i R, da er restklasseringen $R/\mathcal{I}$ noethersk.*

(2) *Bevis.* Lad $\mathcal{J}'$ være et ideal i $R/\mathcal{I}$, og vælg ideal $\mathcal{J}$ i R med $\mathcal{J} \supseteq \mathcal{I}$ og $\mathcal{J}/\mathcal{I} = \mathcal{J}'$. Da R er noethersk findes $a_1, \dots, a_n \in R$ med $\mathcal{J} = R(a_1, \dots, a_n)$. Heraf følger $\mathcal{J}' = \mathcal{J}/\mathcal{I} = (R/\mathcal{I})([a_1]_\mathcal{I}, \dots, [a_n]_\mathcal{I})$, som er endeligt frembragt. □

(3) **Sætning.** *Hvis R er noethersk, og S er et multiplikativt system i R, da er brøkringen $S^{-1}R$ noethersk.*

(4) *Bevis.* Lad $\mathcal{J}'$ være et ideal i $S^{-1}R$, og vælg ideal $\mathcal{J}$ i R med $S^{-1}\mathcal{J} = \mathcal{J}'$. Da R er noethersk findes $a_1, \dots, a_n \in R$ med $\mathcal{J} = R(a_1, \dots, a_n)$. Heraf følger $\mathcal{J}' = S^{-1}\mathcal{J} = S^{-1}R(a_1/1, \dots, a_n/1)$, som er endeligt frembragt. □

(5) **Hilbert's Basissætning.** *Hvis R er noethersk, da er $R[x]$ noethersk.*

(6) *Bevis.* For ethvert ideal $\mathcal{I}$ i $R[x]$ og ethvert $n \in \mathbb{N}_0$ lader vi $\mathcal{I}^{(n)}$ betegne mængden af n'te grad koefficienter til polynomier $f \in \mathcal{I}$ med $\deg f \le n$; altså:

$$\mathcal{I}^{(n)} \overset{\text{def}}{=\!=} \{\, a_n \in R \mid \exists\, a_0, a_1, \dots, a_{n-1} \in R\colon a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \in \mathcal{I} \,\},$$

specielt $\mathcal{I}^{(0)} = \mathcal{I} \cap R$, mængden af konstanter i $\mathcal{I}$. Idealbetingelserne (I1) – (I3) er opfyldt, så $\mathcal{I}^{(n)}$ er et ideal i R. Da der gælder $f \in \mathcal{I} \;\Rightarrow\; xf \in \mathcal{I}$, har vi kæden:

(7) $$\mathcal{I}^{(0)} \subseteq \mathcal{I}^{(1)} \subseteq \cdots \subseteq \mathcal{I}^{(n)} \subseteq \mathcal{I}^{(n+1)} \subseteq \cdots.$$

For alle idealer $\mathcal{I}$ og $\mathcal{J}$ i $R[x]$ gælder:

(8) $$\mathcal{I} \subseteq \mathcal{J} \quad\Rightarrow\quad \big(\forall\, n \in \mathbb{N}_0\colon \mathcal{I}^{(n)} \subseteq \mathcal{J}^{(n)}\big)\,;$$

(9) $$\mathcal{I} \subseteq \mathcal{J} \;\;\wedge\;\; \big(\forall\, n \in \mathbb{N}_0\colon \mathcal{I}^{(n)} = \mathcal{J}^{(n)}\big) \quad\Rightarrow\quad \mathcal{I} = \mathcal{J}\,.$$

Her er (8) oplagt udfra definitionen.

For at indse (9) antages $f \neq 0$ at tilhøre $\mathcal{J}$, og vi beviser $f \in \mathcal{I}$ ved induktion efter $n \overset{\text{def}}{=\!=} \deg f$. Induktionsstart $n = 0$: $f \in \mathcal{J} \cap R = \mathcal{J}^{(0)} = \mathcal{I}^{(0)} = \mathcal{I} \cap R \subseteq \mathcal{I}$.

Induktionstrin $n > 0$: Idet $f = a_0 + \cdots + a_{n-1}x^{n-1} + a_nx^n$ med $a_0, \dots, a_{n-1}, a_n \in R$, har vi $a_n \in \mathcal{J}^{(n)} = \mathcal{I}^{(n)}$, og der findes derfor elementer $b_0, \dots, b_{n-1}$ i R, således at polynomiet $g \overset{\text{def}}{=\!=} b_0 + \cdots + b_{n-1}x^{n-1} + a_nx^n$ tilhører $\mathcal{I}$ ($\subseteq \mathcal{J}$). Da $f - g \in \mathcal{J}$ og $\deg(f - g) < n$, giver induktionsantagelsen $f - g \in \mathcal{I}$, og heraf fås $f = (f - g) + g \in \mathcal{I}$. Hermed er (9) bevist.

For at bevise, at $R[x]$ er noethersk, tager vi udgangspunkt i (*ii*) i sætning 1(3) og lader

$$\mathcal{I}_0 \subseteq \mathcal{I}_1 \subseteq \cdots \subseteq \mathcal{I}_m \subseteq \cdots$$

være en stigende kæde af idealer i $R[x]$, og sætter $\mathcal{I}_m^{(n)} \overset{\text{def}}{=\!=} (\mathcal{I}_m)^{(n)}$ for $m, n \in \mathbb{N}_0$. Betragt det næste diagram af kæder af idealer i R:

$$\begin{array}{ccccccccccc}
\mathcal{I}_0^{(0)} & \subseteq & \mathcal{I}_1^{(0)} & \subseteq & \cdots & \subseteq & \mathcal{I}_m^{(0)} & \subseteq & \cdots & \subseteq & \mathcal{I}_{m+i}^{(0)} & \subseteq & \cdots \\
\cap\!| & & \cap\!| & & & & \cap\!| & & & & \cap\!| \\
\mathcal{I}_0^{(1)} & \subseteq & \mathcal{I}_1^{(1)} & \subseteq & \cdots & \subseteq & \mathcal{I}_m^{(1)} & \subseteq & \cdots & \subseteq & \mathcal{I}_{m+i}^{(1)} & \subseteq & \cdots \\
\cap\!| & & \cap\!| & & & & \cap\!| & & & & \cap\!| \\
\vdots & & \vdots & & & & \vdots & & & & \vdots \\
\cap\!| & & \cap\!| & & & & \cap\!| & & & & \cap\!| \\
\mathcal{I}_0^{(m)} & \subseteq & \mathcal{I}_1^{(m)} & \subseteq & \cdots & \subseteq & \mathcal{I}_m^{(m)} & \subseteq & \cdots & \subseteq & \mathcal{I}_{m+i}^{(m)} & \subseteq & \cdots \\
\cap\!| & & \cap\!| & & & & \cap\!| & & & & \cap\!| \\
\vdots & & \vdots & & & & \vdots & & & & \vdots \\
\cap\!| & & \cap\!| & & & & \cap\!| & & & & \cap\!| \\
\mathcal{I}_0^{(m+i)} & \subseteq & \mathcal{I}_1^{(m+i)} & \subseteq & \cdots & \subseteq & \mathcal{I}_m^{(m+i)} & \subseteq & \cdots & \subseteq & \mathcal{I}_{m+i}^{(m+i)} & \subseteq & \cdots \\
\cap\!| & & \cap\!| & & & & \cap\!| & & & & \cap\!| \\
\vdots & & \vdots & & & & \vdots & & & & \vdots
\end{array}$$

hvor søjlerne kommer fra 2(7) og rækkerne fra 2(8).

Da R er noethersk, giver diagonalen

$$\mathcal{I}_0^{(0)} \subseteq \mathcal{I}_1^{(1)} \subseteq \cdots \subseteq \mathcal{I}_m^{(m)} \subseteq \cdots \subseteq \mathcal{I}_{m+i}^{(m+i)} \subseteq \cdots,$$

at der findes $m_0 \in \mathbb{N}_0$ med $\mathcal{I}_{m_0}^{(m_0)} = \mathcal{I}_{m_0+i}^{(m_0+i)}$ for alle $i \in \mathbb{N}_0$, og dette medfører, at der for alle $j \in \mathbb{N}_0$ gælder $\mathcal{I}_{m_0}^{(m_0+j)} = \mathcal{I}_{m_0+i}^{(m_0+j)}$ for alle $i \in \mathbb{N}_0$.

Betragt nu enhver af de m_0 første rækker: for $h \in \{1, \ldots, m_0\}$ vælges $m_h \in \mathbb{N}_0$ med $\mathcal{I}_{m_h}^{(h-1)} = \mathcal{I}_{m_h+i}^{(h-1)}$ for alle $i \in \mathbb{N}_0$. Lad nu m betegne det største blandt tallene $m_0, m_1, \ldots, m_{m_0}$.

For alle $n \in \mathbb{N}_0$ har vi nu $\mathcal{I}_m^{(n)} = \mathcal{I}_{m+i}^{(n)}$ for alle $i \in \mathbb{N}_0$, og ifølge 2(9) derfor også $\mathcal{I}_m = \mathcal{I}_{m+i}$ for alle $i \in \mathbb{N}_0$ – som ønsket. □

Ved induktion efter n fås:

(1) **Korollar.** *Hvis R er noethersk, da er $R[x_1, \ldots, x_n]$ noethersk.* □

(2) **Korollar.** *Ringene $\mathbb{C}[x_1, x_2]$ og $\mathbb{C}[x_1, x_2, x_3]$ er noetherske.* □

(3) **Korollar.** *Lad P være et punkt i $\mathbb{A}^2_{\mathbb{C}}$. Da er $\mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})$ noethersk, og for enhver affin kurve F er også $\mathcal{O}_P(F)$ noethersk.*

(4) *Bevis.* Første påstand følger af (2) og 2(3), og den anden følger af den første og 2(1). □

(5) **Korollar.** *Lad P være et punkt i $\mathbb{P}^2_{\mathbb{C}}$. Da er $\mathcal{O}_P(\mathbb{P}^2_{\mathbb{C}})$ noethersk, og for enhver projektiv kurve C er også $\mathcal{O}_P(C)$ noethersk.*

(6) *Bevis.* Vælg et projektivt koordinatskift $\alpha\colon \mathbb{P}^2_{\mathbb{C}} \longrightarrow \mathbb{P}^2_{\mathbb{C}}$, så $\alpha(P)$ tilhører $\mathbb{A}^2_{\mathbb{C}}$. Påstandene følger nu af (3) i lys af PAK 6.4(4)&6.3(3). □

(7) **Noetherske moduler.** Man siger, at R–modulen M er *noethersk*, netop hvis enhver undermodul K af M er endeligt frembragt.

(1) **Opgave.** Lad M være en R–modul med en undermodul N. Bevis, at der gælder:

$$M \text{ er noethersk} \iff N \text{ og } M/N \text{ er noetherske.}$$

(2) **Opgave.** Bevis, at hvis M og M' er isomorfe R–moduler, da gælder:

$$M \text{ er noethersk} \iff M' \text{ er noethersk.}$$

(3) **Opgave.** Lad $0 \to L \to M \to P \to 0$ være en exakt følge af R–homomorfier. Bevis, at der gælder:

$$M \text{ er noethersk} \iff L \text{ og } P \text{ er noetherske.}$$

(4) **Opgave.** Lad $M_1, \dots, M_v$ være R–moduler og $v > 1$. Etablér exakt følge

$$0 \to M_1 \oplus \cdots \oplus M_{v-1} \to M_1 \oplus \cdots \oplus M_{v-1} \oplus M_v \to M_v \to 0\,.$$

Bevis, at der gælder:

$$M_1 \oplus \cdots \oplus M_v \text{ er noethersk} \iff M_1, \dots, M_v \text{ er noetherske.}$$

(5) **Opgave.** Lad M være en R–modul.

For $v \in \mathbb{N}$ betegner M^v den direkte sum af v kopier af M, dvs. $M^v = M_1 \oplus \cdots \oplus M_v$ med $M_i = M$ for alle i. Antag, at M er endeligt frembragt af $m_1, \dots, m_v \in M$; altså $M = Rm_1 + \cdots + Rm_v$. Bevis, at afbildningen $\varphi\colon R \to M^v$ defineret ved $\varphi(r) = (rm_1, \dots, rm_v)$ for $r \in R$ er en R–homomorfi med $\operatorname{Ker}\varphi = \operatorname{Ann}_R M$. Bevis, at R–modulen $R/\operatorname{Ann}_R M$ er isomorf med en undermodul af M^v

Bevis, at hvis M er en noethersk R–modul, da er $R/\operatorname{Ann}_R M$ en noethersk ring.

(6) **Opgave.** Lad $(R, \mathcal{M})$ være en lokal ring.

Bevis for *ægte* ideal $\mathcal{I}$ i R, at produktet $\mathcal{M}(R/\mathcal{I})$ af idealet $\mathcal{M}$ og R–modulen $R/\mathcal{I}$ er lig med $(\mathcal{M}+\mathcal{I})/\mathcal{I}$, og at $\mathcal{M}(R/\mathcal{I}) \subset R/\mathcal{I}$.

Bevis, at hvis M er en R–modul, så der findes *ægte* ideal $\mathcal{I}$ i R og *surjektiv* R–homomorfi $\varphi\colon M \to R/\mathcal{I}$, da gælder $\mathcal{M}M \subset M$. (Bevis og udnyt f.eks., at $\varphi(\mathcal{M}M) = \mathcal{M}\varphi(M)$.)

Bevis, at hvis M er en *endeligt frembragt ikke–triviel* R–modul, da findes der *ægte* ideal $\mathcal{I}$ i R og *surjektiv* R–homomorfi $\varphi\colon M \to R/\mathcal{I}$. (Bevis og benyt f.eks., at hvis $M = Rm_1 + \cdots + Rm_v$ med $v > 1$ og $N \overset{\text{def}}{=} Rm_1 + \cdots + Rm_{v-1}$, da er M/N cyklisk, sml. nu Sætning om cykliske moduler 2.3(2).)

Bevis de næste to resultater.

(7) **Nakayama's Lemma.** *Hvis $(R, \mathcal{M})$ er en lokal ring, og M er en R–modul, da gælder:*

$$M \ \textit{endeligt frembragt} \ \wedge \ \mathcal{M}M = M \quad \Rightarrow \quad M = 0\,. \quad \square$$

(8) **Nakayama's Korollar.** *Hvis $(R, \mathcal{M})$ er en lokal ring, og M er en R–modul med undermodul N, da gælder:*

$$M/N \ \textit{endeligt frembragt} \ \wedge \ N + \mathcal{M}M = M \quad \Rightarrow \quad N = M\,. \quad \square$$

(1) **Opgave.** Bevis, at hvis M er en endeligt frembragt modul over en noethersk ring R, da er M en noethersk R–modul. (Benyt f.eks. induktion efter antallet v af frembringere for M og sml. sidste vink i opgave 4(6).)

(2) **Euklidiske integritetsområder.** Et integritetsområde R kaldes *euklidisk*, netop hvis der findes en funktion $\sigma\colon R\setminus\{0\}\longrightarrow\mathbb{N}_0$, så der gælder *"division med rest":*

$$\forall\, a\in R\setminus\{0\}\,\forall\, b\in R\,\exists\, q,r\in R\colon b=aq+r \;\wedge\; \big(r=0\,\vee\,\sigma(r)<\sigma(a)\big)\,,$$

De hele tals ring $\mathbb{Z}$ er euklidisk med $\sigma(a)\overset{\text{def}}{=\!=}|a|$ (numerisk værdi).

Polynomiumsringen $\mathbb{C}[x]$ er euklidisk med $\sigma(a)\overset{\text{def}}{=\!=}\deg a$.

(3) **PID** er forkortelse for *Principal Ideal Domain*, dvs. for *hovedidealområde*. Det er kendt fra Matematik 2AL, at der gælder: R euklidisk $\Rightarrow$ R PID, mens "$\Leftarrow$" ikke gælder.

(4) **UFD** er forkortelse for *Unique Factorization Domain*, dvs. for *faktorielt integritetsområde*. Fra Matematik 2AL vides, at der gælder: R PID $\Rightarrow$ R UFD, mens "$\Leftarrow$" ikke gælder.

(5) **DVR** er forkortelse for *Discrete Valuation Ring*, som er en anden betegnelse for et PID, der er en *lokal* ring. (Da en DVR således – per definition – er et integritetsområde, ville DVD – svarende til Discrete Valuation Domain – have været en bedre betegnelse.) Antag nu, at R er en DVR med maksimalidealet (t), og at R ikke er et legeme. Ethvert ikke–invertibelt element har formen rt med $r\in R$, og det er irreducibelt, netop hvis r er invertibelt. Pånær associering (sml. PAK 3.4(7)) er der således netop et irreducibelt element i R, nemlig t. Da R er UFD, findes der til ethvert $a\in R\setminus\{0\}$ netop ét $\nu(a)\in\mathbb{N}_0$ og netop ét invertibelt $u\in R$, så $a=ut^{\nu(a)}$. Idet $B=R_0$ er brøklegemet, kan funktionen $\nu\colon R\setminus\{0\}\longrightarrow\mathbb{N}_0$ entydigt udvides til en funktion $\nu\colon B\longrightarrow\mathbb{Z}\cup\{\infty\}$ med $\nu(a/s)=\nu(a)-\nu(s)$ for $a/s\in B\setminus\{0\}$ og $\nu(0)=\infty$. Der gælder for alle $b,b'\in B$:

$$\nu(b+b')\geq\min\{\nu(b),\nu(b')\}\quad\text{og}\quad\nu(bb')=\nu(b)+\nu(b')\,,$$

og ν kaldes en *diskret valuation*. For $a=ut^{\nu(a)}, b=vt^{\nu(b)}\in R$ er $b=aq+r$ for $(q,r)=(vu^{-1}t^{\nu(b)-\nu(a)},0)$, når $\nu(b)\geq\nu(a)$, og for $(q,r)=(0,b)$, når $\nu(b)<\nu(a)$. Der gælder altså: R DVR $\Rightarrow$ R euklidisk.

(6) **Lemma.** *Hvis $(R,\mathcal{M})$ er et lokalt, noethersk integritetsområde, hvori $\mathcal{M}$ er et hovedideal, da er R en DVR.*

(7) *Bevis.* Antag $\mathcal{M}=(t)$, lad $\mathbb{I}$ betegne mængden af idealer i R, der ikke er hovedidealer, antag $\mathbb{I}\neq\varnothing$, og søg modstrid. Ifølge 1(3) har $\mathbb{I}$ et maksimalt element $\mathcal{I}_0$. Sæt $\mathcal{J}\overset{\text{def}}{=\!=}\{\,r\in R\mid tr\in\mathcal{I}_0\,\}$, som let ses at være et ideal. Der gælder $\mathcal{I}_0=t\mathcal{J}$, idet inklusionen $\supseteq$ følger af definitionen af $\mathcal{J}$, mens $\subseteq$ følger af $\mathcal{I}_0\subseteq\mathcal{M}=(t)$: til $x\in\mathcal{I}_0$ findes $y\in R$, så $x=ty$, og der gælder $y\in\mathcal{J}$ ifølge definitionen af $\mathcal{J}$, og dermed $x=ty\in t\mathcal{J}$. Nakayama's Lemma anvendt på den endeligt frembragte modul $\mathcal{J}$ giver nu, at $\mathcal{I}_0=t\mathcal{J}\subset\mathcal{J}$, og da $\mathcal{I}_0$ er maksimalt i $\mathbb{I}$, er $\mathcal{J}$ et hovedideal: $\mathcal{J}=(a)$ for et $a\in R$. Altså $\mathcal{I}_0=t\mathcal{J}=(ta)$ i modstrid med $\mathcal{I}_0\in\mathbb{I}$. $\square$

(8) *Alternativt bevis for* (6). (Ikke pensum.) Da R er noethersk, er ethvert element i $R\setminus\{0\}$ produkt af irreducible elementer. Ethvert irreducibelt element p er et primelement: (p) er nemlig maksimalt blandt ægte hovedidealer, og dermed $(p)=\mathcal{M}\in\operatorname{Spec}R$. Heraf følger, at R er UFD, og man indser derfor – ordret som ovenfor i (5) – at R er euklidisk, hvilket medfører, at R er PID. $\square$

(1) **Kommentar.** Bemærk, at *(ii)* og *(iii)* i Sætning 1(3) udtaler sig om egenskaber ved mængden af idealer i R ordnet ved inklusion $\subseteq$.

(2) **Stilopgave.** *Noetherske ringe.*

(a) Angiv definitionen af begrebet "noethersk ring".

(b) Angiv og bevis et interessant resultat, der beskriver en noethersk ring ved egenskaber ved mængden af idealer i ringen ordnet ved inklusion. De enkelte dele af beviset bør fremstå klart.

(c) Formulér og bevis Hilbert's Basissætning. De enkelte dele af beviset bør fremstå klart.

5. Endeligt snit

(1) **Fælles komponent.** To polynomier $f, g \in \mathbb{C}[x_1, x_2]$ siges at være *uden fælles komponent*, netop hvis enhver divisor i både f og g er konstant, altså netop hvis der for alle $p \in \mathbb{C}[x_1, x_2]$ gælder følgende for idealer i ringen $G \overset{\text{def}}{=} \mathbb{C}[x_1, x_2]$:

$$G(f, g) \subseteq Gp \quad \Rightarrow \quad Gp = G\,.$$

(2) **Lemma.** *Hvis $f, g \in \mathbb{C}[x_1, x_2]$ er uden fælles komponent, da findes $a \in \mathbb{C}[x_1]$ og $c, d \in \mathbb{C}[x_1, x_2]$, så*

$$0 \neq a = cf + dg\,.$$

(3) *Bevis.* Sæt $G \overset{\text{def}}{=} \mathbb{C}[x_1, x_2]$, $A \overset{\text{def}}{=} \mathbb{C}[x_1]$, som er en delring af G, og $B = \mathbb{C}(x_1)$, der er brøklegemet for A. Da er $G = A[x_2] \subset B[x_2]$, og sidstnævnte er et PID. Idealet $B[x_2](f, g)$ er således et hovedideal: $B[x_2](f, g) = B[x_2]q$ for et $q \in B[x_2]$, og dermed $f = hq$ og $g = kq$ med $h, k \in B[x_2]$. Lad $s \in A \setminus \{0\}$ være en fællesnævner for koefficienterne i de tre polynomier $h, k, q \in B[x_2]$, dvs. $sh, sk, sq \in A[x_2] = G$.

Vi ønsker nu at bevise, at q er et invertibelt element i $B[x_2]$. Antag derfor, at q ikke er invertibelt i $B[x_2]$, og søg en modstrid. Da q således ikke tilhører B, har vi $sq \in G \setminus A$. Da G er UFD, er sq produkt af sine primdivisorer, og disse kan derfor ikke alle tilhøre A ($\subset G$); lad $p \in G \setminus A$ være en primdivisor i sq, og dermed $Gp \in \operatorname{Spec} G$ (sml. PAK 3.4(10)), $sq \in Gp$ og $s^2 \notin Gp$ (da $s \in A \setminus \{0\}$). Da $s^2 f = (sh)(sq) \in Gp$ og $s^2 g = (sk)(sq) \in Gp$, fås nu $f, g \in Gp$, og dermed $G(f, g) \subseteq Gp \subset G$ i modstrid med, at f og g er uden fælles komponent.

Da q således er invertibel i $B[x_2]$, har vi $B[x_2](f, g) = B[x_2]$. Vælg $c, d \in B[x_2]$ med $cf + dg = 1$ og fællesnævner $a \in A \setminus \{0\}$ for koefficienterne i $c, d \in B[x_2]$: $ac, ad \in G$, og vi har $0 \neq a = (ac)f + (ad)g$ som ønsket. $\square$

(4) **Lokal ring i punkt.** For punkt $P \in \mathbb{A}^2_{\mathbb{C}}$ og $f, g \in \mathbb{C}[x_1, x_2]$ sættes $\mathcal{O}_P(f \bullet g) \overset{\text{def}}{=} \mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})/(f, g)$, idet (f, g) her – selvfølgelig – er idealet $\mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})(f, g)$ i ringen $\mathcal{O}_P(\mathbb{A}^2_{\mathbb{C}})$. Når $f(P) = 0$ og $g(P) = 0$ (og dermed $f, g \in \mathcal{M}_P(\mathbb{A}^2_{\mathbb{C}})$) kaldes $\mathcal{O}_P(f \bullet g)$ den *lokale ring for snittet $f \bullet g$* i punktet P; dens maksimalideal er $\mathcal{M}_P(f \bullet g) \overset{\text{def}}{=} \mathcal{M}_P(\mathbb{A}^2_{\mathbb{C}})/(f, g)$.

(5) **Produkt af ringe.** For kommutative ringe $R_1, \ldots, R_n$ er $\mathbb{Z}$–modulen $R_1 \oplus \cdots \oplus R_n$ en kommutativ ring med produktet $(r_1, \ldots, r_n)(r'_1, \ldots, r'_n) \overset{\text{def}}{=} (r_1 r'_1, \ldots, r_n r'_n)$; et-elementet er $(1, \ldots, 1)$, og ringen betegnes $R_1 \times \cdots \times R_n$.

(6) **Endelighedslemmaet.** *Sæt $G \overset{\text{def}}{=} \mathbb{C}[x_1, x_2]$, lad $f, g \in G$ være uden fælles komponent, og sæt $R = G/G(f, g)$.*

(7) *Da er nulpunktsfællesmængden $\mathrm{V}(f) \cap \mathrm{V}(g)$ endelig.*

Antag nu, at $\mathrm{V}(f) \cap \mathrm{V}(g) = \{P_1, \ldots, P_n\}$ med $P_1, \ldots, P_n \in \mathbb{A}^2_{\mathbb{C}}$ indbyrdes forskellige, og at $\mathrm{W}(f^*) \cap \mathrm{W}(g^*) \cap \mathcal{L}_\infty = \varnothing$. Da gælder:

(8) $$\dim R = (\deg f)(\deg g)\,;$$

(9) $$\operatorname{Max} R = \{\mathfrak{m}_{P_1}/G(f, g), \ldots, \mathfrak{m}_{P_n}/G(f, g)\}\,;$$

og der en en ringisomorfi:

(10) $$R \cong \mathcal{O}_{P_1}(f \bullet g) \times \cdots \times \mathcal{O}_{P_n}(f \bullet g)\,.$$

(1) *Bevis.* Ifølge lemma 1(2) kan $a \in \mathbb{C}[x_1] \setminus \{0\}$ vælges, så $a \in G(f,g)$. Vælg tilsvarende $b \in \mathbb{C}[x_2] \cap G(f,g) \setminus \{0\}$. Nulpunktsmængderne $U \stackrel{\text{def}}{=} \{\, p_1 \in \mathbb{C} \mid a(p_1) = 0 \,\}$ og $W \stackrel{\text{def}}{=} \{\, p_2 \in \mathbb{C} \mid b(p_2) = 0 \,\}$ er endelige, så det samme er produktmængden $U \times W$, og da denne indeholder nulpunktsfællesmængden $\mathrm{V}(f) \cap \mathrm{V}(g)$, er 1(7) bevist.

Beviset for 1(8) forbigås.

Da $P_i \in \mathrm{V}(f) \cap \mathrm{V}(g)$, har vi $G(f,g) \subseteq \mathfrak{m}_{P_i}$ og dermed $\mathfrak{m}_{P_i}/G(f,g) \in \operatorname{Max} R$, og dermed er inklusionen "$\supseteq$" i 1(9) bevist.

For at bevise "$\subseteq$" i 1(9) antages $\mathcal{M} \in \operatorname{Max} R$. Vælg $\mathfrak{m} \in \operatorname{Max} G$ med $\mathfrak{m} \supseteq G(f,g)$ og $\mathcal{M} = \mathfrak{m}/G(f,g)$. Vi har $A \stackrel{\text{def}}{=} G/\mathfrak{m} \cong R/\mathcal{M}$, som er et legeme – og dermed specielt et integritetsområde. Da A er en $\mathbb{C}$–algebra ved ringhomomorfien $\alpha\colon \mathbb{C} \to A$ givet ved $c \mapsto \alpha(c) \stackrel{\text{def}}{=} [c]_{\mathfrak{m}}$, og da $\dim A = \dim(R/\mathcal{M}) \le \dim R$, som er endelig ifølge 1(8), giver Nulpunktslemmaet 4(1), som kommer længere fremme, at α er surjektiv. Til $[x_1]_{\mathfrak{m}}, [x_2]_{\mathfrak{m}} \in A$ findes derfor $a_1, a_2 \in \mathbb{C}$ med $[x_1]_{\mathfrak{m}} = \alpha(a_1) = [a_1]_{\mathfrak{m}}$ og $[x_2]_{\mathfrak{m}} = \alpha(a_2) = [a_2]_{\mathfrak{m}}$, og dermed $\mathfrak{m}_P = (x_1 - a_1, x_2 - a_2) \subseteq \mathfrak{m}$ for $P \stackrel{\text{def}}{=} (a_1, a_2)$, sml. også PAK 6.1(6). Da $\mathfrak{m}_P \in \operatorname{Max} G$ fås $\mathfrak{m}_P = \mathfrak{m}$, og dermed $\mathfrak{m}_P \supseteq G(f,g)$, hvilket medfører $P \in \mathrm{V}(f) \cap \mathrm{V}(g) = \{P_1, \dots, P_n\}$, dvs. $\mathfrak{m} = \mathfrak{m}_{P_i}$ for ét $i \in \{1, \dots, n\}$; altså $\mathcal{M} = \mathfrak{m}_{P_i}/G(f,g)$ som ønsket.

Bevis for 1(10): Ringen R lokaliseret i maksimalidealet $\mathcal{M}_i \stackrel{\text{def}}{=} \mathfrak{m}_{P_i}/G(f,g)$ er ifølge anden isomorfi i 3.5(2) isomorf med

$$G_{\mathfrak{m}_{P_i}}/\big(G(f,g)\big)_{\mathfrak{m}_{P_i}} = G_{\mathfrak{m}_{P_i}}/G_{\mathfrak{m}_{P_i}}(f,g) = \mathcal{O}_{P_i}(\mathbb{A}^2_{\mathbb{C}})/(f,g) = \mathcal{O}_{P_i}(f \bullet g)\,,$$

hvor de sidste to ligheder er definitionerne af de respektive ringe. Vi vil derfor bevise:

$$(2) \qquad R \cong R_{\mathcal{M}_1} \times \cdots \times R_{\mathcal{M}_n}\,.$$

Men først vil vi bevise, at for enhver R–modul M er følgende ensbetydende:

$$(3) \qquad \begin{aligned} &(i) && \dim M = 1\,. \\ &(ii) && M \text{ har netop to } R\text{–undermoduler.} \\ &(iii) && \exists\, i \in \{1, \dots, n\}\colon M \cong R/\mathcal{M}_i\,. \end{aligned}$$

"$(i) \Rightarrow (ii)$": Da $M \neq 0$, har M mindst to undermoduler. Da vektorrummet M højst har to underrum, har R–modulen M højst to undermoduler.

"$(ii) \Rightarrow (iii)$": Da $M \supset 0$, kan vi vælge $x \in M \setminus 0$. Da $Rx \neq 0$, giver forudsætningen $Rx = M$, så M er cyklisk, og dermed har vi ifølge sætningen om cykliske moduler 2.3(2), at $M \cong R/\mathcal{I}$ for et ideal $\mathcal{I}$. Da $R/\mathcal{I}$ har netop to undermoduler, er $\mathcal{I}$ et maksimalideal, dvs. $\mathcal{I} = \mathcal{M}_i$ for ét i.

"$(iii) \Rightarrow (i)$" følger af: $R/\mathcal{M}_i \cong G/\mathfrak{m}_{P_i} \cong \mathbb{C}$, sml. PAK 6.1(4).

Nu er (3) bevist.

For enhver R–modul X betragtes R–modulen $X_{[\mathcal{M}]} \stackrel{\text{def}}{=} X_{\mathcal{M}_1} \oplus \cdots \oplus X_{\mathcal{M}_n}$ med elementer af formen $(x_1/s_1, \dots, x_n/s_n)$ med $x_i \in X$ og $s_i \in R \setminus \mathcal{M}_i$ for alle i. Enhver R–homomorfi $\varphi\colon X \to Y$ inducerer en R–homomorfi $\varphi_{[\mathcal{M}]}\colon X_{[\mathcal{M}]} \to Y_{[\mathcal{M}]}$ givet ved $\varphi_{[\mathcal{M}]}(x_1/s_1, \dots, x_n/s_n) \stackrel{\text{def}}{=} (\varphi(x_1)/s_1, \dots, \varphi(x_n)/s_n)$. Bemærk, at der gælder:

$$(4) \qquad \begin{aligned} \operatorname{Ker} \varphi_{[\mathcal{M}]} &= (\operatorname{Ker} \varphi_{\mathcal{M}_1}) \oplus \cdots \oplus (\operatorname{Ker} \varphi_{\mathcal{M}_n}) \;\; (\subseteq X_{[\mathcal{M}]}\,) \\ \operatorname{Im} \varphi_{[\mathcal{M}]} &= (\operatorname{Im} \varphi_{\mathcal{M}_1}) \oplus \cdots \oplus (\operatorname{Im} \varphi_{\mathcal{M}_n}) \quad (\subseteq Y_{[\mathcal{M}]}\,)\,. \end{aligned}$$

Endvidere er der en R–homomorfi:

$$\underline{\rho}_X : X \to X_{[\mathcal{M}]} \quad \text{defineret ved} \quad \underline{\rho}_X(m) = (m/1, \ldots, m/1)\,.$$

Bemærk, at der gælder $\underline{\rho}_Y \circ \varphi = \varphi_{[\mathcal{M}]} \circ \underline{\rho}_X$, dvs. der er et *kommutativt* diagram:

(1)
$$\begin{tikzcd} X \arrow[r, "\varphi"] \arrow[d, "\underline{\rho}_X"'] & Y \arrow[d, "\underline{\rho}_Y"'] \\ X_{[\mathcal{M}]} \arrow[r, "\varphi_{[\mathcal{M}]}"'] & Y_{[\mathcal{M}]}\,. \end{tikzcd}$$

Der gælder:

(2)
$$\dim X < \infty \quad \Rightarrow \quad \underline{\rho}_X \ \text{ er en isomorfi.}$$

Dette medfører den ønskede isomorfi 2(2) og bevises ved induktion efter $d \overset{\text{def}}{=\!=} \dim X$.

Induktionsstart: $d = 0$: $X = 0$ og $X_{[\mathcal{M}]} = 0$, så $\underline{\rho}_X : 0 \to 0$ er bijektiv.

$d = 1$: Ifølge 2(3) kan vi gerne antage $X \cong R/\mathcal{M}_1$. For $j > 1$ har vi

$$X_{\mathcal{M}_j} \cong (R/\mathcal{M}_1)_{\mathcal{M}_j} \cong R_{\mathcal{M}_j}/(\mathcal{M}_1)_{\mathcal{M}_j} \cong R_{\mathcal{M}_j}/R_{\mathcal{M}_j} = 0\,, \text{ og dermed}$$
$$X_{[\mathcal{M}]} = X_{\mathcal{M}_1} \times 0 \times \cdots \times 0 = X_{\mathcal{M}_1}\,,$$

så $\underline{\rho}_X$ bliver blot til homomorfien $\rho_X : X \to X_{\mathcal{M}_1}$, som er en isomorfi ifølge 3.7(6).

Induktionstrin $d > 0$: Ifølge 2(3) kan vi vælge undermodul U af X, så $0 \subset U \subset X$. Betragt diagrammet:

(3)
$$\begin{tikzcd} 0 \arrow[r] & U \arrow[r, "\iota"] \arrow[d, "\underline{\rho}_U"', "\cong"] & X \arrow[r, "\pi"] \arrow[d, "\underline{\rho}_X"'] & X/U \arrow[r] \arrow[d, "\underline{\rho}_{X/U}"', "\cong"] & 0 \\ 0 \arrow[r] & U_{[\mathcal{M}]} \arrow[r, "\iota_{[\mathcal{M}]}"'] & X_{[\mathcal{M}]} \arrow[r, "\pi_{[\mathcal{M}]}"'] & (X/U)_{[\mathcal{M}]} \arrow[r] & 0\,. \end{tikzcd}$$

Her er ι inklusionshomomorfien og π restklassehomomorfien, så første række i (3) er exakt. Diagrammet er kommutativt, sml. (1). Da $\dim U, \dim(X/U) < \dim X = d$, giver induktionsantagelsen, at $\underline{\rho}_U$ og $\underline{\rho}_{X/U}$ er isomorfier. For ethvert $i \in \{1, \ldots, n\}$ er følgen:

$$0 \to U_{\mathcal{M}_i} \xrightarrow{\iota_{\mathcal{M}_i}} X_{\mathcal{M}_i} \xrightarrow{\pi_{\mathcal{M}_i}} (X/U)_{\mathcal{M}_i} \to 0$$

exakt ifølge 3.4(5), så anden række i (3) er exakt, sml. evt. 2(4).

For at bevise, at $\underline{\rho}_X$ er injektiv, antag, at $x \in X$ og $\underline{\rho}_X(x) = 0$. Da $\underline{\rho}_{X/U}\big(\pi(x)\big) = \pi_{[\mathcal{M}]}\big(\underline{\rho}_X(x)\big) = \pi_{[\mathcal{M}]}(0) = 0$, og da $\underline{\rho}_{X/U}$ er injektiv, er $\pi(x) = 0$, og dermed $x \in U$. Da $\iota_{[\mathcal{M}]}\big(\underline{\rho}_U(x)\big) = \underline{\rho}_X\big(\iota(x)\big) = \underline{\rho}_X(x) = 0$, og da $\iota_{[\mathcal{M}]}$ er injektiv, er $\underline{\rho}_U(x) = 0$, og dermed $x = 0$, da $\underline{\rho}_U$ er injektiv.

For at bevise, at $\underline{\rho}_X$ er surjektiv, antag $z \in X_{[\mathcal{M}]}$. Da $\underline{\rho}_{X/U}$ er surjektiv, kan $y \in X$ vælges, så $\underline{\rho}_{X/U}([y]_U) = \pi_{[\mathcal{M}]}(z)$. Da $\pi_{[\mathcal{M}]}\big(z - \underline{\rho}_X(y)\big) = \pi_{[\mathcal{M}]}(z) - \underline{\rho}_{X/U}\big(\pi(y)\big) = 0$, har vi $z - \underline{\rho}_X(y) \in \operatorname{Ker} \pi_{[\mathcal{M}]} = \operatorname{Im} \iota_{[\mathcal{M}]}$, og derfor findes $w \in U_{[\mathcal{M}]}$, så $\iota_{[\mathcal{M}]}(w) = z - \underline{\rho}_X(y)$. Da $\underline{\rho}_U$ er surjektiv, kan $u \in U$ vælges, så $\underline{\rho}_U(u) = w$, og vi får:

$$\underline{\rho}_X(u) = \underline{\rho}_X\big(\iota(u)\big) = \iota_{[\mathcal{M}]}\big(\underline{\rho}_U(u)\big) = \iota_{[\mathcal{M}]}(w) = z - \underline{\rho}_X(y)\,.$$

Heraf følger $\underline{\rho}_X(u + y) = z$, og dermed $z \in \operatorname{Im} \underline{\rho}_X$. $\square$

(1) **Nulpunktslemmaet.** *Hvis A er et integritetsområde, som er en $\mathbb{C}$–algebra ved ringhomomorfien $\alpha\colon \mathbb{C} \to A$ med $\dim A$ endelig, da er α surjektiv.*

(2) *Bevis.* Sæt $n \stackrel{\text{def}}{=} \dim A$, og antag $a \in A$. De $n+1$ vektorer $1, a, \dots, a^n$ i vektorrummet A er derfor lineært afhængige, så der findes $c_0, c_1, \dots, c_n \in \mathbb{C}$ med $c_0 1 + c_1 a + \cdots + c_n a^n = 0$ og $c_j \neq 0$ for ét j. For $p = b_0 + b_1 x + \cdots + b_m x^m \in \mathbb{C}[x]$ gives evalueringshomomorfien $\varepsilon_a\colon \mathbb{C}[x] \to A$ ved $\varepsilon_a(p) = b_0 1 + b_1 a + \cdots + b_m a^m$. Da $q \stackrel{\text{def}}{=} c_0 + c_1 x + \cdots + c_n x^n \neq 0$ og $\varepsilon_a(q) = 0$, har vi $\operatorname{Ker} \varepsilon_a \neq 0$. Isomorfisætningen (for ringe) giver $\operatorname{Im} \varepsilon_a \cong \mathbb{C}[x]/\operatorname{Ker} \varepsilon_a$. Da $\operatorname{Im} \varepsilon_a$ er en delring af integritetsområdet A, er den selv et integritetsområde, så $\operatorname{Ker} \varepsilon_a$ er et ikke–trivielt primideal i $\mathbb{C}[x]$, som er PID. Derfor er $\operatorname{Ker} \varepsilon_a$ frembragt af et irreducibelt polynomium i $\mathbb{C}[x]$, og algebraens fundamentalsætning giver, at dette irreducible polynomium er af grad 1, dvs. der findes $b_0 \in \mathbb{C}$ med $\operatorname{Ker} \varepsilon_a = \mathbb{C}[x](x - b_0)$. Heraf følger, at $0 = \varepsilon_a(x - b_0) = a - b_0 1 = a - \alpha(b_0)$, idet $\mathbb{C}$–multiplikationen $\mathbb{C} \times A \to A$ (jo) er givet ved $(c, a) \mapsto ca = \alpha(c)a$. Vi har nu bevist, at a tilhører $\operatorname{Im} \alpha$. $\square$

(3) **Opgave.** Giv eksempel på et integritetsområde A, der er en $\mathbb{C}$–algebra ved ringhomomorfien $\alpha\colon \mathbb{C} \to A$, som ikke er surjektiv (og dermed $\dim A = \infty$).

Fra nu af antages:

$$\boxed{\boxed{R \ \textbf{ er en ikke–triviel kommutativ ring.}}}$$

(4) **Opgave.** Lad R være en $\mathbb{C}$–algebra med $\dim R$ endelig. Bevis, at R er noethersk.

(5) **Opgave.** Lad R være en $\mathbb{C}$–algebra med $\dim R$ endelig. Bevis, at R er *artinsk*, hvilket vil sige, at enhver *dalende* kæde $\mathcal{I}_1 \supseteq \mathcal{I}_2 \supseteq \cdots \supseteq \mathcal{I}_m \supseteq \mathcal{I}_{m+1} \supseteq \cdots$ af idealer i R er sluttelig stationær: der findes $m_0 \in \mathbb{N}$, så $\mathcal{I}_{m_0} = \mathcal{I}_{m_0+i}$ for alle $i \in \mathbb{N}_0$.

(6) **Opgave.** Lad R være en $\mathbb{C}$–algebra med $\dim R$ endelig. Bevis, at hvis $\mathcal{M}_1, \dots, \mathcal{M}_n$ er indbyrdes forskellige maksimalidealer og $n > 1$, da er $\mathcal{M}_1 \cap \cdots \cap \mathcal{M}_{n-1} \supset \mathcal{M}_1 \cap \cdots \cap \mathcal{M}_n$ (f.eks. ved at lokalisere i $\mathcal{M}_n$ og udnytte 3.7(9)). Bevis, at $\operatorname{Max} R$ er endelig.

(7) **Den Kinesiske Restklassesætning.** (Ikke pensum.) *For idealer $\mathcal{I}_1, \dots, \mathcal{I}_n$ i R med $\mathcal{I}_i + \mathcal{I}_j = R$ for $i \neq j$ er der en ringisomorfi:*

$$\begin{array}{rcl} \varphi\colon R/(\mathcal{I}_1 \cap \cdots \cap \mathcal{I}_n) & \xrightarrow{\cong} & (R/\mathcal{I}_1) \times \cdots \times (R/\mathcal{I}_n) \\ {[r]}_{\mathcal{I}_1 \cap \cdots \cap \mathcal{I}_n} & \longmapsto & ([r]_{\mathcal{I}_1}, \dots, [r]_{\mathcal{I}_n}) \, . \end{array}$$

(8) *Bevis.* (Ikke pensum.) Betragt R–modulerne $V \stackrel{\text{def}}{=} R/(\mathcal{I}_1 \cap \cdots \cap \mathcal{I}_n)$ og $H \stackrel{\text{def}}{=} (R/\mathcal{I}_1) \oplus \cdots \oplus (R/\mathcal{I}_n)$ samt R–homomorfien $\varphi\colon V \to H$, der er (korrekt) defineret ved $\varphi([r]_{\mathcal{I}_1 \cap \cdots \cap \mathcal{I}_n}) \stackrel{\text{def}}{=} ([r]_{\mathcal{I}_1}, \dots, [r]_{\mathcal{I}_n})$. Faktisk er V og H kommutative ringe (og som sådan betegnes den sidstnævnte $(R/\mathcal{I}_1) \times \cdots \times (R/\mathcal{I}_n)$), og φ er en ringhomomorfi; vi skal bevise, at den er bijektiv, og til dette vil vi benytte 3.7(12)&(13) og (blot) betragte φ som R–homomorfi.

Lad nu $\mathcal{M}$ tilhøre $\operatorname{Max} R$. Betragt $R_{\mathcal{M}}$–modulen:

$$V_{[\mathcal{M}]} \stackrel{\text{def}}{=} R_{\mathcal{M}}/(\mathcal{I}_1 \cap \cdots \cap \mathcal{I}_n)_{\mathcal{M}} = R_{\mathcal{M}}/\big((\mathcal{I}_1)_{\mathcal{M}} \cap \cdots \cap (\mathcal{I}_n)_{\mathcal{M}}\big) \, ,$$

hvor sidste lighed kommer fra opgave 3.7(9), og $R_{\mathcal{M}}$–isomorfien $\alpha_{[\mathcal{M}]}\colon V_{[\mathcal{M}]} \xrightarrow{\cong} V_{\mathcal{M}}$ fra Brøkmodullemmaet, se 3.4(2). Betragt endvidere $R_{\mathcal{M}}$–modulen:

$$H_{[\mathcal{M}]} \overset{\text{def}}{=} \big(R_{\mathcal{M}}/(\mathcal{I}_1)_{\mathcal{M}}\big) \oplus \cdots \oplus \big(R_{\mathcal{M}}/(\mathcal{I}_n)_{\mathcal{M}}\big)$$

og $R_{\mathcal{M}}$–isomorfien $\beta_{[\mathcal{M}]}\colon H_{\mathcal{M}} \xrightarrow{\cong} H_{[\mathcal{M}]}$ fra opgave 3.7(14). Betragt endelig $R_{\mathcal{M}}$–homomorfien:

$$\begin{gathered}\varphi_{[\mathcal{M}]}\colon V_{[\mathcal{M}]} \longrightarrow H_{[\mathcal{M}]}\\ \varphi_{[\mathcal{M}]}([r/s]_{(\mathcal{I}_1\cap\cdots\cap\mathcal{I}_n)_{\mathcal{M}}} \overset{\text{def}}{=} ([r/s]_{(\mathcal{I}_1)_{\mathcal{M}}}, \ldots, [r/s]_{(\mathcal{I}_n)_{\mathcal{M}}})\,.\end{gathered}$$

Da $\varphi_{[\mathcal{M}]} = \beta_{[\mathcal{M}]} \circ \varphi_{\mathcal{M}} \circ \alpha_{[\mathcal{M}]}$, er $\varphi_{\mathcal{M}}\colon V_{\mathcal{M}} \longrightarrow H_{\mathcal{M}}$ er bijektiv, netop hvis $\varphi_{[\mathcal{M}]}$ er det.

Ifølge 3.7(12)&(13) er det derfor tilstrækkeligt at bevise:

$$\varphi_{[\mathcal{M}]}\colon V_{[\mathcal{M}]} \longrightarrow H_{[\mathcal{M}]} \;\text{ er bijektiv for alle }\; \mathcal{M} \in \operatorname{Max} R\,.$$

Antag derfor $\mathcal{M} \in \operatorname{Max} R$. Der inddeles i to tilfælde.

1° *$\mathcal{I}_i \not\subseteq \mathcal{M}$ for alle $i \in \{1, \ldots, n\}$.* Vi har $(\mathcal{I}_i)_{\mathcal{M}} = R_{\mathcal{M}}$ for alle i, og dermed

$$\begin{aligned} V_{[\mathcal{M}]} &= R_{\mathcal{M}}/(R_{\mathcal{M}} \cap \cdots \cap R_{\mathcal{M}}) = R_{\mathcal{M}}/R_{\mathcal{M}} = 0 \;\text{ og}\\ H_{[\mathcal{M}]} &= (R_{\mathcal{M}}/R_{\mathcal{M}}) \times \cdots \times (R_{\mathcal{M}}/R_{\mathcal{M}}) = 0 \times \cdots \times 0 = 0\,.\end{aligned}$$

Heraf følger, at $\varphi_{[\mathcal{M}]}$ er nulhomomorfier $0 \longrightarrow 0$, som i dette tilfælde er bijektiv.

2° *$\mathcal{I}_i \not\subseteq \mathcal{M}$ for ét $i \in \{1, \ldots, n\}$.* Vi kan gerne antage $\mathcal{I}_1 \subseteq \mathcal{M}$ og dermed (ifølge forudsætningen) $\mathcal{I}_j \not\subseteq \mathcal{M}$ for $j > 1$. Vi har $(\mathcal{I}_j)_{\mathcal{M}} = R_{\mathcal{M}}$ for $j > 1$, og dermed

$$\begin{aligned} V_{[\mathcal{M}]} &= R_{\mathcal{M}}/\big((\mathcal{I}_1)_{\mathcal{M}} \cap R_{\mathcal{M}} \cap \cdots \cap R_{\mathcal{M}}\big) = R_{\mathcal{M}}/(\mathcal{I})_{\mathcal{M}} \;\text{ og}\\ H_{[\mathcal{M}]} &= (R_{\mathcal{M}}/(\mathcal{I}_1)_{\mathcal{M}}) \times (R_{\mathcal{M}}/R_{\mathcal{M}}) \times \cdots \times (R_{\mathcal{M}}/R_{\mathcal{M}})\\ &= (R_{\mathcal{M}}/(\mathcal{I}_1)_{\mathcal{M}}) \times 0 \times \cdots \times 0 = R_{\mathcal{M}}/(\mathcal{I}_1)_{\mathcal{M}}\,.\end{aligned}$$

Nu er $\varphi_{[\mathcal{M}]}$ blevet til identiteten $R_{\mathcal{M}}/(\mathcal{I}_1)_{\mathcal{M}} \longrightarrow R_{\mathcal{M}}/(\mathcal{I}_1)_{\mathcal{M}}$, som er bijektiv. $\square$