Affin och projektiv geometri

Magnus Jacobsson

August 29, 2022

Contents

1 Introduktion och Varning

Det här är mer föreläsningsanteckningar än en bok än så länge, så det finns garanterat fel och slarvigheter i dem. Vissa avsnitt (speciellt de mer diskuterande) är inte så noggrant genomarbetade. Det rekommenderas verkligen att gå på föreläsningarna för att kunna följa med i kursen. Jag är tacksam för alla kommentarer. Sist i kompendiet finns lite referenslitteratur som jag har

använt när jag har pusslat ihop den här kursen. Boken av Bix har varit officiell kurslitteratur på kursen tidigare.

2 Repetition: Algebra.

Detta avsnitt innehåller en del grundläggande algebraiska resultat och definitioner som vi kommer att använda oss av i denna kurs. Det mesta i detta avsnitt är repetition från kurserna Algebra I och II. Jag har där det varit möjligt inkluderat bevis när jag är osäker på om beviset ges i dessa kurser, men i de fall beviset är för avancerat och kräver för mycket bakgrundsarbete har jag helt enkelt hänvisat till senare kurser i abstrakt algebra. Hursomhelst rekommenderas att gå tillbaka till detta avsnitt när du inser att du är osäker på något algebraiskt faktum.

2.1 Ringar och kroppar.

Definition. En *kommutativ ring* är en mängd R med två binära operationer $+$ (addition) och $\cdot$ (multiplikation) och två speciella element $0, 1$ sådan att

(i) $+$ är kommutativ och associativ med enhetselement 0 och det finns additiv invers $-x$ till varje element x[1]:

- $x + (y + z) = (x + y) + z$ för alla $x, y, z \in R$.
- $0 + x = x + 0 = x$ för alla $x \in R$.
- För varje $x \in R$ finns $-x \in R$ så att $x + (-x) = (-x) + x = 0$.
- $x + y = y + x$ för alla $x, y \in R$.

(ii) $\cdot$ är kommutativ och associativ och 1 är dess enhetselement, dvs.

- $x \cdot y = y \cdot x$ för alla $x, y \in R$.
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ för alla $x, y, z \in R$.
- $1 \cdot x = x \cdot 1 = x$ för alla $x \in R$.

(iii) Den distributiva lagen $(x + y) \cdot z = x \cdot z + y \cdot z$ gäller.

Multiplikationstecknet utelämnas vanligen enligt $x \cdot y = xy$.

Med ett mer oansvarigt uttryckssätt är en kommutativ ring således en algebraisk struktur där addition, subtraktion och multiplikation uppfyller "de vanliga räknelagarna". Vi kommer bara att möta kommutativa ringar i denna kurs, så vi kallar dem bara ringar i fortsättningen. Vi kommer också alltid att anta att $0 \neq 1$.

Exempel. Heltalen $\mathbb{Z}$ är ett exempel på en ring. Detsamma gäller talområdena $\mathbb{Q}$, $\mathbb{R}$ och $\mathbb{C}$.

[1] En mängd med en associativ binär operation med enhetselement och där varje element har en invers kallas en *grupp*. Om operationen är kommutativ så kallas gruppen *abelsk* och operationen betecknas ofta med $+$.

Definition. Ett element $x \neq 0$ i en ring kallas en *nolldelare* om det finns ett element $y \neq 0$ sådant att $xy = 0$.

Definition. En ring kallas ett *integritetsområde* om den saknar nolldelare.

Definition. En ring k kallas en *kropp* om varje nollskilt element har en multiplikativ invers, dvs.

- Om $x \neq 0$ så finns ett $x^{-1} \in k$ så att $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

Exempel. $\mathbb{Q}$, $\mathbb{R}$ och $\mathbb{C}$ är alla kroppar. Alla kroppar är integritetsområden. $\mathbb{Z}$ är inte en kropp (bara ± 1 har multiplikativ invers). Däremot är $\mathbb{Z}$ ett integritetsområde.

Exempel. Låt k vara en kropp. Vi betecknar med $k[x_1, ..., x_n]$ mängden av alla polynom i n variabler med koefficienter i k. De naturliga additions- och multiplikationsoperationerna mellan polynom gör denna mängd till en ring, som kallas *polynomringen i n variabler (med koefficienter i k)*.

Envariabelfallet $n = 1$ är förhoppningsvis välbekant från tidigare algebrakurser. Vi kommer mest att hålla oss till fallen $n = 2, 3$ i den här kursen och k kommer nästan alltid vara antingen $\mathbb{R}$ eller $\mathbb{C}$. I dessa fall använder vi som vanligt beteckningar $k[x], k[x, y]$ etc.

Polynomringar har ytterligare en egenskap, nämligen att de är vektorrum över k. I t.ex. $\mathbb{C}[x, y]$ kan vi multiplicera elementen p med komplexa tal λ på ett naturligt sätt och denna multiplikation uppfyller vektorrumsaxiomen. Dessutom uppfyller den regeln

$$(\lambda p) \cdot (\mu q) = (\lambda \mu) pq.$$

En sådan algebraisk struktur kallas en *(kommutativ) k-algebra*. Vi kommer i fortsättningen att referera till $k[x_1, ..., x_n]$ som *polynomringen i n variabler*, men (något motsägelsefullt) alltid att behandla den som en k-algebra.

Anmärkning. Polynomringarna över en kropp k är integritetsområden.

2.2 Faktorisering och irreducibilitet.

Låt R vara en ring.

Definition. Om $x \in R$ har en multiplikativ invers kallas x en *enhet*.

Definition. Ett element p i R kallas *irreducibelt* om $p \neq 0$, p inte är en enhet och p inte kan faktoriseras i en produkt av två icke-enheter.

Exempel. Låt $p = p(x_1, ..., x_n) \in k[x_1, ..., x_n]$. Att p är irreducibelt betyder då för det första

att det inte är konstant, för det andra att det inte kan faktoriseras i en produkt $p = p_1 p_2$ av två icke-konstanta polynom.

Exempel. I $\mathbb{Z}$ är de irreducibla elementen de som är $\pm$ ett primtal. Ett tal $p \in \mathbb{Z}$ är $\pm$ ett primtal om och endast om det är skilt från ± 1 och uppfyller att om $p = p_1 p_2$ så är antingen $p_1 = \pm 1$ eller $p_2 = \pm 1$.

Kom ihåg från grundläggande kurser i algebra att varje heltal har en unik primtalsfaktorisering. Motsvarande påstående om polynom är följande. Det torde vara bekant i envariabelfallet $n = 1$.

Sats. Varje polynom i $k[x_1, ..., x_n]$ kan faktoriseras på ett unikt sätt i irreducibla faktorer (upp till ordning och multiplikation med konstanter).

Definition. Egenskapen som beskrivs i satsen kan uttryckas genom att säga att $k[x_1, ..., x_n]$ är en *faktoriell ring*.

Anmärkning. I envariabelfallet kan man bevisa ovanstående sats ganska lätt. Sådana polynomringar $k[x]$ är s.k. *euklidiska ringar*, vilket innebär att det finns en explicit algoritm (Euklides algoritm) för att beräkna $\gcd(p, q)$ av två element. Vi har då följande användbara sats. som alltså gäller både i $R = \mathbb{Z}$ och i $R = k[x]$ och som antagligen är känd från tidigare kurser[2].

Sats. (Bezouts lemma) Låt R vara en euklidisk ring och $p, q \in R$. Då existerar $a, b \in R$ så att

$$ap + bq = \gcd(p, q).$$

Talen a och b kan bestämmas med Euklides algoritm.

Anmärkning. Från denna sats följer satsen om entydig faktorisering ganska lätt. Den gäller dock inte i polynomringar i flera variabler. Ovannämnda bevis av faktorisering i dessa får därför anstå till en senare algebrakurs.

Anmärkning. Frågan om ett polynoms irreducibilitet beror på i vilken ring vi tänker oss att polynomet ligger. Detta är bekant redan från envariabelfallet, där ju t.ex. $f(x) = x^2 + 1$ är irreducibelt som element i $\mathbb{R}[x]$ men inte som element i $\mathbb{C}[x]$, där vi kan skriva $x^2 + 1 = (x + i)(x - i)$.

Exempel.

1. Alla polynom av grad 1 i $k[x_1, ..., x_n]$ är irreducibla. (Notera att graden av en produkt är summan av graderna.)
2. $p(x, y) = x^2 - y^2$ har faktoriseringen $p(x, y) = (x - y)(x + y)$ i irreducibla faktorer. Notera att $p(x, y) = 0$ består av två linjer som skär varandra i origo. Var och en av linjerna är

[2]Ett av de centrala resultaten i denna kurs är "Bezouts sats". Det rör sig om samma Bezout, men ett annat resultat varför jag kommer att hänvisa till denna sats som Bezouts lemma.

nollställesmängd till en av de irreducibla faktorerna.

3. $p(x,y) = x^2 + y^2 - 1$ är irreducibelt i $\mathbb{C}[x,y]$ och därför även i $\mathbb{R}[x,y]$. Om inte, skulle p vara produkten av två linjära polynom. (Varför är detta inte möjligt?)

4. $p(x,y) = x^2 + y^2$ är irreducibelt i $\mathbb{R}[x,y]$ men inte i $\mathbb{C}[x,y]$, där det kan skrivas $p(x,y) = (x+iy)(x-iy)$.

Som sagt finns det alltså ingen allmän divisionsalgoritm i $k[x,y]$. Följande speciella division kan dock alltid genomföras, och detta kommer att vara användbart i kapitlet om skärningsmultiplicitet senare.

Sats. Låt $p(x)$ och $f(x,y)$ vara polynom. Då finns unika polynom $q(x,y)$ och $r(x)$ så att

$$f(x,y) = (y - p(x))q(x,y) + r(x).$$

Vidare är

$$r(x) = f(x, p(x)).$$

Bevis. Beviset sker med induktion på y-graden hos $f(x,y)$. Om $\deg_y f(x,y) = 0$ är $r = f$ och det finns inget att visa. Antag att påståendet är sant för alla funktioner f med $\deg_y f < n$. Låt nu $\deg_y f = n$. Antag att

$$f(x,y) = a_n(x)y^n + ... + a_1(x)y + a_0(x).$$

Då kan vi skriva om som följer:

$$f(x,y) = a_n(x)y^n + ... + a_1(x)y + a_0(x) =$$

$$= (y - p(x))(a_n(x)y^{n-1} + ... + a_1(x)) + p(x)(a_n(x)y^{n-1} + ... + a_1(x)) + a_0(x) =$$

$$= (y - p(x))q_1(x,y) + r_1(x,y),$$

där vi har använt beteckningarna

$$q_1(x,y) = a_n(x)y^{n-1} + ... + a_1(x)$$

och

$$r_1(x,y) = p(x)(a_n(x)y^{n-1} + ... + a_1(x)) + a_0(x)$$

Eftersom $\deg_y r_1 < n$ är enligt induktionsantagandet

$$p(x)(a_n(x)y^{n-1} + ... + a_1(x)) + a_0(x) = (y - p(x))q_2(x,y) + r_2(x)$$

och det följer att

$$f(x,y) = (y - p(x))(q_1(x,y) + q_2(x,y)) + r_2(x),$$

vilket bevisar existensdelen av påståendet, om vi sätter $q = q_1 + q_2$ och $r = r_2$.

För entydigheten antar vi att vi har två sätt att skriva f som angivet:

$$f = (y - p)q + r = (y - p)q' + r'.$$

Subtraheras leden får vi

$$(y - p(x))(q(x, y) - q'(x, y)) = (r'(x) - r(x)).$$

Men här har högerledet y-grad 0 så detsamma gäller vänsterledet, vilket medför att $q = q'$ varifrån följer att $r = r'$.

Slutligen är det uppenbart från formeln att $f(x, p(x)) = 0 + r(x)$.

Vi kan också generalisera existensdelen av denna sats.

Sats. $f, g \in k[x, y]$. Låt $n = \deg_y g$ och beteckna med $a_n(x)$ koefficienten framför y^n i g. Då finns ett tal $k \in \mathbb{N}$ och polynom $q(x, y)$ och $r(x, y)$, där $\deg_y r < \deg_y g$ sådana att

$$a_n^k(x)f(x, y) = q(x, y)g(x, y) + r(x).$$

Bevis.

Övningar.

1. Kontrollera att polynomringen $k[x, y]$ är en ring, genom att gå igenom alla axiom.
2. Är $k[x, y]$ en kropp?
3. Låt $f(x)$ och $g(x)$ vara två polynom som saknar gemensamma faktorer (förutom konstanter). Visa att $f(x) + yg(x)$ är irreducibelt.
4. Låt $f(x)$ vara ett polynom. Visa att $y^2 + f(x)$ är reducibelt om och endast om $f(x) = -g(x)^2$ för något polynom g.
5. Låt $f(x)$ vara ett polynom. Visa att $y^3 + f(x)$ är reducibelt om och endast om $f(x) = g(x)^3$ för något polynom g.

2.3 Ideal och kvotringar.

Definition. En icke-tom delmängd $I \subset R$ kallas ett *ideal* om den är sluten under addition och multiplikation med element ur R. Med andra ord, om $x, y \in I$, $r, s \in R$ så är också $rx + sy \in I$.

Definition. Om $S \subset R$ är en icke-tom delmängd så utgör mängden av linjärkombinationer av element ur S med koefficienter i R ett ideal i R, som vi betecknar med (S) och kallar för idealet genererat av S.

Exempel.

(i) Varje ideal i $\mathbb{Z}$ genereras av ett enda element k: $(k) = \{nk | n \in \mathbb{Z}\}$ (det minsta positiva elementet i I genererar I, använd divisionsalgoritmen). Detta ideal betecknas också $k\mathbb{Z}$.

(ii) Varje ideal genereras av ett enda polynom $p(x)$, och består av alla polynom som har $p(x)$ som faktor: $(p(x)) = \{m(x)p(x) | m(x) \in k[x]\}$.

(iii) Ideal som i (i) och (ii) som genereras av ett enda element, kallas *huvudideal*.

(iv) Alla ideal i $\mathbb{C}[x, y]$ är inte huvudideal. T.ex. kan idealet (x, y) inte genereras av ett enskilt polynom.

Definition. Ett integritetsområde där alla ideal är huvudideal kallas en *huvudidealring*.

Definition. Ett ideal $I \neq R$ kallas ett *maximalt ideal* om det enda ideal (förutom I) som innehåller I är R.

Definition. Ett ideal $I \neq R$ kallas ett *primideal* om $f, g \notin I \implies fg \notin I$.

Exempel.

(i) Varje nollskilt primideal i $\mathbb{Z}$ är maximalt (detta är sant i alla huvudidealringar) och det är precis de som genereras av ett primtal $I = (p)$.

(ii) Varje nollskilt primideal i $k[x]$ är maximalt (detta är ju också en huvudidealring). Dessa är precis de ideal som genereras av ett irreducibelt polynom.

(iii) I $\mathbb{C}[x, y]$ är t.ex. idealet (x, y) maximalt. Huvudideal (p) som genereras av irreducibla polynom p är primideal.

Definition. Om R är en ring och I ett ideal, kan vi definiera relationen $r \sim s \iff r - s \in I$. Mängden av ekvivalensklasser $r + I$ betecknas R/I och kallas kvotringen. Namnet motiveras av följande sats.

Sats. R/I är en ring under de naturliga additions- och multiplikationsoperationerna $(r + I) + (s + I) = (r + s) + I$ och $(r + I)(s + I) = rs + I$. Enhetselementen ges av de klasserna $0 + I$ och $1 + I$.

2.4 Ringhomomorfier.

Definition. Låt R och S vara ringar. En funktion $f : R \to S$ kallas en *ringhomomorfi* om

- $f(x + y) = f(x) + f(y)$
- $f(xy) = f(x)f(y)$.
- $f(1) = 1$

Exempel. Låt $a = (a_1, ..., a_n) \in k^n$ vara en given punkt. Funktionen

$$ev_a : k[x_1, ..., x_n] \to k,$$

definierad genom $ev_a(f) = f(a_1, ..., a_n)$ kallas *evalueringshomomorfin* i punkten a. Detta är en ringhomomorfi.

Sats. Om $f : R \to S$ är en ringhomomorfi är $\ker(f) = f^{-1}(0)$ ett ideal i R.

Bevis. Om $x, y \in \ker(f)$ och $r, s \in R$ så är $f(rx + sy) = f(r)f(x) + f(s)f(y) = 0$, så $rx + sy \in \ker(f)$.

Följande kallas ibland Noethers första isomorfisats (för ringar) och är mycket användbar.

Sats. Om $f : R \to S$ är en surjektiv ringhomomorfi är $R/\ker(f) \cong S$, via avbildningen $\hat{f}$ given av $\hat{f}(x + \ker(f)) = f(x)$.

Bevis. $\hat{f}$ är väldefinierad: Om $x - y \in \ker(f)$ så är $f(x) = f(y + x - y) = f(y) + f(x - y) = f(y)$.
$\hat{f}$ är en homomorfism:

$$\hat{f}((x+\ker(f))(y+\ker(f))) = \hat{f}(xy+\ker(f)) = f(xy) = f(x)f(y) = \hat{f}((x+\ker(f))\hat{f}(y+\ker(f))).$$

På liknande sätt visas additivitet.

$$\hat{f}(1 + \ker f) = f(1) = 1.$$

$\hat{f}$ är surjektiv: Uppenbart.
$\hat{f}$ är injektiv: $\hat{f}(x + \ker(f)) = 0 \iff f(x) = 0 \iff x \in \ker(f)$.

Anmärkning. Den naturliga avbildningen $\pi : R \to R/I$ som ges av $r \mapsto r + I$ är en surjektiv ringhomomorfism.

Följande sats ingår måhända inte i Algebra II.

Sats. Det finns en bijektion mellan idealen i R/I och de ideal i R som innehåller idealet I. Korrespondensen ges av att idealet $J \subset R/I$ motsvarar idealet $\pi^{-1}(J) \subset R$.

*Bevis.*Skriv in detta bevis

Sats. Ett ideal $I \neq R$ är maximalt om och endast om R/I är en kropp.

Bevis. R/I är en kropp $\iff$ De enda idealen i R/I är $\{0\}$ och $R/I \iff$ Det enda ideal i R som innehåller I är $R \iff I$ är maximalt.

Sats. Ett ideal $I \neq R$ är ett primideal om och endast om R/I saknar nolldelare (dvs.

$x \neq 0$, $y \neq 0$ s.a. $xy = 0$).

Bevis. Notera att $r + I$, $s + I$ är nolldelare om och endast om $r \notin I$, $s \notin I$ och

$$(r + I)(s + I) = I.$$

Men detta är ekvivalent med att $r \notin I$, $s \notin I$ och

$$rs \in I,$$

vilket per definition är detsamma som att I inte är ett primideal.

Korollarium. Varje maximalt ideal är ett primideal.

Bevis. Varje kropp saknar nolldelare.

Anmärkning. Om R är en $\mathbb{C}$-algebra kräver vi också av idealen att de är delvektorrum. Då är kvotringarna också $\mathbb{C}$-algebror. I alla våra exempel kommer detta att vara uppfyllt.

Exempel.

(i) Kvotringen $\mathbb{Z}/(k)$ är restklassringen modulo k. Om k är ett primtal p är idealet $(p) \subset \mathbb{Z}$ maximalt och kvotringen $\mathbb{Z}/(p)$ en kropp. Om $k = mn$ inte är ett primtal är klasserna för m och n nolldelare i $\mathbb{Z}/(k)$.

(ii) I $\mathbb{Q}[x]$ är idealet $(x^2 - 2)$ ett maximalt ideal eftersom $p(x) = x^2 - 2$ är irreducibelt över $\mathbb{Q}$. Kvotringen är $\mathbb{Q}[x]/(x^2 - 2) = \mathbb{Q}(\sqrt{2})$. I $\mathbb{R}[x]$ är av samma anledning $(x^2 + 1)$ maximalt och kvotringen $\mathbb{R}[x]/(x^2 + 1) = \mathbb{C}$.

(iii) I $\mathbb{C}[x, y]$ är idealet (x, y) förstås maximalt, med kvotring $\mathbb{C}$. Ideal genererade av ett irreducibelt polynom $p(x, y)$ är primideal, så t.ex. $\mathbb{C}[x, y]/(x^2 + y^2 - 1)$ saknar nolldelare. I motsats till detta har t.ex. $\mathbb{C}[x, y]/(xy)$ nolldelarna x och y eftersom $xy = 0$.

3 Repetition: Linjär algebra.

I den här kursen kommer ni att behöva kunna er linjära algebra. Nedan följer de grundläggande satser som vi kommer att använda. I alla satser är V, W etc linjära rum.

3.1 Grundläggande satser om linjära rum.

Vi formulerar den mesta teorin över en allmän kropp k, till skillnad från er kurs i Linjär algebra II, där allt görs med $k = \mathbb{R}$. Om ni går igenom bevisen ser ni dock lätt att det enda som används är kroppsaxiomen.

Definition. Linjärt rum över k.

Låt V vara ett linjärt rum över k.
Definition. Vektorer $\mathbf{v}_1, ..., \mathbf{v}_m$ i V kallas *linjärt oberoende* om

$$a_1\mathbf{v}_1 + ... + a_m\mathbf{v}_m = \mathbf{0} \implies a_1 = ... = a_m = 0.$$

Definition. Om $S \subset V$ kallas mängden av alla linjärkombinationer av element ur S med koefficienter i k det *linjära höljet* av S, span$S$.

Definition. En följd vektorer $\mathbf{v}_1, ..., \mathbf{v}_n$ kallas en *bas* för V om de är linjärt oberoende och $V = \text{span}\{\mathbf{v}_1, ..., \mathbf{v}_n\}$.

Sats. Varje bas för V har samma kardinalitet.

Definition. Kardinaliteten i satsen ovan kallas V:s *dimension.*

Definition. En funktion $F : V \to W$ kallas en *linjär avbildning* om

$$F(\mathbf{v} + \mathbf{w}) = F(\mathbf{v}) + F(\mathbf{w})$$

och

$$F(\lambda\mathbf{v}) = \lambda F(\mathbf{v}).$$

Sats. En linjär avbildning är unikt bestämd av sina värden på elementen i en bas.

Anmärkning. Ovanstående sats

Sats. Två vektorrum av samma dimension är isomorfa.

3.2 Kvadratiska former.

I detta avsnitt antar vi att $k = \mathbb{R}$ eller $\mathbb{C}$ eller åtminstone att char $k \neq 2$.

Definition. En funktion $q : V \to k$ kallas en *kvadratisk form* om det finns en bas $\mathbf{v}$ i V och en symmetrisk matris Q s.a.

$$q(\mathbf{r}) = [\mathbf{r}]_{\mathbf{v}}^t Q [\mathbf{r}]_{\mathbf{v}}.$$

Anmärkning. Det är lätt att se att detta är detsamma som en homogen polynomfunktion av grad 2 i n variabler (de n koordinaterna $(x_1, ..., x_n)$ i basen $\mathbf{v}$).

3.3 Reella kvadratiska former.

I kursen i Linjär algebra lär man sig ortogonal diagonalisering av symmetriska matriser över $\mathbb{R}$. T.ex. lär man sig följande sats:

Spektralsatsen. Varje reell symmetrisk $n \times n$-matris Q har n stycken reella egenvärden. Det finns en ON-bas i $\mathbb{R}^n$ bestående av egenvektorer till Q.

Ortogonal diagonalisering av kvadratiska former. Låt $q(\mathbf{r})$ vara en reell kvadratisk form och låt basbytesmatrisen från basen av egenvektorer till standardbasen vara matrisen T, så att $T^{-1}\mathbf{r} = \mathbf{u}$ är $\mathbf{r}$:s koordinater i basen av egenvektorer. Då är $q(\mathbf{r}) = q(T\mathbf{u}) = \mathbf{u}^t T^t Q T \mathbf{u}$. Med andra ord, i basen av egenvektorer ges den kvadratiska formen av den diagonala matrisen $T^t Q T$. I koordinater har den då formen

$$q(y_1, ..., y_n) = \lambda_1 y_1^2 + ... + \lambda_n y_k^2,$$

där λ_i är det i:te egenvärdet och vi har antagit att $n - k$ st egenvärden är 0.

Definition. *Signaturen* av en kvadratisk form q som ovan är paret (k_1, k_2) där k_1 är antalet positiva egenvärden och k_2 är antalet negativa egenvärden.

Ekvivalens av kvadratiska former. I en annan version av denna sats, som är viktigare för oss i denna kurs, tillåter vi oss allmänna basbyten, inte bara ortogonala.

Sats. Varje reell kvadratisk form kan, genom ett (inte nödvändigtvis ortogonalt) basbyte tas till standardformen

$$q(y_1, ..., y_n) = y_1^2 + ... + y_k^2 - y_{k+1}^2 - ... - y_{k+m}^2.$$

Här är k, m bestämda av den kvadratiska formen q, inte av valet av bas.

4 Lite flervariabelanalys.

Här repeterar vi några fakta om kurvor i det reella planet $\mathbb{R}^2$, som vi lärde oss i flervariabelkursen. Vi antar att alla funktioner är av klass $\mathcal{C}^\infty$.

4.1 Nivåkurvor, gradient, linjarisering och Taylorutveckling.

Definition. Låt $f : \mathbb{R}^n \to \mathbb{R}$ och $C \in \mathbb{R}$ ett tal. Mängden av lösningar till ekvationen $f = C$,

$$\{(x_1, ..., x_n) \in \mathbb{R}^n \mid f(x_1, ..., x_n) = C\},$$

kallas *nivåmängden till f hörande till värdet C*. Om vi är intresserade av en speciell nivåmängd kan vi alltid anta att $C = 0$ genom att istället undersöka $g = 0$, där $g = f - C$. Då talar vi om *nollställesmängden* till g.

Anmärkning. I denna kurs kommer vi att studera nivåkurvor till polynomfunktioner, främst av två variabler. Dessa kommer att kallas plana algebraiska kurvor.

Definition. Gradienten av $f : \mathbb{R}^n \to \mathbb{R}$ är vektorfältet

$$\nabla f = \left(\frac{\partial f}{\partial x_1}, ..., \frac{\partial f}{\partial x_n} \right).$$

Definition. Låt f vara som i föregående definition. *Linjariseringen* till f i punkten $\mathbf{r}_0$ är funktionen

$$L(\mathbf{r}) = f(\mathbf{r}_0) + \nabla f(\mathbf{r}_0) \bullet (\mathbf{r} - \mathbf{r}_0).$$

Anmärkning. Mer allmänt kan funktioner Taylorutvecklas till vilken önskad ordning som helst i närheten av en given punkt. Taylorutvecklingen till ordning n kan sägas vara det polynom av grad n (eller lägre), som ger den bästa approximationen till f i närheten av punkten ifråga. Linjariseringen är Taylorpolynomet av grad 1. Genom att linjarisera vänsterledet i ekvationen $f(x, y) = 0$ i någon lösningspunkt (a, b) får vi en linjär ekvation, vars lösningar är nära lösningarna till $f(x, y) = 0$ i närheten av (a, b). Detta ger följande definition.

Definition. *Tangentlinjen* till en kurva $f(x, y) = 0$ i en punkt (a, b), där $\nabla f(a, b) \neq (0, 0)$, är kurvan som ges av

$$\frac{\partial f}{\partial x}(a, b)(x - a) + \frac{\partial f}{\partial y}(a, b)(y - b) = 0.$$

Anmärkning. I högre dimension får vi tangentrum som lösningarna till

$$\nabla f(\mathbf{r}_0) \bullet (\mathbf{r} - \mathbf{r}_0) = 0.$$

4.2 Implicita funktionssatsen.

Sats. Låt $f(x, y)$ vara en glatt funktion på $\mathbb{R}^2$. Låt $(a, b) \in \mathbb{R}^2$ och antag att $f(a, b) = 0$. Om $\dfrac{\partial f}{\partial y}(a, b) \neq 0$ så finns en omgivning kring (a, b) i $\mathbb{R}^2$, sådan att kurvan $f(x, y) = 0$ i denna omgivning sammanfaller med en funktionsgraf $y = g(x)$ till en glatt funktion g. (Motsvarande påstående med x utbytt mot y gäller givetvis också.)

Exempel. Låt

$$f(x, y) = y^2 - x^3 - x.$$

Gradienten av $f(x, y)$ är då

$$\nabla f(x, y) = (-3x^2 + 1, 2y).$$

De enda punkter där $\nabla f(x, y) = (0, 0)$ är

$$(x, y) = (\pm \frac{1}{\sqrt{3}}, 0)$$

och ingen av dessa ligger på kurvan. Implicita funktionssatsen garanterar då att kurvan är (lokalt kring varje punkt) en parametriserbar glatt kurva, som kan beskrivas som grafen till en glatt funktion av en av koordinaterna x, y.

Exempel. Låt $g(x, y) = y^2 - x^3 - x^2$. Motsvarande övning för $g(x, y)$ ger att kurvan ifråga är glatt i alla punkter utom möjligen $(0, 0)$. Taylorutvecklar vi $g(x, y)$ till ordning 2 kring $(0, 0)$ får vi $g(x, y) \approx y^2 - x^2 = 0$ och ser att kurvan skär sig själv i $(0, 0)$ och lokalt alltså där ser ut som ett linjekors $(y - x)(y + x) = 0$.

Definition. Två kurvor $f(x, y) = 0$ och $g(x, y) = 0$ sägs ha *transversell skärning* i en punkt (a, b) om $f(a, b) = g(a, b) = 0$, $\nabla f(a, b) \neq (0, 0)$, $\nabla g(a, b) \neq (0, 0)$ och $\nabla f(a, b)$ och $\nabla g(a, b)$ är icke-parallella där (ekvivalent, tangentlinjerna är icke-parallella).

Övningar.

1. Gå igenom resonemanget med gradienträkningarna i förra stycket och kontrollera alla påståenden i detalj för dig själv. Se också till att du förstår hänvisningarna till implicita funktionssatsen och Taylorutveckling.
2. Se till att du förstår från deras ekvationer hur de två exempelkurvorna i förra uppgiften ser ut i sin helhet.
3. Gör samma analys av kurvan $(x^2 + y^2)^2 = x^2 - y^2$. Försök också skissa kurvan i sin helhet, genom att använda t.ex. symmetrier och metoder från en- och flervariabelanalys.
4. Försäkra dig om att ovanstående definition överensstämmer med din favoritdefinition av tangentlinjer.
5. Finn de reella skärningspunkterna mellan de två kurvorna $x^2 + y^2 = 1$ och $y = 1 - 2x^2$ och avgör om kurvorna skär varandra transversellt. Beräkna också kurvornas tangentlinjer i de givna punkterna.

5 Reell affin geometri.

5.1 Reella algebraiska kurvor.

Det huvudsakliga studieobjektet i denna kurs är *plana algebraiska kurvor*. Om k är en kropp kallar vi den kartesiska produkten $k \times k = k^2$ för det *affina planet*. Vi definierar algebraiska kurvor som vissa nivåmängder till polynom i detta plan.

Definition. En *plan affin algebraisk kurva* är nollställesmängden $V(f)$ till ett icke-konstant polynom $f \in k[x, y]$, dvs.

$$V(f) = \{(x, y) \in k^2 | f(x, y) = 0\} \subset k^2.$$

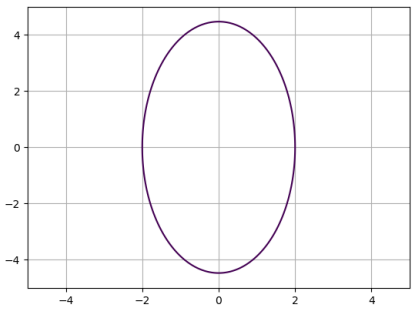


Figure 1: $\frac{x^2}{4} + \frac{y^2}{20} = 1$.

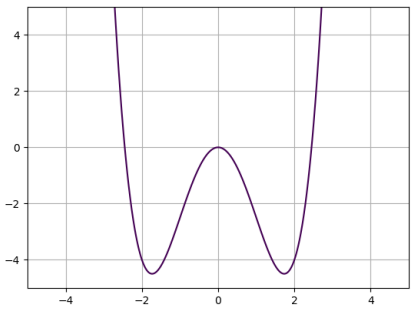


Figure 2: $y = \frac{x^4}{4} - 3x^2$.

Tillfällig begränsning. I detta kapitel låter vi $k = \mathbb{R}$ och tittar alltså på delmängder av $\mathbb{R}^2$ som ges som nollställena till *reella* polynom.

Exempel. Följande välbekanta mängder utgör exempel på algebraiska kurvor.

1. Linjer, beskrivna av $ax + by - c = 0$.
2. Ellipser $\frac{(x-x_0)^2}{a^2} + \frac{(y-y_0)^2}{b^2} - 1 = 0$.
3. Hyperbler $\frac{(x-x_0)^2}{a^2} - \frac{(y-y_0)^2}{b^2} - 1 = 0$.
4. Parabler $y = ax^2$, och mer allmänt grafer $y = f(x)$ till polynom $f(x)$ av en variabel.
5. Linjekors $xy = 0$ (unionen av x- och y-axlarna).

Det sista exemplet framstår kanske som något märkligt. Det verkar intuitivt sett vara mer *två* kurvor som skär varandra i en punkt, än *en* kurva. Vi kommer att reda ut detta i senare kapitel, så det finns ingen anledning till oro. Lösningen är att göra åtskillnad på *irreducibla* och *reducibla* kurvor, där linjekorset visar sig vara ett exempel på det senare. Följande exempel belyser till synes allvarligare problem med den givna definitionen.

Underliga exempel.

1. Kurvan $(x-a)^2 + (x-b)^2 = 0$ utgörs av en enstaka punkt (a, b). Det är väl inte så mycket till kurva alls kan man tycka. Den verkar alltför degenererad.
2. Än värre, polynomekvationen $x^2 + y^2 + 1 = 0$ har inga reella lösningar alls. Så *tomma mängden* måste betraktas som en algebraisk kurva enligt den definition vi har ovan. Nu börjar man vilja protestera än mer högljutt.

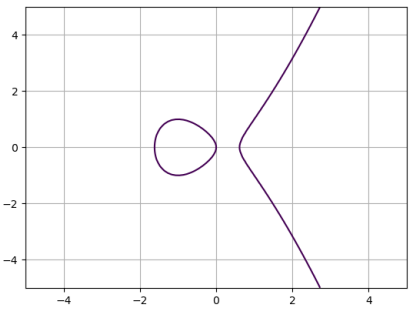


Figure 3: Kurvan $y^2 = x^3 - x$.

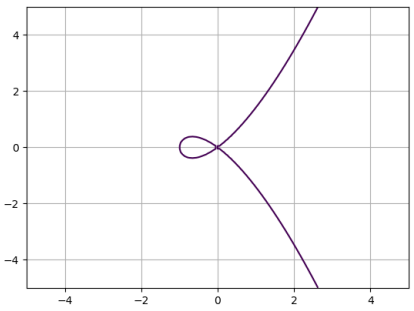


Figure 4: Kurvan $y^2 = x^3 + x^2$.

3. Många olika polynom kan ge upphov till samma nollställesmängd, t.ex. har ju f och f^n förstås alltid samma nollställen. Med användning av det förra exemplet ser vi också att t.ex. $x(x^2 + y^2 + 1) = 0$ beskriver y-axeln, precis som den enklare ekvationen $x = 0$ gör.

Om du tänker på fallet med polynom i en variabel, inser du att ovanstående underligheter har att göra med att $\mathbb{R}$ inte är en algebraiskt sluten kropp. När vi senare övergår till att acceptera komplexa lösningar, dvs. studerar *komplexa* plana affina kurvor i $\mathbb{C}^2$ kommer alla underligheterna i exemplet ovan att försvinna. Vi skjuter dock upp detta en stund och tittar på några fler mer väluppfostrade exempel.

Exempel. De tidigare exemplen är alla av grad ≤ 2. Här är några exempel på tredjegradskurvor (se figurerna ovan.)

1. $f(x, y) = y^2 - (x^3 - x) = 0$
2. $g(x, y) = y^2 - (x^3 + x^2) = 0$

Dessa kurvor studerade vi med analytiska metoder i förra avsnittet, där vi repeterade flervariabelanalys. Notera dock att derivator av polynom kan definieras utan hänvisning till några gränsvärden, enligt $\dfrac{\partial}{\partial x} x^n y^m = n x^{n-1} y^m$, osv. Speciellt är tangentlinjen till en kurva ett väldefinierat begrepp över varje kropp k.

Definition. En punkt (a, b) på en algebraisk kurva $f(x, y) = 0$ kallas *singulär* om $\nabla f(a, b) = (0, 0)$.

Övning. Finn eventuella reella singulära punkter till kurvan $x^2y^3 + x^2 + y^2 = 0$.

5.2 Begreppet klassificering.

Låt

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

vara en andragradskurva. Minst en av a, b, c antar vi är nollskild, eftersom vänsterledet annars inte har grad 2. I det här kapitlet ska vi försöka avgöra hur många 'typer' av sådana kurvor som finns. För detta måste vi bestämma oss för vad vi ska mena med 'typer'. Jämför med följande biologiska klassifikationsproblem: Vi kan klassificera djur i ganska grova kategorier som däggdjur, reptiler etc, eller vi kan vara mer precisa och skilja lejon från tigrar, ormar från krokodiler osv. Vilken klassifikation vi väljer lägger fokus på olika egenskaper hos objekten och beror på vad vi ska använda klassifikationen till. På samma sätt kan vi välja en klassifikation som betraktar två ellipser lika om de har samma halvaxlar eller vi kan t.ex. säga att en övergripande skalningsfaktor inte ska spela någon roll (och därigenom t.ex. betrakta alla cirklar som ekvivalenta). Det första är rimligt om vi vill betrakta kurvorna som fysikaliska stela kroppar så att vi vill att de längdmätningar vi utför på dem ska speglas i klassifikationen. Men det senare kan vara rimligt om t.ex. arbetar med en spelgrafik där vi vill kunna titta på samma objekt i spelet från olika avstånd. Då kan ju samma ellips se olika stor ut. Och den cirkulära randen på en mugg ser ju t.o.m elliptisk ut sedd från sidan!

För att få ett precist sätt att tala om klassifikation använder vi i matematiken funktioner och identifierar (betraktar som ekvivalenta) två objekt om de på något sätt kan överföras i varandra med hjälp av funktioner ur en fixerad klass. Det enklaste exemplet är ändliga mängder, som vi kan betrakta som ekvivalenta om de har samma kardinalitet. Detta kan vi definiera med hjälp av funktioner, genom att säga att det ska finnas en bijektion från den ena till den andra mängden.

Ett något mer avancerat exempel på detta har ni sett i den linjära algebran, där två linjära rum betraktas som ekvivalenta om det finns en linjär bijektion (isomorfi) från det ena till det andra. Man visar att det i denna mening finns exakt ett linjärt rum av varje dimension ≥ 0.

Ett sista exempel, är klassificeringen av reella kvadratiska former, som nämns i repetitionskapitlet för linjär algebra ovan. Ett sätt att klassificera dessa är med hjälp av ortogonala avbildningar. Då är två kvadratiska former "desamma" om deras matriser har samma egenvärden. Alternativt kan vi klassificera reella kvadratiska former upp till allmänna linjära inverterbara avbildnignar och då betrakta två kvadratiska former som ekvivalenta om de har samma signatur.

5.3 Affina och euklidiska transformationer

Från linjär algebra är ni bekanta med linjära avbildningar. Sådana kommer att spela en stor roll i denna kurs också. Men vi vill också kunna translatera geometriska objekt från en plats till en annan utan att rotera dem (dvs. till varje ortsvektor addera en fix vektor).

Definition. Låt $\mathbf{a} \in \mathbb{R}^n$. Avbildningen $T_{\mathbf{a}} : \mathbb{R}^n \to \mathbb{R}^n$ given av $T_{\mathbf{a}}(\mathbf{v}) = \mathbf{v} + \mathbf{a}$, kallas *translation* med $\mathbf{a}$.

Notera att om $\mathbf{a} \neq 0$ så är $T_{\mathbf{a}}$ inte linjär (varför?). Avbildningar som vi får genom att till de linjära avbildningarna lägga till translationer kallas *affina*. De kommer att spela en stor roll i denna kurs.

Definition. En avbildning på formen $F(\mathbf{v}) = L(\mathbf{v}) + \mathbf{a}$ $(= (T_{\mathbf{a}} \circ L)(\mathbf{v}))$, där L är linjär och $\mathbf{a}$ är en vektor kallas en *affin avbildning*. Om L är bijektiv kallas F en *affin transformation*.

Anmärkning. Notera att den linjära avbildningen L normalt beskrivs av multiplikation med en $n \times n$-matris.

Exempel: Avbildningen

$$F\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 4 & -2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

är en affin transformation $F : \mathbb{R}^2 \to \mathbb{R}^2$. Om vi avstår matrisnotation kan vi istället skriva $F(x, y) = (3x + 2, 4x - 2y + 1)$.

Sats.

(a) Sammansättningen av två affina avbildningar är affin.

(b) Affina transformationer är inverterbara.

(c) Bilden av en linje under en affin transformation är en linje.

(d) Affina transformationer bevarar parallellitet.

(e) Affina transformationer bevarar transversalitet.

Bevis.

(a) Låt $F(\mathbf{v}) = L(\mathbf{v}) + \mathbf{a}$ och $G(\mathbf{w}) = M(\mathbf{w}) + \mathbf{b}$ vara två affina avbildningar. Sammansättningen blir då:

$$G(F(\mathbf{v})) = G(L(\mathbf{v}) + \mathbf{a}) = M((L(\mathbf{v}) + \mathbf{a})) + \mathbf{b} = (ML)(\mathbf{v}) + (M(\mathbf{a}) + \mathbf{b}),$$

som är affin.

(b) Övning. Ange en formel för inversen.

(c) Detta torde vara geometriskt uppenbart. Om linjen framställs på parameterform som $\mathbf{r}(t) = \mathbf{v}t + \mathbf{r}_0$ får vi

$$F(\mathbf{r}(t)) = F(\mathbf{v}t + \mathbf{r}_0) = A(\mathbf{v}t + \mathbf{r}_0) + \mathbf{a} = A(\mathbf{v})t + (A(\mathbf{r}_0) + \mathbf{a}),$$

vilket också är en linje på parameterform.

(d) Jämför med (c). Om två linjer har parallella riktningsvektorer har deras bilder det också.

(e) Om två kurvor skär varandra så att deras tangentvektorer är icke-parallella så gäller detsamma bilderna av tangentvektorerna, eftersom den affina transformationens derivata är L, som är en linjär isomorfi. (Mer allmänt gäller påståendet (e) för diffeomorfier.)

Anmärkning. (a) och (b) tillsammans med det uppenbara faktum att identitetsavbildningen är en affin transformation, visar att mängden av affina transformationer på $\mathbb{R}^n$ utgör en *grupp*.

Definition. Gruppen av affina transformationer av $\mathbb{R}^n$ betecknar vi med $\mathrm{Aff}(n)$.

Sats. Låt F vara en affin transformation.

(a) Om $f(x, y)$ är ett polynom av grad k så är $f(F(x, y))$ också av grad k. (Notera att detta implicerar förra satsens c-del om $k = 1$.)

(b) Om A, B, C, D är kolinjära (dvs. ligger på samma linje) bevarar F längdförhållanden dem emellan, dvs. om vi med $|\overline{AB}|$ betecknar vektorn från A till B, $\dfrac{|\overline{AB}|}{|\overline{CD}|} = \dfrac{|\overline{F(A)F(B)}|}{|\overline{F(C)F(D)}|}$.

Bevis.

(a) Eftersom F:s komponenter är polynom av grad ≤ 1 så är det uppenbart att $\deg f(F(x, y)) \leq \deg f(x, y)$. Men eftersom inversen F^{-1} också är affin har vi även

$$\deg f(x, y) = \deg f(F^{-1}(F((x, y)))) \leq \deg f(F(x, y)),$$

så resultatet följer.

(b) Beteckna med $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$, $\mathbf{d}$ ortsvektorerna för de givna punkterna och skriv $\mathbf{b} - \mathbf{a} = \lambda(\mathbf{d} - \mathbf{c})$, så att vi har $\dfrac{|\overline{AB}|}{|\overline{CD}|} = |\lambda|$. Vi får (med $F(\mathbf{v}) = L(\mathbf{v}) + \xi$):

$$\frac{|\overline{F(A)F(B)}|}{|\overline{F(C)F(D)}|} = \frac{|F(\mathbf{b}) - F(\mathbf{a})|}{|F(\mathbf{d}) - F(\mathbf{c})|} = \frac{|L(\mathbf{b}) + \xi - \mathbf{L}(\mathbf{a}) - \xi|}{|L(\mathbf{d}) + \xi - \mathbf{L}(\mathbf{c}) - \xi|} = \frac{|L(\mathbf{b} - \mathbf{a})|}{|L(\mathbf{d} - \mathbf{c})|} = \frac{|L(\lambda(\mathbf{d} - \mathbf{c}))|}{|L(\mathbf{d} - \mathbf{c})|} = |\lambda|.$$

Definition. Om L i definitionen av affin transformation är en *ortogonal* linjär avbildning kallar vi F en *euklidisk transformation*.

Ortogonala linjära avbildningar torde vara välbekanta från den linjära algebrans studium av inre produktrum, men om du har glömt följer här definitionen.

Definition. En linjär avbildning $A : \mathbb{R}^n \to \mathbb{R}^n$ kallas *ortogonal* om $AA^t = I = A^tA$.

Anmärkning. Poängen med ortogonala avbildningar är att de bevarar skalärprodukten $\langle A\mathbf{v}, A\mathbf{w}\rangle = \langle \mathbf{v}, \mathbf{w}\rangle$ och därför längder och vinklar, vilka ju definieras med hjälp av denna.

Definition. En affin transformation $F : \mathbb{R}^n \to \mathbb{R}^n$ inducerar en avbildning

$$F^* : \mathbb{R}[x_1, ..., x_n] \to \mathbb{R}[x_1, ..., x_n]$$

via $F^*(f) = f \circ F$. Vi kallar F^* den av F *inducerade avbildningen*. Vi säger att två polynom f och g är *affint ekvivalenta* om det finns ett tal $\lambda \in \mathbb{R} \setminus \{0\}$ så att $\lambda g = F^*(f)$ för någon affin

transformation F.

Anmärkning. Vi kommer att nästan uteslutande betrakta fallet $n = 2$ i denna kurs.

Anmärkning. Observera att den inducerade avbildningen bara är ett sofistikerat sätt att tala om affina variabelbyten. Om t.ex. $F(x, y) = (x + 2y, 3y + 1)$ och $f(x, y) = x^2 + y^2$ så är $F^*(f)(x, y) = (x + 2y)^2 + (3y + 1)^2 = x^2 + 13y^2 + 4xy + 6y + 1$.

Anmärkning. Talet λ i definitionen kommer sig av att vi egentligen är intresserade av polynomets ifråga nollställesmängd. T.ex. har ju $x^2 + 1$ och $2x^2 + 2$ samma nollställesmängd, men det finns inget affint variabelbyte som transformerar det ena polynomet till det andra.

Definition. Om R är en ring betecknar vi med $\mathrm{Aut}(R)$ mängden av alla ringisomorfismer från R till sig själv (sådana kallas också ringautomorfismer, varav beteckningen).

Sats. Avbildningen $F^* : \mathbb{R}[x_1, ..., x_n] \to \mathbb{R}[x_1, ..., x_n]$ är en ringisomorfism. Rentav är den faktiskt en $\mathbb{R}$-algebraisomorfism, dvs. den uppfyller också $F^*(\lambda f) = \lambda F^*(f)$.

Bevis. Vi behöver visa $F^*(f + g) = F^*(f) + F^*(g)$, $F^*(fg) = F^*(f)F^*(g)$ och $F^*(1) = 1$ samt $F^*(\lambda f) = \lambda F^*(f)$. Detta lämnas med varm hand till läsaren.

Sats. Avbildningen $(-)^* : \mathrm{Aff}(n) \to \mathrm{Aut}(\mathbb{R}[x_1, ..., x_n])$ som ges av $F \mapsto F^*$ har följande egenskaper[3].

- $id^*_{\mathbb{R}^n} = id_{\mathbb{R}[x_1,...,x_n]}$
- $(F \circ G)^* = G^* \circ F^*$

Bevis. Rättframt.

Sats. Relationen på $\mathbb{R}[x_1, ..., x_n]$ given av

$$f \sim g \iff \exists F \in \mathrm{Aff}(n), \exists \lambda \in \mathbb{R} \setminus \{0\} : \lambda g = F^*(f),$$

är en ekvivalensrelation.

Bevis. Detta följer enkelt från de två föregående satserna.

Kom ihåg att vi betecknade med $V(f)$ nollställesmängden till f i k^2.

Sats. Om $(x, y) \in V(f)$ så är $F^{-1}(x, y) \in V(F^*(f))$.

Bevis. Uppenbart.

[3]För den som är bekant med sådan terminologi (eller vill bli det) betyder detta precis att ϕ definierar en *gruppverkan från höger* av gruppen $\mathrm{Aff}(n)$ på $\mathbb{R}[x, y]$

Anmärkning. Poängen med denna sats är bara att notera att kurvor är affint ekvivalenta om deras definierande polynom är det.

Övningar.

1. Visa att varje translation är inverterbar.
2. Visa att varje affin transformation är inverterbar och finn en allmän formel för inversen.
3. Beteckna med $T_{\mathbf{a}}$ den affina avbildningen som är translation med vektorn $\mathbf{a}$. Låt F vara en linjär inverterbar avbildning. Visa att $F \circ T_{\mathbf{a}} \circ F^{-1} = T_{F(\mathbf{a})}$.
4. Visa att bilden av en konvex mängd under en affin avbildning är konvex.
5. Visa att om P är en singulär punkt på en kurva $p = 0$ så är $F^{-1}(P)$ en singulär punkt på kurvan $F^*(p) = p \circ F = 0$
6. Låt $f(x, y) = 2x^2 + 2xy + 13y^2 - 1$. och $F(x, y) = \frac{1}{5}(2x + 3y, x - y)$. Beräkna $F^*(f(x, y))$.
7. Utgå ifrån förra uppgiften. Skissa kurvorna $f(x, y) = 0$ och $F^*(f(x, y))$.
8. Visa satsen ovan: Om $(x, y) \in V(f)$ så är $F^{-1}(x, y) \in V(F^*(f))$.

5.4 Klassificering av reella linjer i planet.

Vi sticker emellan med ett kort men viktigt påpekande som uppvärmning för klassificeringsprojektet i nästa avsnitt, nämligen att det upp till affina transformationer bara finns en linje i planet.

Sats. Alla linjer i $\mathbb{R}^2$ är affint (rentav euklidiskt) ekvivalenta.

Bevis. Geometriskt är det förstås trivialt att vi kan translatera linjen så att den går igenom origo och sedan rotera den så att den är vertikal, men vi ger ett algebraiskt bevis som uppvärmning för nästa avnitt, där beviset vi ska genomföra är mindre geometriskt uppenbart. Låt L vara en linje $ax + by = c$ i $\mathbb{R}^2$. Om $a \neq 0$ så tar den affina transformationen $x' = ax + by - c, y' = y$ L till linjen med ekvationen $x' = 0$ i $x'y'$-systemet. Om $a = 0$ kan vi sätta $x' = y - c/b$ och $y' = x$ med samma resultat. (Med marginellt mer arbete kan du förstås rentav skriva ned ett ortogonalt variabelbyte som gör samma jobb.)

5.5 Klassificering av reella andragradspolynom upp till affina transformationer.

Vi kommer i detta avsnitt att visa att varje andragradspolynom är ekvivalent med ett polynom på en viss standardform, där ekvivalens som i förra kapitlet betyder upp till affina transformationer och multiplikation med nollskilda konstanter.

Sats. Varje andragradspolynom av grad 2 över $\mathbb{R}$ är ekvivalent med exakt ett av följande polynom. Nollställesmängdens typ står beskriven i parentes.

(a) $x^2 + y^2 - 1$ (Cirkel.)

(b) $x^2 - y^2 - 1$ (Hyperbel.)

(c) $x^2 - y$ (Parabel.)

(d) $x^2 - y^2$ (Linjekors.)

(e) $x^2 + y^2$ (Punkt.)

(f) $x(x-1)$ (Två parallella linjer.)

(g) x^2 (En 'dubbellinje'.)

(h) $x^2 + 1$ (Tomma mängden.)

(i) $x^2 + y^2 + 1$ (Tomma mängden.)

Bevis. Låt

$$p(x,y) = ax^2 + bxy + cy^2 + dx + ey + f = Q(x,y) + dx + ey + f,$$

vara ett allmänt andragradspolynom med reella koefficienter. Vi antar att $a^2 + b^2 + c^2 \neq 0$, eftersom polynomet annars är av grad mindre än 2. Vi kan skriva uttrycket på matrisform om vi vill, enligt:

$$p(x,y) = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} d & e \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + f.$$

Vi ska nu transformera detta polynom till en "standardform", mha affina transformationer och multiplikation med konstanter. Vi börjar med att utföra ett linjärt koordinatbyte (basbyte) sådant att den kvadratiska formen i de nya koordinaterna, som vi också betecknar (x, y) ges av en diagonalmatris, där elementen på diagonalen är ± 1 eller 0. Något diagonalelement måste vara nollskilt och vi kan, efter att eventuellt ha multiplicerat med -1, anta att koefficienten framför x^2 är $+1$. Uttryckt i de nya koordinaterna får p då formen

$$p(x,y) = x^2 + \lambda y^2 + Dx + Ey + f,$$

där $\lambda \in \{1, -1, 0\}$. Observera att det givna variabelbytet är linjärt, så de nya koordinaterna är linjära uttryck i de gamla koordinaterna: $F(x,y) = (\alpha x + \beta y, \gamma x + \delta y)$. Alltså omvandlas uttrycket $dx + ey$ till $Dx + Ey$ för några konstanter D, E. Nu behöver vi dela upp vår vidare analys i flera fall.

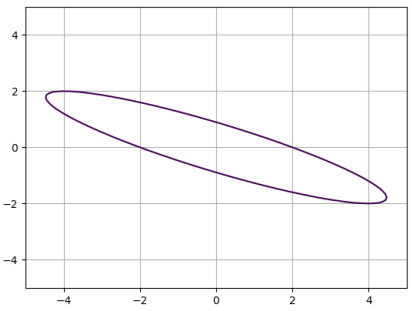


Figure 5: Kurvan $x^2 + 5y^2 - 4xy = 4$. En ellips.

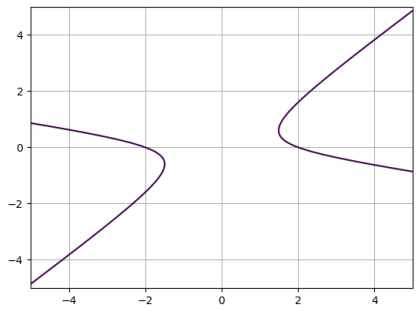


Figure 6: Kurvan $x^2 - 5y^2 - 4xy = 4$. En hyperbel.

5.5.1 Fall A. $\lambda = \pm 1$.

Vi kan då kvadratkomplettera

$$p(x,y) = (x + \frac{D}{2})^2 - \frac{D^2}{4} + \lambda(y + \frac{E}{2\lambda})^2 - \frac{E^2}{4\lambda} + f.$$

Om vi nu utför translationen $x \mapsto x - \frac{D}{2}$, $y \mapsto y - \frac{E}{2\lambda}$ och kallar konstanten, för läsbarhetens skull, för $F = f - \frac{D^2}{4} - \frac{E^2}{4\lambda}$, så får vi polynomet

$$x^2 + \lambda y^2 + F.$$

Vi får nu dela upp i fall.

Om $F = 0$ har vi direkt, eftersom $\lambda = \pm 1$, polynomet

$$x^2 \pm y^2,$$

som är något av uttrycken i (d) respektive (e).

Om $F \neq 0$ kan vi göra transformationen $T(x,y) = (\sqrt{|F|}x, \sqrt{|F|}y)$ och få, i fallet $\lambda = 1$,

$$x^2 + \lambda y^2 + F \sim (\sqrt{|F|}x)^2 + (\sqrt{|F|}y)^2 + F =$$

$$= |F|(x^2 + y^2 \pm 1) \sim x^2 + y^2 \pm 1,$$

vilket är uttrycken i (a) respektive (i), och i fallet $\lambda = -1$,

$$x^2 - y^2 + F \sim x^2 - y^2 \pm 1 \sim x^2 - y^2 - 1,$$

vilket är uttrycket i (b).

5.5.2 Fall B. $\lambda = 0$.

Vi kvadratkompletterar i x på samma sätt som ovan och får:

$$p(x,y) \sim (x + \frac{D}{2})^2 - \frac{D^2}{4} + Ey + f.$$

Fall B1. $E \neq 0$. Om $E \neq 0$ skriver vi de sista tre termerna som $E(y + f/E - D^2/4E)$ och gör translationen $T(x,y) = (x - \frac{D}{2}, y - f/E + D^2/4E)$. Detta ger polynomet

$$Ey + x^2 \sim E(y/(-E)) + x^2) = x^2 - y,$$

som i (c).

Fall B2. $E = 0$. Om $E = 0$ är $p(x,y) = (x + D/2)^2 + F$, vilket om vi gör transformationen $T(x,y) = (x - D/2, y)$ blir $x^2 + F$. Om $F = 0$ är detta polynom detsamma som i (g) och om $F \neq 0$ kan det transformeras vidare enligt

$$X^2 + F \sim (\sqrt{|F|}X)^2 + F = |F|(X^2 \pm 1) \sim X^2 \pm 1.$$

I fallet med plustecken är detta (h) och i fallet med minustecken kan det faktoriseras och visas ekvivalent med (f).

Vi måste också visa att inga av dessa nio polynom är ekvivalenta med varandra. Signaturen hos den kvadratiska formen är en invariant. Signaturen $(1,1)$ förekommer i fallen (a), (e) och (i). Affina transformationer bevarar kardinaliteten hos nollställesmängden så dessa tre är sinsemellan icke-ekvivalenta. Signaturen $(1,-1)$ förekommer i fallen (b) och (d). Affina transformationer bevarar singulära punkter. En sådan förekommer i (d) men inte i (b) så dessa är olika. Signaturen $(1,0)$ förekommer i (c),(f),(g) och (h). Affina transformationer avbildar varje linje på *en* linje, vilket räcker för att skilja dessa fall åt. Detta avslutar beviset.

Övningar.

1. Klassificera följande andragradskurvor och ange en affin transformation som tar dem till standardformen i satsen ovan. Om två av dem är ekvivalenta, ange en affin transformation som tar den ena till den andra.

   (a) $x^2 + 2xy + y^2 + 3x + y - 1 = 0$

   (b) $xy = 0$

   (c) $x^2 + y^2 + 2xy + 4x + 4y + 4 = 0$

   (d) $x^2 + 4y^2 - 1 = 0$

   (e) $x^2 - 2xy + y^2 = 0$

   (f) $x^2 - y^2 - 2xy + x - 3y + 2 = 0$

6 Algebraiska kurvor.

6.1 Irreducibilitet hos kurvor.

I följande definition kan k i princip vara vilken kropp som helst, även om vi i denna kurs håller oss till $\mathbb{R}$ eller $\mathbb{C}$.

Definition. En *algebraisk kurva* är nollställesmängden $V(f)$ till ett polynom: $f(x,y) \in k[x,y]$ är

$$V(f) = \{(x,y) \in k^2 | f(x,y) = 0\}.$$

Sats. Om $f(x,y) = p(x,y)q(x,y)$ är $V(f) = V(p) \cup V(q)$.

Bevis. Övning.

Definition. Eftersom f har en unik faktorisering i irreducibla faktorer, är $V(f)$ på ett entydigt sätt unionen av nollställesmängderna till dessa faktorer. Var och en av dem kallas en *irreducibel komponent* av $V(f)$.

Anmärkning. Över en icke algebraiskt sluten kropp kan det hända att en faktor saknar nollställen så att $V(f) = V(fg)$. T.ex. har polynomet $f(x) = x^2 + 1$ inga reella nollställen, så $V((x+y)(x^2+1)) = V(x+y)$ över $\mathbb{R}$. Det indikerar att för en elegant teori bör vi egentligen arbeta över $\mathbb{C}$ snarare än över $\mathbb{R}$. Då kommer algebra och geometri att ligga närmare varandra.

Anmärkning. Ett polynom kan ha multipla faktorer, vilket inte påverkar nollställesmängden: t.ex. $V(y-x^2) = V((y-x^2)^2)$. Det finns tillfällen då det är naturligt att betrakta nollställesmängder med 'högre multiplicitet'. Det enklaste fallet är i en variabel: De två polynomen $f(x) = x$ and $g(x) = x^2$ har samma nollställesmängd, dvs. bara $\{0\}$ men vi vet att det är 'rätt' att räkna g:s nollställe 'med multiplicitet 2'. En högre dimensionell variant av samma sak hände i klassifikationen av affina andragradskurvor i förra kapitlet, där 'dubbellinjen' $x^2 = 0$ naturligt dök upp.

Det är en nu naturlig fråga att ställa hur snittet mellan de irreducibla komponenterna kan se ut. Vi svarar på fråga i nästa avsnitt.

6.2 En sats om algebraiska kurvor.

Vi bevisar här att två algebraiska kurvor antingen skär varandra i ändligt många punkter eller sammanfaller längs en hel irreducibel komponent. Beviset är överkurs och kommer inte på tentan.

Sats. Låt k vara vilken kropp som helst. Låt $f(x,y)$, $g(x,y) \in k[x,y]$ och antag att $f(x,y)$ är irreducibelt. Antag vidare att $f(x,y)$ inte delar $g(x,y)$. Då har ekvationssystemet $f(x,y) = 0 = g(x,y)$ endast ändligt många lösningar.

Bevis. Vi börjar med slutklämmen. Vi kommer att kunna visa att vi kan skriva

$$u(x,y)f(x,y) + v(x,y)g(x,y) = a(y), \quad (*)$$

där $u, v \in k[x,y]$ och $a(y) \in k[y] \setminus \{0\}$. Men då ser vi att om $f(a,b) = g(a,b) = 0$ så blir vänsterledet noll och $y = b$ måste vara ett av de ändligt många nollställena till $a(y)$. För varje sådant b är $f(x,b)$ ett (nollskilt[4]) polynom av en variabel och det finns bara ändligt många nollställen $x = a$ också. Således finns bara ändligt många lösningar (a,b) till systemet.

Var kommer då likheten (*) ifrån? För att visa den betraktar vi tillfälligtvis $f(x,y)$ och $g(x,y)$ som polynom i en variabel x med koefficienter i kroppen $k(y)$ av *rationella funktioner* i y. Med andra ord $f, g \in k(y)[x]$. Nedan ska jag visa att f fortfarande är irreducibelt i denna större ring och att f fortfarande inte delar g. Detta innebär att f och g är relativt prima och vi kan skriva[5]

$$U(x,y)f(x,y) + V(x,y)g(x,y) = 1, \quad (**)$$

för några $U(x,y)$ och $V(x,y) \in k(y)[x]$. Explicit kan U och V skrivas på formen

$$U(x,y) = \frac{g_m(y)}{d_m(y)}x^m + ... + \frac{g_1(y)}{d_1(y)}x + \frac{g_0(y)}{d_0(y)}.$$

$$V(x,y) = \frac{h_n(y)}{e_n(y)}x^n + ... + \frac{h_1(y)}{e_1(y)}x + \frac{h_0(y)}{e_0(y)},$$

där alla d, e, g, h är polynom i y. Om vi alltså multiplicerar (**) med $a(y) = d_0(y)...d_m(y)e_0(y)...e_n(y)$ får vi (*), där $u(x,y) = a(y)U(x,y)$ och $v(x,y) = a(y)V(x,y)$).

Nu återstår bara att visa att $f(x,y)$ och $g(x,y)$ verkligen är relativt prima betraktade som element i $k(y)[x]$. Antag först att f är reducibelt och därför kan skrivas på formen[6]

$$f(x,y) = \left(\frac{g_m(y)}{d_m(y)}x^m + ... + \frac{g_1(y)}{d_1(y)}x + \frac{g_0(y)}{d_0(y)}\right)\left(\frac{h_n(y)}{e_n(y)}x^n + ... + \frac{h_1(y)}{e_1(y)}x + \frac{h_0(y)}{e_0(y)}\right).$$

Multiplicerar vi med alla nämnare får vi en identitet i $k[x,y]$:

$$A(y)f(x,y) = (g_m(y)x^m + ... + g_1(y)x + g_0(y))(h_n(y)x^n + ... + h_1(y)x + h_0(y)),$$

Nu kan vi använda unik faktorisering på högerledets faktorer och samla ihop de faktorer som tillhör $A(y)$. Vi får då:

$$A(y)f(x,y) = A(y)(\hat{g}_m(y)x^m + ... + \hat{g}_1(y)x + \hat{g}_0(y))(\hat{h}_n(y)x^n + ... + \hat{h}_1(y)x + \hat{h}_0(y)).$$

Detta medför att $f(x,y)$ är reducibelt i $k[x,y]$, vilket är en motsägelse. Således är $f(x,y)$ irreducibelt i $k(y)[x]$.

[4]Om $f(x,b)$ vore nollpolynomet skulle $y - b$ dela $f(x,y)$ men f är ju irreducibelt.

[5]Här använder vi Bezouts lemma i polynomringen i en variabel över kroppen av rationella funktioner i y, $k(y)$.

[6]Jag återanvänder samma symboler som ovan men det är förstås inte samma funktioner!

Om f antas dela g i $k(y)[x]$ får vi:

$$g(x,y) = f(x,y)\left(\frac{g_m(y)}{d_m(y)}x^m + ... + \frac{g_1(y)}{d_1(y)}x + \frac{g_0(y)}{d_0(y)}\right).$$

Multiplicerar vi med alla nämnare här så får vi en identitet i $k[x,y]$ på formen:

$$B(y)g(x,y) = f(x,y)(g_m(y)x^m + ... + g_1(y)x + g_0(y)),$$

vilken betyder att $f(x,y)$ delar $g(x,y)$ eftersom $f(x,y)$ är en irreducibel faktor och antingen måste dela $B(y)$ (vilket är omöjligt) eller $g(x,y)$. Detta avslutar beviset av att f och g är relativt prima och att användningen av Bezouts lemma ovan är giltig.

7 Bezouts sats, diskussion

Ett av huvudmålen med den här kursen är att bevisa Bezouts sats. Lite oprecist uttryckt säger den följande.

Pseudosats. (Bezout) Två algebraiska kurvor av grad m respektive n skär varandra i mn punkter.

Detta är som ni ser en oerhört elegant, naturlig och kraftfull sats, med den enda olyckliga bristen att den är uppenbart falsk. Låt oss se vad det är som inte stämmer. I figuren nedan ser vi en parabel (grad 2) och tre linjer (var och en grad 1). Den heldragna linjen och parabeln skär varandra i två ($2 \cdot 1 = 2$) punkter, vilket stämmer med vår pseudosats, så allt verkar vara frid och fröjd. Om vi istället betraktar den prickade linjen, så skär den dock inte parabeln i några punkter alls. Det verkar inte bra. Vad ska vi göra? Om vi räknar på saken inser vi att problemet här är att vi ritar kurvorna i det reella planet. Parabeln kan här vara kurvan $y = x^2$ och linjen $y = C$. Vi ser att om $C > 0$ finns två skärningspunkter, vilka båda har reella koordinater. Om $C < 0$ finns algebraiskt sett fortfarande två lösningar, men de har komplexa koordinater $(0, \pm\sqrt{-C}) \in \mathbb{C}$. Så om vi arbetar komplext, verkar vår pseudosats överleva. Men detta är tyvärr inte det enda problemet. Om $C = 0$ i vårt exempel (vilket i bilden motsvarar den streckade linjen) har vi bara en skärningspunkt $(0,0)$, även om vi räknar. Men om vi tittar noga inte bara på hur många skärningspunkter vi har, utan också hur kurvorna beter sig i närheten av skärningspunkten, inser vi att det ändå finns en kvalitativ geometrisk skillnad. I de andra (åtminstone de reella, som vi kan se) skärningspunkterna skär kurvorna varandra transversellt (som ett X, med linjärt oberoende tangentvektorer), men här tangerar de varandra. Vi skulle behöva hitta ett sätt att räkna skärningspunkterna med multiplicitet. Den vaksamma läsaren noterar förstås att vi här har att göra med samma problem som i 'envariabelalgebra' där ett komplext polynom av grad n har nollställen om de räknas med multiplicitet. Här vore det rimligt att räkna nollstället med multiplicitet 2. Isåfall skulle pseudosatsen undvika detta problem.

Tyvärr är vi inte ute ur skogen än. Det återstår ändå märkligheter, redan med de enklaste av alla plana kurvor, linjerna. Begrunda nämligen fallet med två parallella linjer. Dessa borde enligt Bezouts pseudosats skära varandra i en punkt, men de skär inte varandra alls! Ack! Är då

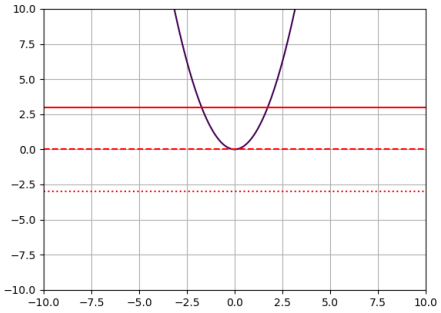


Figure 7: Tre olika konfigurationer av en parabel och en linje.

allt förlorat? Alls inte. Det visar sig att det finns en naturlig lösning på detta också. Vi kommer i senare kapitel att lägga till oändligheten på ett fiffigt sätt till planet, så att parallella linjer får någonstans att skära varandra. Det affina planet med en oändlighet på detta sätt kommer att kallas det projektiva planet och geometri i detta kommer att kallas projektiv geometri.

Vi har alltså tre saker att fixa. Vi behöver *komplexa tal*, *skärningsmultiplicitet* samt *projektiv geometri*. Vi tar itu med dem ordentligt en i taget i de följande kapitlen.

8 Komplex affin geometri.

8.1 Komplexa affina linjer och kurvor.

En linje i $\mathbb{C}^n$ på parameterform är per definition mängden av punkter $\mathbf{r} = (z_1, ..., z_n)$ som kan skrivas

$$\mathbf{r} = \mathbf{r}_0 + t\mathbf{v},\ t \in \mathbb{C},$$

för några $\mathbf{r}_0, \mathbf{v} \in \mathbb{C}$. Om $n = 2$ kan varje linje också beskrivas med en ekvation på formen $ax + by = c$, genom att parametern t elimineras (samma räkningar som i reella fallet!). Två linjer på parameterform kallas parallella om deras riktningsvektorer $\mathbf{v}$ är komplexa multipler av varandra. En linje på formen $a'x + b'y = c'$ är då parallell med ovanstående linje $ax + by = c$ om och endast om $(a, b) = (ka, kb)$ för något $k \in \mathbb{C}$.

Sats. Genom varje par av skilda punkter i $\mathbb{C}^n$ går exakt en komplex linje.

Bevis. Antag att de två linjerna $\mathbf{r} = \mathbf{r}_0 + t\mathbf{v}$, $t \in \mathbb{C}$ resp $\mathbf{u} = \mathbf{u}_0 + s\mathbf{w}$, $s \in \mathbb{C}$, båda innehåller två punkter, med parametervärden t_i och s_i. Detta ger oss två ekvationer enligt nedan:

$$\mathbf{r}_0 + t_i\mathbf{v} = \mathbf{u}_0 + s_i\mathbf{w},\ i \in \{1, 2\}.$$

Subtraheras den andra ekvationen från den första får vi:

$$(t_1 - t_2)\mathbf{v} = (s_1 - s_2)\mathbf{w}$$

så att $\mathbf{w} = \dfrac{t_1 - t_2}{s_1 - s_2}\mathbf{v}$. Vi använder detta för att i ekvationen

$$\mathbf{u}_0 = \mathbf{r}_0 + t_1\mathbf{v} - s_1\mathbf{w},$$

uttrycka $\mathbf{w}$ i termer av $\mathbf{v}$ och får

$$\mathbf{u}_0 = \mathbf{r}_0 + \left(t_1 - s_1\frac{t_1 - t_2}{s_1 - s_2}\right)\mathbf{v}.$$

Till slut kan vi skriva

$$\mathbf{u} = \mathbf{u}_0 + s\mathbf{w} = \mathbf{r}_0 + \left(t_1 - s_1\frac{t_1 - t_2}{s_1 - s_2}\right)\mathbf{v} + s\frac{t_1 - t_2}{s_1 - s_2}\mathbf{v} = \mathbf{r}_0 + \left(t_1 - s_1\frac{t_1 - t_2}{s_1 - s_2} + s\frac{t_1 - t_2}{s_1 - s_2}\right)\mathbf{v}.$$

Vi har då visat att en godtycklig punkt på $\mathbf{u}$-linjen ligger på $\mathbf{r}$-linjen. Detta avslutar beviset.

Sats. Två linjer $L_1 \neq L_2$ i $\mathbb{C}^2$ som inte är parallella skär varandra i en unik punkt.

Bevis. Detta är bara ett linjärt ekvationssystem med två obekanta och två ekvationer, med koefficienter i $\mathbb{C}$ istället för i $\mathbb{R}$. Men räkningarna är desamma.

Alla kurvor som vi studerat tidigare över $\mathbb{R}$ kan också betraktas över $\mathbb{C}$ och de allra flesta exemplen i denna kurs kommer att ha reella koefficienter. Men varje (nollskilt) polynom $p(x, y) \in \mathbb{C}[x, y]$ definierar en kurva i $\mathbb{C}^2$.

Exempel. Ekvationen $x^2 + 2ixy + y^2 + (2 + i)x - y + 1 = 0$ definierar en komplex affin kurva i $\mathbb{C}^2$. Med hjälp av kvadratkomplettering kan vi skriva detta som $(x + iy)^2 + (2 + i)x - y + 1 = 0$, vilket efter variabelbytet $x \mapsto x - iy, y \mapsto y$ blir

$$x^2 + (2 + i)(x - iy) - y = x^2 + (2 + i)x + (1 - 2i)y + 1 = 0.$$

Ytterligare ett linjärt variabelbyte $x \mapsto x, y \mapsto \dfrac{2 + i}{2i - 1}y$ ger ekvationen $x^2 - y = 0$. Vi ser att denna kurva är en (komplex) parabel.

Definition. En punkt på en komplex kurva kallas *singulär*, precis som i det reella fallet, om Taylorutvecklingen av polynomet i denna punkt inte har någon linjär term.

8.2 Generaliserade tangentlinjer.

Proposition. Ett *homogent* polynom $f(x, y) \in \mathbb{C}[x, y]$ har en unik faktorisering i linjära faktorer.

Bevis. Antag att $f(x, y) = c_0y^d + c_1xy^{d-1} + ... + c_dx^d$ är av grad d. Bryt ut y^d och använd algebrans fundamentalsats på den resterande faktorn som är ett komplext polynom i en variabel $\dfrac{x}{y}$ enligt:

$$f(x, y) = y^d\left(c_0 + c_1\frac{x}{y} + ... + c_d\left(\frac{x}{y}\right)^d\right) = y^d(\delta_1\frac{x}{y} - \epsilon_1)\cdot...\cdot(\delta_d\frac{x}{y} - \epsilon_d) = (\delta_1x - \epsilon_1y)\cdot...\cdot(\delta_dx - \epsilon_dy).$$

Definition. Låt $f(x,y)$ vara ett polynom sådan att $f(a,b)=0$ och $\nabla f(a,b)=0$. Låt m vara den minsta ickeförsvinnande graden i Taylorutvecklingen i (a,b) och f_m det homogena polynom (i variablerna $(x-a, y-b)$ förstås) som består av termerna av denna grad. Då är $f_m = l_1 \cdot ... \cdot l_m$. Kurvorna $V(l_j)$ kallas de *generaliserade tangentlinjerna* till $V(f)$ i (a,b).

Exempel. De generaliserade tangentlinjerna till kurvan $f(x,y) = x^4 - 4y^4 + x^3y^5 = 0$ i origo fås genom att faktorisera $f_4(x,y) = x^4 - 4y^4$. Vi får

$$x^4 - 4y^4 = (x^2 - 2y^2)(x^2 + 2y^2) = (x - \sqrt{2}y)(x + \sqrt{2}y)(x - \sqrt{2}iy)(x + \sqrt{2}iy).$$

De fyra komplexa linjerna $x - \sqrt{2}y = 0$, $x + \sqrt{2}y = 0$, $x - \sqrt{2}iy = 0$, $x + \sqrt{2}iy = 0$ är alltså de generaliserade tangentlinjerna.

8.3 Komplexa affina transformationer.

Definitionen av linjär avbildning mellan komplexa vektorrum är ordagrant densamma som i reella fallet och sådana ges av matriser med komplexa koefficienter. Det är fortfarande fallet att en linjär avbildning A är inverterbar om och endast om $\det(A) \neq 0$. Mängden av inverterbara komplexa linjära avbildningar betecknas $GL(n,\mathbb{C})$. Affina transformationer definieras på samma sätt också. Mängden av affina transformationer på $\mathbb{C}^2$, $\mathrm{Aff}_{\mathbb{C}}(2)$, är en grupp och den verkar från höger på $\mathbb{C}[x,y]$ på samma sätt som motsvarande grupp i det reella fallet. Vi definierar ekvivalens mellan komplexa polynom på samma sätt också. Vi kan på samma sätt som tidigare klassificera komplexa polynom av en given grad upp till affina transformationer och multipler av komplexa tal. Notera att alla reella affina transformationer också är komplexa transformationer.

Sats. Upp till affina transformationer finns bara en komplex linje i $\mathbb{C}^2$.

Bevis. Övning.

8.4 Komplexa kvadratiska former.

Sats. Varje komplex kvadratisk form på $\mathbb{C}^n$ är ekvivalent med en kvadratisk form av typen

$$Q(x_1, ..., x_n) = x_1^2 + ... + x_k^2.$$

Bevisskiss. Vad som behöver visas är att varje symmetrisk matris A med komplexa koefficienter är ekvivalent med en diagonal matris $D = T^tAT$ med bara 1:or och 0:or på diagonalen. Vi använder en sats som säger att varje inverterbar matris T kan skrivas som en produkt av elementära matriser. Det är lätt att övertyga sig om att en elementär matris E som vid multiplikation från höger utför en viss kolumnoperation har egenskapen att E^t utför motsvarande radoperation vid multiplikation från vänster. Alltså är frågan om vi kan diagonalisera varje A genom att successivt utföra par av rad och kolumnoperationer. Låt oss kalla ett sådant par en rad-kolumnoperation (RKO). Om $A = 0$ är vi klara. Vi kan alltid skaffa ett nollskilt element på diagonalen genom att utföra en RKO. Om $a_{ij} \neq 0$ kan vi nämligen utföra RKO:en som adderar rad i till j och kolumn i till j. Det gör $a_{jj} \neq 0$. Efter ett rad-kolumnbyte kan vi anta

att $j = 1$. Med hjälp av *RKO*:er kan vi nu rensa rad/kolumn 1 från nollskilda element och fortsätta med induktion på den resulterande $(n-1) \times (n-1)$-undermatrisen. Till sist kan vi förvandla varje nollskilt diagonalelement till en etta genom att multiplicera från båda håll med $\text{diag}((\sqrt{a_{11}})^{-1}, ..., (\sqrt{a_{kk}})^{-1}, 0, ..., 0)$ eftersom vi arbetar över $\mathbb{C}$ och kan hitta kvadratrötter. Här är k antalet nollskilda element på diagonalen.

Anmärkning. Med andra ord är varje kvadratisk form ekvivalent med en som ges av en matris med bara 1:or och 0:or på diagonalen. Det enklaste sättet att finna denna form är normalt att göra en kvadratkomplettering.

8.5 Klassificering av komplexa andragradspolynom upp till affin ekvivalens.

Komplexa andragradskurvor kan också klassificeras upp till affina transformationer med samma metod vi använde i reella fallet. Vi börjar med att diagonalisera den kvadratiska formen med hjälp av satsen ovan och sedan gör vi samma saker som i det reella beviset, förutom att vi kan ignorera fallet då $\lambda = -1$. Klassificeringen förenklas substantiellt i jämförelse med det reella fallet. Resultatet blir som följer.

Sats. Varje polynom av grad 2 över $\mathbb{C}$ är ekvivalent med exakt ett av följande. Nollställesmängden beskrivs i ord i parentes.

(a) $x^2 + y^2 - 1$ (Cirkeln)

(b) $x^2 - y$ (Parabeln.)

(c) $x^2 + y^2$ (Linjekorset.)

(d) $x(x-1)$ (Två parallella linjer.)

(e) x^2 ('Dubbellinjen')

Diskussion. Beviset är redan skisserat ovan, men för att det ska bli tydligare vad som händer, går vi här igenom hur den reella klassificeringen förändras när vi tillåter oss komplexa transformationer. Cirkeln och hyperbeln är komplext ekvivalenta genom den affina transformationen $T(x, y) = (x, iy)$. Detsamma gäller punkten och linjekorset. Observera att x^2+y^2 som över $\mathbb{R}$ såg ut att ha nollställe en punkt, har många komplexa nollställen. Eftersom $x^2+y^2 = (x+iy)(x-iy)$ så består nollställesmängden av två linjer som skär varandra i origo! De tre resterande fallen svarar mot en degenererad kvadratisk form. och skiljer sig åt eftersom även komplexa affina transformationer tar varje linje till en linje. Linjekorset är singulärt och affina transformationer över $\mathbb{C}$ bevarar singulariteter, så det är annorlunda än cirkeln. Notera till sist att polynomen som till synes hade tomma mängden som nollställesmängd inte längre har det. Det första exemplet är ekvationen $x^2 + y^2 + 1$ är via det komplexa affina variabelbytet $T(x, y) = (ix, iy)$ ekvivalent med $-x^2 - y^2 + 1$. Till sist är $x^2 + 1$ ekvivalent med $x^2 - 1 = (x + 1)(x - 1)$ med samma variabelbyte och faller därför i kategori (d). Detta avslutar diskussionen.

8.6 Två satser till om komplexa kurvor.

Vi har sett att över $\mathbb{R}$ kan nollställesmängden $f(x,y)=0$ bestå av enstaka punkter, eller rentav vara tom, så att till synes radikalt olika polynom ha samma nollställen. Vi har också sett att situationen i fallet med andragradskurvor är betydligt mindre patologisk över $\mathbb{C}$. Här är ett par allmänna satser som visar att detta är ett generellt fenomen för kurvor över $\mathbb{C}$.

Sats. Låt $f(x,y) \in \mathbb{C}[x,y]$ vara ett icke-konstant polynom. Då har $f(x,y)=0$ oändligt (överuppräkneligt) många lösningar i $\mathbb{C}^2$.

Bevis. Betrakta, för varje fixt $c \in \mathbb{C}$, envariabelpolynomet $f(x,c)$. Om det är icke-konstant eller 0 har det nollställen. Antag att det är konstant $= d$, så att $f(x,c)-d=0$ för alla x. Men det betyder precis att c en rot till varje koefficient till $f(x,y)-d$ (betraktat som ett polynom i y med koefficienter i $\mathbb{C}[x]$). Det finns maximalt ändligt många sådana rötter. Detta bevisar satsen.

Exempel. Argumentet i beviset blir kanske tydligare med ett exempel. Betrakta polynomet

$$f(x,y) = x^2y^2 + xy^2 + 2ixy + 4x^2 + 1$$

t.ex. Fixerar vi $y=c$ får vi

$$f(x,c) = x^2c^2 + xc^2 + 2ixc + 4x^2 + 1 = (c^2+4)x^2 + (c^2+2ic)x + 1.$$

Om detta ska vara konstant måste vi ha $c^2+4 = c^2+2ic = 0$, vilket är två polynomekvationer i en variabel vilka har som mest ändligt många lösningar (här $c=-2i$). Alltså är detta polynom med ändligt många (ett) c som undantag icke-konstant, och har alltså två lösningar (x_1,c) och (x_2,c) (med multiplicitet).

Nästa sats kommer vi inte att bevisa heller. Den är ett specialfall av en mer avancerad sats som gäller för allmänna algebraiska mängder (vi formulerar den i ett senare kapitel). I fallet med kurvor är formuleringen betydligt enklare. Vi ser det viktiga faktum att vi över $\mathbb{C}$ inte behöver göra någon större åtskillnad mellan ett polynom och dess nollställesmängd. De bestämmer mer eller mindre varandra. Den enda skillnaden är eventuella multipla faktorer.

Sats. (Hilberts Nullstellensatz för kurvor.) Om $f(x,y)$ och $g(x,y)$ är polynom med komplexa koefficienter, med nollställesmängder $V(f)$ respektive $V(g)$ i $\mathbb{C}^2$, så gäller: $V(f)=V(g)$ om och endast om f och g har samma irreducibla faktorer (men som kan förekomma med olika multiplicitet).

Bevis. Se till exempel Atiyah/MacDonald, *Introduction to commutative algebra.*

8.7 Komplex analys.

I det här avsnittet fördjupar vi oss lite i vad den geometriska och analytiska meningen hos algebraiska kurvor över $\mathbb{C}$ är. Vi börjar med lite komplex analys i en variabel z.

8.7.1 Komplex derivata.

$\mathbb{C}$ är detsamma som $\mathbb{R}^2$ som reellt vektorrum betraktat. Avståndsbegreppet och därför gränsvärdesbegreppet är också detsamma: $|z - z_0|^2 = (x - x_0)^2 + (y - y_0)^2$.

Definition Låt $f : U \subset \mathbb{C} \to \mathbb{C}$ vara en funktion definierad på en öppen delmängd av $\mathbb{C}$. Funktionen f kallas *komplext deriverbar* i $z_0 \in U$ om gränsvärdet

$$\lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0}$$

existerar. Det kallas då den komplexa derivatan i z_0, $f'(z_0)$.

Detta villkor visar sig vara *mycket starkare* än reell deriverbarhet av motsvarande funktion $f : U \subset \mathbb{R}^2 \to \mathbb{R}^2$, $f(z) = f(x + iy) = u(x, y) + iv(x, y) = (u(x, y), v(x, y))$

Sats. Om f är komplext deriverbar uppfyller $u(x, y)$ och $v(x, y)$ Cauchy-Riemanns ekvationer $u_x = v_y$ och $u_y = -v_y$, d v s Jacobimatrisen har den speciella formen

$$\begin{bmatrix} u_x & u_y \\ v_x & v_y \end{bmatrix} = \begin{bmatrix} u_x & u_y \\ -u_y & u_x \end{bmatrix}$$

Bevis. Om $f'(z_0)$ existerar måste speciellt gränsvärdet existera längs x- och y-riktningarna separat:

$$f'(z_0) = \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0} = \lim_{x \to x_0} \frac{u(x, y_0) + iv(x, y_0) - (u(x_0, y_0) + iv(x_0, y_0)}{(x - x_0) + i(y - y_0)}$$

$$= \lim_{x \to x_0} \frac{u(x, y_0) - u(x_0, y_0)}{x - x_0} + i \lim_{x \to x_0} \frac{v(x, y_0) - v(x_0, y_0)}{x - x_0} = u_x + iv_x$$

och på samma sätt får vi i y-riktningen

$$f'(z_0) = \frac{1}{i}(u_y + iv_y) = v_y - iu_y.$$

Jämför vi de två uttrycken för $f'(z_0)$ får vi påståendet i satsen.

Notera att en matris av formen i satsen kan skrivas

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \sqrt{a^2 + b^2} \begin{bmatrix} \frac{a}{\sqrt{a^2 + b^2}} & \frac{b}{\sqrt{a^2 + b^2}} \\ \frac{-b}{\sqrt{a^2 + b^2}} & \frac{a}{\sqrt{a^2 + b^2}} \end{bmatrix}.$$

Med andra ord är den en sammansättning av en rotation och en skalning. Detta är inte så konstigt: Matrisen är bara ett reellt sätt att beskriva multiplikation med det *komplexa talet* $f'(z_0)$! Hur som helst, detta *geometriska krav* på derivatan medför att komplext deriverbara funktioner har väldigt speciella egenskaper.

Exempel. De enda funktioner av komplexa variabler vi ska studera i denna kurs är polynom. Derivatan av ett polynom $f(z) = z^m$ fungerar algebraiskt precis som vanligt: $f'(z) = mz^{m-1}$. Låt t.ex. $m = 2$:

$$\lim_{h\to 0} \frac{f(z+h) - f(z)}{h} = \lim_{h\to 0} \frac{(z+h)^2 - z^2}{h} = \lim_{h\to 0} \frac{z^2 + h^2 + 2hz - z^2}{h} = 2z.$$

Partiella derivator definieras på det uppenbara sättet.

Definition. Om $f = f(z, w)$ är en komplex funktion av två komplexa variabler så definieras

$$f_z = \frac{\partial f}{\partial z} = \lim_{h\to 0} \frac{f(z+h, w) - f(z, w)}{h}.$$

Förstås definieras f_w analogt.

Funktioner i den här kursen är som bekant oftast polynom av två komplexa variabler $f(z, w)$. Notera att vi kan tänka på ett sådant som en funktion $f : \mathbb{C}^2 \to \mathbb{C}$, men också som en funktion $f : \mathbb{R}^4 \to \mathbb{R}^2$. Vi skriver då variablerna som

$$\mathbb{C}^2 \ni (z, w) = (x_1 + iy_1, x_2 + iy_2) = (x_1, y_1, x_2, y_2) \in \mathbb{R}^4$$

och funktionsvärdena som

$$\mathbb{C} \ni f(z, w) = u(x_1, y_1, x_2, y_2) + iv(x_1, y_1, x_2, y_2) = (u(x_1, y_1, x_2, y_2), v(x_1, y_1, x_2, y_2)) \in \mathbb{R}^2.$$

Då blir den reella derivatan (Jacobimatrisen)

$$\frac{\partial(u, v)}{\partial(x_1, y_1, x_2, y_2)} = \begin{bmatrix} u_{x_1} & u_{y_1} & u_{x_2} & u_{y_2} \\ v_{x_1} & v_{y_1} & v_{x_2} & v_{y_2} \end{bmatrix} = \begin{bmatrix} u_{x_1} & u_{y_1} & u_{x_2} & u_{y_2} \\ -u_{y_1} & u_{x_1} & -u_{y_2} & u_{x_2} \end{bmatrix}$$

Notera att vi kan gå tillbaka till komplex notation om vi vill och skriva detta helt enkelt som en komplex gradient, 1×2-matrisen:

$$\begin{bmatrix} \dfrac{\partial f}{\partial z} & \dfrac{\partial f}{\partial w} \end{bmatrix}$$

8.7.2 Algebraiska kurvor som reella ytor.

Sats. (Implicita funktionssatsen för polynom i komplexa kläder.) Låt $f(z, w)$ vara ett polynom som ovan. Om $\dfrac{\partial f}{\partial z} \neq 0$ eller $\dfrac{\partial f}{\partial w} \neq 0$ i en punkt (z_0, w_0) så är den komplexa kurvan $f(z, w) = 0$ lokalt runt (z_0, w_0) en graf av en oändligt deriverbar funktion av två reella variabler.
Bevis. Vi har

$$\frac{\partial f}{\partial z} = \frac{\partial u}{\partial x_1} + i\frac{\partial v}{\partial x_1} = \frac{\partial u}{\partial x_1} - i\frac{\partial u}{\partial y_1}$$

så

$$\frac{\partial f}{\partial z} = 0 \iff \frac{\partial u}{\partial x_1} = 0 = \frac{\partial u}{\partial y_1} = 0.$$

Därför, om $\frac{\partial f}{\partial z} \neq 0$, så är den vänstraste underdeterminanten i matrisen

$$\frac{\partial(u,v)}{\partial(x_1,y_1,x_2,y_2)} = \begin{bmatrix} u_{x_1} & u_{y_1} & u_{x_2} & u_{y_2} \\ -u_{y_1} & u_{x_1} & -u_{y_2} & u_{x_2} \end{bmatrix}$$

nollskild. Enligt den vanliga implicita funktionssatsen och det faktum att polynom är oändligt deriverbara följer satsen i detta fall. Fallet $\frac{\partial f}{\partial w} \neq 0$ ger samma resultat med hjälp av den högraste underdeterminanten.

Anmärkning. Denna sats innebär att i närheten av varje punkt som inte är *singulär* är en algebraisk kurva en glatt reellt tvådimensionell yta.

9 Skärningsmultiplicitet

I detta kapitel kommer vi att ställa upp sex stycken axiom för skärningsmultipliciteten och motivera vart och ett av dessa intuitivt. Vi kommer sedan att härleda en mängd konsekvenser från axiomen. Konstruktionen av skärningsmultipliciteten måste anstå till slutet av kursen, då den kräver en del abstrakt algebraisk teori som vi inte vill haka upp oss vid just nu. Nu till saken.

9.1 Axiomen

Vi kommer att definiera ett tal $I_P(f,g) \in \mathbb{N} \cup \{\infty\}$ för varje par av polynom (f,g) och varje punkt P, som ska kallas skärningsmultipliciteten mellan f och g i punkten P.

Axiom 0. Om F är en affin transformation bör $I_{F^{-1}(P)}(f \circ F, g \circ F) = I_P(f,g)$.

Motivering. Vi vet sedan tidigare åtminstone att affina transformationer bevarar transversalitet, vilket bör betraktas som den enklaste sortens skärning. Här lyfter vi detta till ett axiom.

Axiom 1. $I_P(f,g) = I_P(g,f)$

Motivering. Det är väl ett rimligt krav att f skär g på samma sätt som g skär f.

Axiom 2. $I_P(f,g) \neq 0$ om och endast om $f(P) = g(P) = 0$.

Motivering. Detta betyder att om kurvorna skär varandra i P är skärningsmultipliciteten nollskild, och om de inte skär varandra i P är den noll. Även detta verkar som ett rimligt axiom.

Axiom 3. $I_0(x,y) = 1$.

Motivering. De två axlarna skär varandra på enklaste möjliga sätt i origo, vilket borde betecknas med multiplicitet 1. T.ex. vore det ju trevligt om vi kunde återfå nollställens multiplicitet hos envariabelpolynom som skärningsmultipliciteter mellan grafen till polynomet och x-axeln. (Se nedan.)

Axiom 4. $I_P(f, gh) = I_P(f, g) + I_P(f, h)$.

Motivering. Kom ihåg att $V(gh) = V(g) \cup V(h)$, vilket tillsammans med bilden ??? borde vara tillräcklig motivering.

Axiom 5. $I_P(f, g + fh) = I_P(f, g)$, dvs. multipliciteten skall inte ändras om en multipel av det ena polynomet läggs till det andra. Här är h vilket polynom som helst.

Motivering. Vi ger två motiveringar. Att $V(f)$ och $V(g)$ skär varandra i P är ekvivalent med $f(P) = 0$ och $g(P) = 0$. Detta är i sin tur ekvivalent med att $f(P)= 0$ och $g(P)+f(P)h(P) = 0$ för alla h vilket är detsamma som att $V(f)$ och $V(g + fh)$ skär varandra i P'. Det vill säga, med axiom 2, att $I_P(f, g + fh) = 0 \iff I_P(f, g) = 0$.

Vi kan också se att om $V(f)$ och $V(g)$ skär varandra *transversellt* i P, så gör $V(f)$ och $V(g+fh)$ detsamma. Notera nämligen att, eftersom $f(P) = 0$,

$$\nabla(g + fh)(P) = \nabla g(P) + f(P)\nabla h(P) + h(P)\nabla f(P) = \nabla g(P) + h(P)\nabla f(P).$$

Från detta ser vi genast att $\nabla f(P)$ och $\nabla g(P)$ är parallella om och endast om $\nabla f(P)$ och $\nabla(g + fh)(P)$ är parallella.

Anmärkning. I smyg har vi här gjort en förskjutning från geometri till algebra. I_P är en funktion av f och g, inte av motsvarande nollställesmängder $V(f)$ och $V(g)$, vilket gör att $I_P(f, g)$ kommer att plocka upp sådant som multipliciteten hos en irreducibel faktor. T.ex. kommer "dubbellinjen" $x^2 = 0$ att skära x-axeln två gånger, inte en! (Detta framgår av första exemplet i nästa avsnitt.)

9.2 Preliminära konsekvenser av axiomen.

Exempel. Om $f(x, y) = y$ och $g(x, y) = y - x^2$ får vi

$$I_0(y, y - x^2) = I_0(y, -x^2) = I_0(y, -1) + I_0(y, x) + I_0(y, x) = 2I_0(x, y) = 2.$$

Här har vi använt i tur och ordning, axiomen (5), (4), (1) och (3). Resultatet är det förväntade: Grafen $y = x^2$ skär x-axeln 2 ggr i 0! Notera att $I_0(y, x^2) = 2$ också följer från dessa räkningar - dvs. dubbellinjen $x^2 = 0$ skär $y = 0$ "två gånger".

Proposition.

(a) Om $f|g$ och $f(P) = 0$ är $I_P(f, g) = \infty$.

(b) Om $h|f$ och $h|g$ och $h(P) = 0$ så är $I_P(f, g) = \infty$.

(c) Om $g(P) \neq 0$ så $I_P(f, gh) = I_P(f, h)$.

Bevis.

(a) Skriv $f = gk$. Då har vi

$$I_P(f, g) = I_P(gk, g) = I_P(g, k) + I_P(g, g) \geq I_P(g, g),$$

från Axiom 4,5. Vidare är, med Axiom 5, för alla $n \in \mathbb{N}$:

$$I_P(g, g) = I_P(g, 0) = I_P(g, 0^n) = nI_P(g, 0) \geq n,$$

vilket avslutar beviset.

(b) Övning.

(c) $I_P(f, gh) = I_P(f, g) + I_P(f, h) = I_P(f, h)$, enligt Axiom 4 och 2.

Anmärkning. Meningen med (a) och (b) är att om kurvorna har en gemensam komponent så är skärningstalet oändligt i varje punkt på denna.

Följande visar att skärningsmultipliciteten generaliserar multipliciteten hos ett nollställe från tidigare algebrakurser, genom skärningen mellan grafen och x-axeln $y = 0$.

Sats. Om a är ett nollställe av multiplicitet k till polynomet $p(x)$ så är $I_{(a,0)}(y - p(x), y) = k$.

Bevis. $I_{(a,0)}(y - p(x), y) = I_{(a,0)}(p(x), y) = I_{(a,0)}((x - a)^k q(x), y) = I_{(a,0)}((x - a)^k, y) = I_{(0,0)}(x^k, y) = k$.

Nästa sats visar hur vi kan beräkna skärningstalet då en av kurvorna är en funktionsgraf.

Sats. Låt $f(x, y) = y - p(x)$ och låt $g(x, y)$ vara ett polynom. Antag att $p(0) = 0 = g(0, 0)$ (så att båda kurvorna går genom origo) och att f inte delar g. Låt vidare k vara multipliciteten av $x = 0$ som nollställe till $g(x, p(x))$. Då är $I_{(0,0)}(f, g) = k$.

Bevis. Enligt satsen i slutet av avsnitt 2.2 ovan kan vi skriva

$$g(x, y) = q(x, y)(y - p(x)) + r(x),$$

där $r(x) = f(x, p(x))$. Vi kan nu beräkna skärningstalet som

$$I_0(f, g) = I_0(y - p(x), q(x, y)(y - p(x)) + r(x)) = I_0(y - p(x), r(x)) =$$

$$I_0(y - p(x), f(x, p(x))) = I_0(y - p(x), x^k q(x)) = kI_0(y - p(x), x) = k.$$

Föregående sats kan generaliseras:

Sats. Låt $f(x,y) = y - p(x)$ och låt $g(x,y)$ vara ett polynom. Antag att f inte delar g. Faktorisera

$$g(x,p(x)) = C(x-a_1)^{s_1} \cdot ... \cdot (x-a_\nu)^{s_\nu},$$

där $C \neq 0$. Då är $I_{(a_i,p(a_i))}(f,g) = s_i$ och det finns inga andra skärningspunkter i xy-planet.

Bevis. Beviset är en direkt räkning av den typ vi har genomfört tidigare. Antag att vi vill beräkna skärningstalet i $(a_1, p(a_1))$ t.ex. Vi flyttar punkten $(a_1, p(a_1))$ till $(0,0)$ genom variabelbytet $x \mapsto x + a_1$, $y \mapsto y + p(a_1)$ och får

$$I_{(a_1,p(a_1))}(y-p(x), g(x,y)) = I_{(0,0)}(y+p(a_1)-p(x+a_1), g(x+a_1, y+p(a_1))) = \text{mult}_0(g(x+a_1, p(x+a_1)).$$

Enligt formeln i satsformuleringen är

$$g(x+a_1, p(x+a_1)) = C(x+a_1-a_1)^{s_1}(x+a_1-a_2)^{s_2} \cdot ... \cdot (x+a_1-a_\nu)^{s_\nu} = x^{s_1}h(x),$$

där $h(0) = (a_1-a_2)^{s_2} \cdot ... \cdot (a_1-a_\nu)^{s_\nu} \neq 0$, så $\text{mult}_0 g(x+a_1, p(x+a_1)) = s_1$. Detsamma kan göras med vilken punkt $(a, p(a))$ som helst på $y = p(x)$ med resultatet att om $a = a_i$ blir skärningstalet s_i och om $a \neq a_i$ för alla i så blir skärningstalet 0. Detta avslutar beviset.

Vi kan nu också se att transversell skärning verkligen motsvarar skärningstal 1.

Sats. Om $f(a,b) = 0 = g(a,b)$ och $\nabla f(a,b) \neq 0$ så är $I_{(a,b)}(f,g) = 1$ om och endast om $\nabla g(a,b) \neq (0,0)$ och skärningen i (a,b) är transversell.

Bevis. Med en affin transformation (som inte påverkar skärningstalet enligt Axiom 1) kan vi anta att $(a,b) = (0,0)$ och att tangentlinjen till $f = 0$ är y-axeln. Då kan vi skriva (Taylorutveckling) $f = ax +$ högre ordningens termer, där $a \neq 0$. Vi väljer att skriva om detta ytterligare genom att samla ihop alla rena y-termer enligt $f(x,y) = xp(x,y) + y^2q(y)$. Notera att $p(0,0) \neq 0$, eftersom $a \neq 0$. På liknande sätt gör vi med $g(x,y) = yv(y) + xu(x,y)$ (där vi inte antar något om v och u). Nu kan vi räkna ut $I_0(f,g)$. Vi multiplicerar först g med p. Detta ändrar inte skärningstalet enligt tidigare sats, eftersom $p(0,0) \neq 0$. Sedan använder vi Axiom 5 och subtraherar uf ifrån lucka två. Vi får

$$I_0(f,g) = I_0(xp+y^2q, yv+xu) = I_0(xp+y^2q, yvp+xup) = I_0(xp+y^2q, yvp-y^2qu) =$$

Med Axiom 4 får vi vidare

$$I_0(xp+y^2q, y(vp-yqu)) = I_0(xp+y^2q, vp-yqu) + I_0(xp+y^2q, y) =$$

I den andra termen kan nu y^2q elimineras med hjälp av Axiom 5. Dessutom är $p(0,0) \neq 0$ så den blir

$$I_0(xp+y^2q, y) = I_0(xp, y) = I_0(x,y) = 1.$$

Sammanfattningsvis har vi nu

$$I_0(f,g) = I_0(f, vp - yqu) + 1.$$

Nu behöver vi analysera den återstående termen här. Eftersom $f(0,0) = 0$ är denna term $= 0$ om och endast om den andra luckan också är 0 i $(0,0)$. Men dess värde är $v(0)p(0,0)$ som är 0 om och endast om $v(0) = 0$. Men detta betyder precis att $g(x,y)$ inte innehåller någon term på formen by där $b \neq 0$. Detta är ekvivalent med att $g(x,y)$ antingen är singulär i $(0,0)$ eller har gradient parallell med ∇f där. Detta avslutar beviset.

Korollarium. Om F är icke-singulär i P finns exakt en linje T (tangentlinjen) som uppfyller $I_P(T,F) \geq 2$. Övriga linjer uppfyller $I_P(L,F) = 1$.

Övningar:

1. Beräkna skärningsmultipliciteten i origo, $I_0(f,g)$, av följande polynom. (Tagna ur [Bix]).
   (a) $f = y - x^3$ och $g = y^4 + 6x^3y + x^8$.
   (b) $f = y - x^2 - x$ och $g = y^2 - 3x^2y - x^2$.
   (c) $f = y^2 + x^2y - x^3$ och $g = y^2 + x^3y + 2x$
   (d) $f = y^5 - x^7$ och $g = y^2 - x^3$.
2. Visa att det finns s linjer genom origo som skär den givna kurvan mer än t gånger där och att alla andra linjer skär kurvan exakt t gånger där. Rita kurvan och de exceptionella linjerna.
   (a) $y = x^3 - 2x$, $s = 1$, $t = 1$.
   (b) $y^2 = x^3$, $s = 1$, $t = 1$.
   (c) $y^2 = x^4 + 4x^2$, $s = 2$, $t = 2$.
   (d) $y^2 = x^4 - 4x^2$, $s = 0$, $t = 2$.
3. Beräkna alla skärningspunkter mellan $y^2 = x^3$ och $y = x^2 - x$ samt skärningstalen i dessa.

10 Reell projektiv geometri

10.1 Historia.

Projektiv geometri upptäcktes av renässanskonstnärer, inte minst Filippo Brunelleschi (1377-1446), vilka utarbetade en vetenskaplig perspektivlära, i syfte att åstadkomma realistiska målningar. De första matematiska arbetena i ämnet gjordes av Girard Desargues (1591-1661). Den ganska abstrakta formulering vi använder i denna kurs lutar sig på linjär algebra och nådde denna form under andra hälften av 1800-talet (kanske?).

10.2 Motiverande diskussion.

Vi är alla bekanta med det faktum att parallella linjer (t.ex. en tågräls) som sträcker sig bort från oss verkar närma sig varandra och t.o.m. mötas i horisonten. Varken affin eller euklidisk geometri tar hänsyn till denna "upplevda" geometriska effekt. Den är ett resultat av den centrala projektion som ligger bakom vår visuella perception (våra ögon sitter på ett ställe (well, nästan)). Vi observerar de ljusstrålar som når detta ställe, inga andra. I Figur Ditten ser vi två parallella linjer i ett xy-koordinatsystem, givna av ekvationerna $x = \pm c$, som vi kan tänka på som en modell för en lång rak tågräls. Om vi istället tänker oss att vi står på koordinatsystemet och tittar på de två rälen, kommer vi att se dem gå ihop i horisonten, som i Figur Datten. I figur Drutten ser vi detta ur ett annat perspektiv. De streckade linjerna är ljusstrålar som når våra ögon från olika punkter på rälsen. Notera att horisonten ligger i vår ögonhöjd: Gränsläget för dessa ljusstrålar.

Notera att saker som ligger på samma räta linje genom vårt öga kommer att se ut att vara på samma plats i synfältet (i verkligheten förstås skymma varandra). Projektiva geometrin bygger på dessa iakttagelser.

10.3 Det reella projektiva planet.

Betrakta följande relation på $\mathbb{R}^3 \setminus \{\mathbf{0}\}$.

$$\mathbf{u} \sim \mathbf{v} \iff \exists \lambda \in \mathbb{R} : \lambda \mathbf{u} = \mathbf{v}$$

.

Sats. Denna relation är en ekvivalensrelation.

Bevis. Lämnas som övning.

Definition. Det projektiva planet $\mathbb{R}P^2$ är mängden av ekvivalensklasser av ovanstående ekvivalensrelation.

Anmärkning. En ekvivalensklass består av alla vektorer som spänner upp samma linje och kan alltså identifieras med denna linje. Vi kan alltså tänka på $\mathbb{R}P^2$ som mängden av linjer genom origo i $\mathbb{R}^3$.

Definition. En ekvivalensklass kallas en *projektiv punkt* eller helt enkelt en *punkt i det projektiva planet* $\mathbb{R}P^2$. Vi betecknar punkter i projektiva planet med s.k. *homogena koordinater*, vilket helt enkelt är komponenterna (x, y, z) av någon vektor i ekvivalensklassen ifråga.

Anmärkning. I annan litteratur förekommer andra mer komplicerade beteckningssätt, t.ex. $[x : y : z]$. Vi ansluter oss dock till samma princip som vi använder när vi betecknar rationella tal som bråk och underförstår att olika bråk ibland representerar samma ekvivalensklass. På samma sätt som vi skriver $2/3 = 4/6$ kommer vi att skriva $(2, 3, 4) = (4, 6, 8)$ när dessa tripler

står för samma projektiva punkt. Förhoppningsvis uppstår inte oklarheter av denna anledning. När det passar oss skriver vi dessa koordinater som kolonnvektorer också.

Det projektiva planet är ett tvådimensionellt objekt i bemärkelsen att varje punkt har en omgivning som kan parametriseras med reella talpar i $\mathbb{R}^2$. För att täcka hela $\mathbb{R}P^2$ med sådana omgivningar behöver vi tre stycken. Dessa omgivningar gör det möjligt att undersöka $\mathbb{R}P^2$ bit för bit, som i en kartbok. Det är meningen med följande definition.

Definition. Vi definierar *den affina xy-kartan* (kort: xy-kartan) på $\mathbb{R}P^2$ som mängden av alla projektiva punkter vars homogena z-koordinat är nollskild. På motsvarande sätt definieras de affina yz- och $xz-$kartorna.

Anmärkning. Observera att varje projektiv punkt som har nollskild z-koordinat har en unik representant av formen $(x, y, 1)$. Därför kan den affina xy-kartan naturligt identifieras med xy-planet i $\mathbb{R}^3$ och därför med $\mathbb{R}^2$ via avbildningen $(x, y) \to (x, y, 1)$.

De punkter som inte ryms i xy-kartan får också sitt eget namn i nästa definition.

Definition. *Linjen i oändligheten sedd från den affina xy-standardkartan* är komplementet av den i $\mathbb{R}P^2$, dvs mängden av alla projektiva punkter (x, y, z) som har $z = 0$. På motsvarande sätt definieras *linjen i oändligheten* för de andra kartorna.

Anmärkning. (För dem som har läst topologi.) $\mathbb{R}P^2$ är en tvådimensionell glatt kompakt Hausdorffmångfald. Beviset är rättframt, men utelämnas. Det får vara en övning för dem som har sett sådana saker förr.

10.4 Homogena polynom och projektiva plana algebraiska kurvor

Definition. Ett polynom $F(x, y, z)$ av grad d kallas *homogent* om alla dess termer har total grad d. Ekvivalent, $F(tx, ty, tz) = t^d F(x, y, z)$ för alla $t \in \mathbb{R}$.

En polynomekvation $F(x, y, z) = 0$ definierar typiskt sett en yta i $\mathbb{R}^3$. Om $F(x, y, z)$ är ett homogent polynom är ytan en 'generaliserad dubbelkon', eftersom den innehåller den räta linjen $(tx, ty, tz), t \in \mathbb{R}$ så fort den innehåller (x, y, z). Nämligen, om $F(x, y, z) = 0$ är också $F(tx, ty, tz) = t^d F(x, y, z) = 0$.

Exempel. Ytan som ges av $x + y - z = 0$ är en yta av detta slag. Detsamma gäller förstås alla plan genom origo.

Exempel. Ytan som ges av $x^2 + y^2 - z^2 = 0$ är en vanlig cirkulär kon.

Exempel. Ytan som ges av $yz - x^2 = 0$ är en elliptisk kon. Försök att rita den.

Eftersom ett homogent polynom $F(x, y, z)$ är noll i (x, y, z) om och endast om det är noll på

hela den linje som spänns upp av (x, y, z) är det meningsfullt att tala om dess nollställesmängd $V(F)$ i $\mathbb{R}P^2$.

Definition. Låt $F(x, y, z)$ vara ett homogent polynom i $\mathbb{R}[x, y, z]$. Mängden $V(F) \subset \mathbb{R}P^2$ av projektiva punkter sådana att $F(x, y, z) = 0$ kallas för en *plan projektiv algebraisk kurva*. (Kort: *projektiv kurva* i denna kurs, där vi endast studerar plana kurvor).

Anmärkning. Man bör notera för framtida bruk att ett homogent polynom $F(x, y, z)$ inte definierar en funktion på $\mathbb{R}P^2$ om inte F är konstant. (Övning att reflektera över.)

Snittet mellan $V(F)$ och standardkartorna utgör affina kurvor i dessa. Varje projektiv kurva har alltså flera affina representationer.

Definition. En *projektiv linje* är alla lösningar $(x, y, z) \in \mathbb{R}P^2$ till en linjär ekvation:

$$ax + by + cz = 0.$$

Exempel 1. Ekvationen

$$x + 2y + 3z = 0$$

beskriver en projektiv linje. I de affina xy-kartan ser den ut som (sätt $z = 1$) den affina linjen

$$x + 2y + 3 = 0.$$

Exakt en punkt på den projektiva linjen hamnar utanför kartan, dvs. i linjen i oändligheten. Om $z = 0$ får vi nämligen $x + 2y = 0$ som har den (unika) projektiva lösningen $(2, 1, 0)$.

Exempel 2. $yz = x^2 + z^2$ är en homogen ekvation av grad 2 som definierar en projektiv kurva. I de affina standardkartorna ser den ut i tur och ordning som en parabel i xy-kartan: $y = x^2 + 1$, en cirkel i xz-kartan: $z = x^2 + z^2$, och en hyperbel i yz-kartan: $z(y - z) = 1$.

Definition. Givet ett polynom $f(x, y)$ av grad d i $\mathbb{R}^2$ definierar vi dess *homogenisering* som det homogena polynomet

$$F(x, y, z) = z^d f\left(\frac{x}{z}, \frac{y}{z}\right).$$

Anmärkning. Vi noterar att $F(x, y, z)$ kan fås från $f(x, y)$ genom att varje term i $f(x, y)$ multipliceras med en potens av z på så sätt att den får grad d. Eftersom F är homogent finns det två sätt att tänka på $V(F)$: Antingen som en yta i $\mathbb{R}^3$ eller som en projektiv kurva i $\mathbb{R}P^2$. Ytan $V(F)$ skär planet $z = 1$ i (en kopia av) kurvan $f(x, y) = 0$ vilket är detsamma som bilden av den projektiva kurvan i den affina xy-kartan. Omvänt, unionen av alla linjer genom origo som går genom punkter på kurvan $f(x, y) = 0, z = 1$ är en delmängd av $V(F)$ vars komplement i $V(F)$ ges av de linjer längs vilka $z = 0$.

Sats.

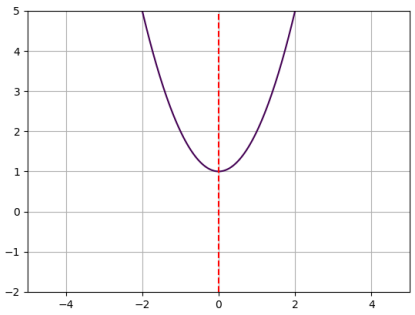


Figure 8: Den projektiva andragrad-skurvan $yz = x^2 + z^2$ i xy-kartan. Den streckade linjen indikerar punkten i ∞.

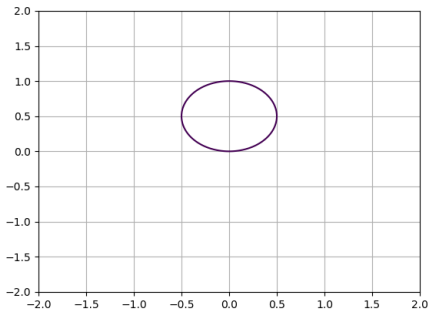


Figure 9: Samma kurva betraktad i xz-kartan. Här syns alla kurvans (reella) punkter.

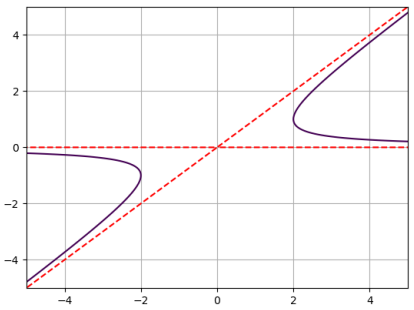


Figure 10: Och i yz-kartan. De streckade linjerna indikerar punkterna i ∞, även om dessa inte syns i kartan.

(a) Givet två skilda projektiva punkter finns en unik projektiv linje som går igenom dem.

(b) Givet två skilda projektiva linjer finns en unik projektiv punkt som ligger på båda.

Bevis.

(a) Detta är en direkt omformulering av att två linjer genom origo bestämmer ett unikt plan i $\mathbb{R}^3$.

(b) Detta är en direkt omformulering av att två plan genom origo skär varandra i en unik linje i $\mathbb{R}^3$.

Definition. Om $F(x, y, z)$ är ett homogent polynom och $F(a, b, c) = 0$ och $\nabla F(a, b, c) \neq 0$ så kallas

$$\frac{\partial F}{\partial x}(a, b, c)x + \frac{\partial F}{\partial y}(a, b, c)y + \frac{\partial F}{\partial z}(a, b, c)z = 0$$

för *tangentlinjen till* F i P.

Anmärkning. Om $f(x, y)$ är en affin kurva är tangentlinjen i punkten (a, b)

$$\frac{\partial f}{\partial x}(a, b)(x - a) + \frac{\partial f}{\partial y}(a, b)(y - b) = 0.$$

Vi kan homogenisera denna ekvation. Vi får då

$$\frac{\partial f}{\partial x}(a, b)(x - az) + \frac{\partial f}{\partial y}(a, b)(y - bz) = 0. \iff$$

$$\frac{\partial f}{\partial x}(a, b)x + \frac{\partial f}{\partial y}(a, b)y - \left(a\frac{\partial f}{\partial x}(a, b) + b\frac{\partial f}{\partial y}(a, b)\right) z.$$

Å andra sidan, homogeniseringen av f är $F(x, y, z) = z^d f(\frac{x}{z}, \frac{y}{z})$ så

$$\frac{\partial F}{\partial x}(x, y, z) = z^{d-1}\frac{\partial f}{\partial x}(\frac{x}{z}, \frac{y}{z}),$$

$$\frac{\partial F}{\partial y}(x, y, z) = z^{d-1}\frac{\partial f}{\partial y}(\frac{x}{z}, \frac{y}{z}),$$

$$\frac{\partial F}{\partial z}(x, y, z) = dz^{d-1}f(\frac{x}{z}, \frac{y}{z}) - z^{d-2}(x\frac{\partial f}{\partial x}(\frac{x}{z}, \frac{y}{z}) + y\frac{\partial f}{\partial y}(\frac{x}{z}, \frac{y}{z})).$$

Om vi sätter in punkten $(x, y, z) = (a, b, 1)$ här får vi

$$\frac{\partial F}{\partial x}(a, b, 1) = \frac{\partial f}{\partial x}(a, b),$$

$$\frac{\partial F}{\partial y}(a, b, 1) = \frac{\partial f}{\partial y}(a, b),$$

$$\frac{\partial F}{\partial z}(a,b,1) = -\left(a\frac{\partial f}{\partial x}(a,b) + b\frac{\partial f}{\partial y}(a,b)\right).$$

Från dessa ekvationer ser vi att homogeniseringen av tangentlinjen är tangentlinjen till homogeniseringen.

Övningar.

1. Vilka av följande projektiva punkter ligger i xy-kartan? Ange deras affina xy-koordinater. För dem som ligger i ∞ sett från denna karta, beskriv punkterna dels som linjer i planet $z = 0$, dels ge deras affina koordinater i någon annan affin karta.

   (a) (1,2,3)
   (b) (2,0,1)
   (c) (3,4,0)
   (d) (0,2,0)

2. Utgående från att nedanstående är affina koordinater för punkter i xy-kartan, ange deras koordinater i xz-kartan respektive yz-kartan, om detta är möjligt. Ange också deras homogena koordinater.

   (a) $(-2, 4)$
   (b) $(3, 2)$
   (c) $(0, 5)$
   (d) $(0, 0)$

3. Nedan följer ekvationer för projektiva linjer. Beskriv deras ekvationer i xy-kartan resp. yz-kartan om möjligt. Vad betyder det att det inte är möjligt?

   (a) $2x + 3y + z = 0$
   (b) $x + 3y = 0$
   (c) $2z = 0$
   (d) $5x + 2z = 0$

4. Nedan följer ekvationer för linjer i olika affina kartor. Ange linjernas ekvationer i homogena koordinater.

   (a) xy-kartan: $2x + y = 1$
   (b) $x + 3z = 5$
   (c) $z = 0$ i xz-kartan
   (d) $5x + 2y = 14$

5. Nedan följer ekvationer för par av projektiva linjer. Ange homogena koordinater för den punkt där de skär varandra.

(a) $2x + y + z = 0$, $x + y + 3z = 0$

(b) $5x + 2y = 0$, $3x + 2y + z = 0$

(c) $x = 0$, $z = 0$

6. Nedan följer koordinater för par av projektiva punkter. Ange ekvationen för den linje som passerar igenom båda.

   (a) $(1, 2, 3)$ $(0, 2, 3)$

   (b) $(1, 2, 1)$ $(1, 3, 4)$

   (c) Vad går fel i fallet $(1, -2, 3)$, $(3, -6, 9)$?

7. Nedan är några affina plana kurvor givna (i xy-kartan). Ange motsvarande projektiva kurva i homogena koordinater (dvs. med ett homogent trevariabelpolynom). Ange koordinaterna för de punkter som ligger på linjen i oändligheten.

   (a) $x^4 + 3x^2y - 4y^4 + 5y^3 + y^2 - 2y - 6 = 0$.

   (b) $y^2 - 3xy + 5x - 2y - 21 = 0$.

   (c) $y^2 = x^3 + 5x$.

   (d) $y^3 = 4x^2y + 8x + 12$

8. För vart och ett av svaren i den förra uppgiften, ange kurvans ekvation i xz-kartan och i yz-kartan. Ange dessutom koordinaterna för vad som var punkterna i oändligheten i förra uppgiften.

10.5 Den sfäriska modellen av $\mathbb{R}P^2$. Skivmodellen.

Varje linje genom origo i $\mathbb{R}^3$ skär enhetssfären S^2 i exakt två antipodala punkter $\mathbf{x}$ och -$\mathbf{x}$. Därför kan vi också tänka på det projektiva planet som mängden av sådana par på sfären. Eller mer precist som mängden av ekvivalensklasser av punkter på S^2 under ekvivalensrelationen $\mathbf{x} \sim -\mathbf{x}$:

Definition. $\mathbb{R}P^2 = S^2/(\mathbf{x} \sim -\mathbf{x})$.

Med andra ord, vi kan tänka på det projektiva planet som sfären, vi måste bara komma ihåg att motstående punkter är samma punkt och inte olika. Projektiva linjer motsvarar storcirklar på sfären, återigen med motstående punkter identifierade.

Notera vidare att varje linje genom origo skär *öppna övre halvsfären* i exakt en punkt. Detta ger oss ytterligare en modell för projektiva planet. En halvsfär är bara en krökt cirkelskiva, så projektiva planet är en cirkelskiva $\mathbb{D}^2$ där motstående punkter på randen betraktas som samma punkt.

Definition. $\mathbb{R}P^2 = \mathbb{D}^2/(\mathbf{x} \sim -\mathbf{x}$ om $\mathbf{x} \in \partial\mathbb{D}^2$.)

Notera att ett diagonalt band tvärsöver disken är ett möbiusband. Ett enkelt topologiskt klipp-

och klistra-argument kan användas för att visa att det reella projektiva planet är en cirkelskiva med ett Möbiusband klistrat längs randen.

10.6 Projektiva transformationer och fyrpunktssatsen.

Definition. En inverterbar linjär avbildning $F : \mathbb{R}^3 \to \mathbb{R}^3$ inducerar en avbildning $F_P : \mathbb{R}P^2 \to \mathbb{R}P^2$ eftersom F tar linjer genom origo till linjer genom origo. En sådan avbildning F_P kallas en *projektiv transformation* och vi betecknar ofta $F_P = F$ om inga missförstånd riskerar att uppstå.

Exempel 1. Om F ges av matrisen nedan

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

så är $F_P = id$, eftersom

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2x \\ 2y \\ 2z \end{bmatrix} = \begin{bmatrix} x \\ y \\ z \end{bmatrix},$$

i $\mathbb{R}P^2$

Exempel 2. Om F ges av matrisen nedan

$$\begin{bmatrix} a & b & h \\ c & d & k \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} ax + bx + hz \\ cx + dy + kz \\ z \end{bmatrix},$$

så ser vi att i xy-kartan ser den ut som $(x, y, 1) \mapsto (ax + bx + h, cx + dy + k, 1)$, eller med vanlig affin notation $(x, y) \mapsto (ax + by + h, cx + dy + k)$ som beskriver en allmän affin transformation. Från detta exempel ser vi att varje plan affin transformation kan realiseras med en projektiv transformation. Speciellt, om $h = k = 0$ beskriver F en linjär avbildning i planet, och om

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

har vi att göra med en translation med vektorn (h, k).

Exempel 3. Notera att en projektiv transformation

$$\begin{bmatrix} a & b & h \\ c & d & k \\ e & f & g \end{bmatrix}$$

bevarar L_∞ ($z = 0$) precis om $ex + fy = 0$ för alla x, y, så att $e = f = 0$, dvs. transformationen är affin i xy-kartan. Den fixerar L_∞ punktvis precis om den motsvarar en ren translation. Att kontrollera dessa påståenden lämnas till läsaren.

Exempel 4. Om F ges av

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x \\ z \\ y \end{bmatrix},$$

så $F_P(x, y, z) = (x, z, y)$, en spegling i $y = z$, som alltså byter plats på $xy-$ och $xz-$ko inatplanen. Om $z = 1$ ger detta $F_P(x, y, 1) = (x, 1, y) = \left(\frac{x}{y}, \frac{1}{y}, 1\right)$, så i ett xy-system ser avbildningen ser alltså ut som den rationella avbildningen $(x, y) \mapsto \left(\frac{x}{y}, \frac{1}{y}\right)$. Notera att detta är precis den avbildning som byter affina koordinater från (x, y) till (x, z). T.ex. parabeln $y = x^2 + 1$ avbildas till $(1/y) = (x/y)^2 + 1$ vilket är detsamma som cirkeln $y = x^2 + y^2$ och vi har återskapat vårt standardexempel från tidigare.

Sats. Mängden av projektiva transformationer Proj(2) är en *grupp*, eftersom identitetsavbildningen är en projektiv transformation, sammansättningen av två projektiva transformationer är en projektiv transformation, varje projektiv transformation har en projektiv invers och sammansättning är associativ.

Bevis. Omedelbart från definitionen.

Här följer en viktig sats. (Ett antal punkter kallas *kolinjära* om de ligger på samma linje.)

Sats. Givet fyra projektiva punkter $z_1, z_2, z_3, z_4 \in \mathbb{R}P^2$ sådana att inte tre av dem är kolinjära, och givet $w_1, w_2, w_3, w_4 \in \mathbb{R}P^2$ med samma egenskap, finns en unik projektiv transformation $F : \mathbb{R}P^2 \to \mathbb{R}P^2$ sådan att $F(z_i) = w_i$ för alla $i = 1, ..., 4$.

Bevis. Representera de givna punkterna med vektorer i $\mathbb{R}^3$, $Z_1, ..., Z_4$ och $W_1, ...W_4$. Villkoret om kolinjaritet betyder att inte tre av Z_i:na ligger i samma plan, och detsamma för W_i. Speciellt betyder det att Z_4 och W_4 kan skrivas som unika linjärkombinationer

$$Z_4 = \sum_{i=1}^{3} a_i Z_i,$$

$$W_4 = \sum_{i=1}^{3} b_i W_i.$$

Notera vidare att inga av a_i och b_i kan vara 0. Om t.ex. $a_1 = 0$ skulle vi ha $Z_4 = a_2 Z_2 + a_3 Z_3$ så $Z_2, .., Z_4$ skulle ligga i ett plan. Definiera $F : \mathbb{R}^3 \to \mathbb{R}^3$ genom $F(Z_i) = \frac{b_i}{a_i} W_i$, $i = 1, ..., 3$. Då gäller

$$F(Z_4) = \sum_{i=1}^{3} a_i F(Z_i) = \sum_{i=1}^{3} a_i \frac{b_i}{a_i} W_i = \sum_{i=1}^{3} b_i W_i = W_4.$$

Detta visar att det finns en sådan projektiv transformation som efterfrågas. Låt $G : \mathbb{R}^3 \to \mathbb{R}^3$ vara en annan linjär avbildning med samma egenskap. Då uppfyller den $G(Z_i) = \lambda_i W_i$ för några λ_i, $i = 1, ..., 4$ och därför är å ena sidan

$$G(Z_4) = \sum_{i=1}^{3} a_i G(Z_i) = \sum_{i=1}^{3} a_i \lambda_i W_i,$$

och å andra sidan är

$$G(Z_4) = \lambda_4 W_4 = \sum_{i=1}^{3} \lambda_4 b_i W_i.$$

Vi ser att detta medför att $\lambda_i = \lambda_4 b_i / a_i$, i=1,...,3. Så F och G definierar samma projektiva transformation som därför är entydigt bestämd.

Korollarium. Låt P,$Q \in \mathbb{R}P^2$. Då finns en projektiv transformation som tar P till Q. Låt P, P' och Q, Q'. Då finns en projektiv transformation som tar P till Q och P' till Q'. Låt P, P', P'' och Q, Q', Q'' vara icke-kolinjära. Då finns en projektiv transformation som tar P till Q, P' till Q' och P'' till Q''.

Anmärkning. Se övningarna till nästa avsnitt för att lista ut vad som gäller om de tre punkterna P, P', P'' och Q, Q', Q'' ligger på en linje.

Beteckna med $\mathbb{R}^h_d[x, y, z] \subset \mathbb{R}[x, y, z]$ mängden av homogena polynom av grad d i tre variabler. En linjär transformation F inducerar en ringisomorfi $F^* : \mathbb{R}[x, y, z] \to \mathbb{R}[x, y, z]$ via $F^*(f) = f \circ F$, enligt avsnittet om affina transformationer.

Sats. Om $f \in \mathbb{R}^h_d[x, y, z]$ så $F^*(f) \in \mathbb{R}^h_d[x, y, z]$.
Bevis. Eftersom F är linjär och bijektiv bevarar den både grad och homogenitet.

Definition. Två homogena polynom f, g av grad d kallas *projektivt ekvivalenta* om det finns en linjär transformation $F : \mathbb{R}^3 \to \mathbb{R}^3$ så att $F^*(f) = g$.

Övningar.

1. Skriv ned uttrycket för en allmän projektiv transformation i xy-kartan.
2. Hur kan bilden av en kvadrat se ut under en affin transformation av planet?
3. Hur kan bilden av en kvadrat se ut under en projektiv transformation?
4. Ange en projektiv transformation som tar punkten $(1, 1, 1)$ till punkten $(0, 2, 3)$.
5. Ange en projektiv transformation som tar linjen $2x + 3y + z = 0$ till linjen $3x + y + z = 0$.
6. Ange en projektiv transformation som tar punkterna $(1, 1, 0)$, $(1, 0, 1)$, $(0, 1, 1)$ till punkterna $(1, 0, 0)$, $(0, 1, 0)$ resp. $(0, 0, 1)$.

7. Ange en projektiv transformation som gör allt i föregående uppgift och dessutom tar $(0, 0, 1)$ till $(1, 1, 1)$.

10.7 Den reella projektiva linjen och dess transformationer.

Mängden av alla linjer genom origo i $\mathbb{R}^n$ ger med liknande konstruktion som ovan projektiva rum i varje dimension. Här betraktar vi det enklaste exemplet, $\mathbb{R}P^1$. Det är av intresse för oss eftersom varje projektiv linje i $\mathbb{R}P^2$ ser ut som en kopia av $\mathbb{R}P^1$. Dessutom är motsvarande konstruktion över $\mathbb{C}$ central i komplex analys, och vi återkommer till detta i kapitlet om komplexa projektiva rum.

Definition. Den projektiva linjen $\mathbb{R}P^1$ är mängden av alla linjer genom origo i $\mathbb{R}^2$. Med andra ord är det mängden av ekvivalensklasser av nollskilda punkter (x, y) i $\mathbb{R}^2$ under ekvivalensrelationen $(x, y) \sim (tx, ty)$, $t \in \mathbb{R} \setminus \{0\}$.

Definition. Vi betecknar punkter i projektiva linjer med *homogena koordinater*, vilket helt enkelt är komponenterna (x, y) av någon punkt i ekvivalensklassen ifråga. En ekvivalensklass kallas en *projektiv punkt*.

Vi har även här affina kartor, i vilka man kan se de punkter där en viss koordinat är nollskild. T.ex. innehåller den affina x-kartan alla projektiva punkter $(x, 1)$ med nollskild y-koordinat. Dessa kan betecknas med ett unikt reellt tal x och utgör därför en kopia av $\mathbb{R}$. Notera att oändligheten här bara består av en projektiv punkt (linjen $y = 0$) och att $\mathbb{R}P^1$ därför ser ut som en cirkel.

En *projektiv transformation* av $\mathbb{R}P^1$ ges av en inverterbar linjär avbildning på $\mathbb{R}^2$, dvs. en inverterbar matris

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

10.7.1 Den cirkulära modellen för $\mathbb{R}P^1$.

Eftersom varje linje genom origo i $\mathbb{R}^2$ skär enhetscirkeln i precis två antipodala punkter kan den projektiva linjen betraktas som mängden av ekvivalensklasser av par av antipodala punkter på $\mathbb{S}^1$. Eftersom varje linje skär öppna övre halvcirkeln i exakt en punkt kan vi också tänka på den som den övre halvcirkeln med punkterna $(-1, 0)$ och $(1, 0)$ identifierade. Topologiskt sett är detta förstås bara en cirkel.

10.7.2 Dubbelförhållandet.

Vi har redan konstaterat att väldigt lite av "normal" geometri är invariant under projektiva transformationer. Till exempel kan en kvadrat i det reella planet avbildas på vilken som helst fyrhörning (fyrpunktsatsen), så längder och vinklar är inte invarianta. I det här avsnittet ska vi studera en invariant - "dubbelförhållandet" - som innehåller det fragment av längdbegreppet som fortfarande återstår. Vi har sett att förhållanden mellan tre punkter på en linje bevaras under affina transformationer. Till exempel, om A och C är två punkter på en linje, och B är mittpunkten mellan dem, så kommer $F(B)$ att vara mittpunkten mellan $F(A)$ och $F(C)$. Detta är uppenbarligen inte sant under projektiva transformationer. Beteckna med $(\mathbf{v}, \mathbf{w})$ den 2×2-matris som har vektorerna $\mathbf{v}$ och $\mathbf{w}$ som kolonner.

Definition. Låt P_1, P_2, P_3 och P_4 vara projektiva punkter på $\mathbb{R}P^1$ och låt $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ och $\mathbf{e}_4$ vara vektorrepresentanter i $\mathbb{R}^2 \setminus \{0\}$ för dessa punkter. *Dubbelförhållandet* $R(P_1, P_2, P_3, P_4) \in \mathbb{R}$ definieras som

$$R(P_1, P_2, P_3, P_4) = \frac{\det(\mathbf{e}_1, \mathbf{e}_2)\det(\mathbf{e}_3, \mathbf{e}_4)}{\det(\mathbf{e}_1, \mathbf{e}_4)\det(\mathbf{e}_3, \mathbf{e}_2)}.$$

Sats. Dubbelförhållandet är oberoende av valet av representanter.

Bevis. Låt $\mathbf{f}_1 = \lambda_1\mathbf{e}_1, ..., \mathbf{f}_4 = \lambda_4\mathbf{e}_4$ vara en alternativ uppsättning representanter. Eftersom determinanten är en bilinjär funktion av sina kolonner följer resultatet direkt:

$$\frac{\det(\mathbf{f}_1, \mathbf{f}_2)\det(\mathbf{f}_3, \mathbf{f}_4)}{\det(\mathbf{f}_1, \mathbf{f}_4)\det(\mathbf{f}_3, \mathbf{f}_2)} = \frac{\lambda_1\lambda_2\lambda_3\lambda_4}{\lambda_1\lambda_2\lambda_3\lambda_4}\frac{\det(\mathbf{e}_1, \mathbf{e}_2)\det(\mathbf{e}_3, \mathbf{e}_4)}{\det(\mathbf{e}_1, \mathbf{e}_4)\det(\mathbf{e}_3, \mathbf{e}_2)} = R(P_1, P_2, P_3, P_4).$$

Sats. Dubbelförhållandet är invariant under projektiva transformationer.

Bevis. Låt den projektiva transformationen ges av 2×2-matrisen A. Vi får med hjälp av multiplikativiteten hos determinanten:

$$\frac{\det(A\mathbf{e}_1, A\mathbf{e}_2)\det(A\mathbf{e}_3, A\mathbf{e}_4)}{\det(A\mathbf{e}_1, A\mathbf{e}_4)\det(A\mathbf{e}_3, A\mathbf{e}_2)} = \frac{\det(A(\mathbf{e}_1, \mathbf{e}_2))\det A(\mathbf{e}_3, \mathbf{e}_4))}{\det(A(\mathbf{e}_1, \mathbf{e}_4))\det(A(\mathbf{e}_3, \mathbf{e}_2))} =$$

$$\frac{(\det A)^2\det(\mathbf{e}_1, \mathbf{e}_2)\det(\mathbf{e}_3, \mathbf{e}_4)}{(\det A)^2\det(\mathbf{e}_1, \mathbf{e}_4)\det(\mathbf{e}_3, \mathbf{e}_2)} = \frac{\det(\mathbf{e}_1, \mathbf{e}_2)\det(\mathbf{e}_3, \mathbf{e}_4)}{\det(\mathbf{e}_1, \mathbf{e}_4)\det(\mathbf{e}_3, \mathbf{e}_2)},$$

från vilket resultatet följer.

Det är vanligare att se dubbelförhållandet definierat i en affin karta. Där ser det ut som följer. Låt $\mathbf{e}_1 = (a, 1)^t, \mathbf{e}_2 = (b, 1)^t, \mathbf{e}_3 = (c, 1)^t$ och $\mathbf{e}_4 = (d, 1)^t$. Då blir

$$R(P_1, P_2, P_3, P_4) = \frac{\det(\mathbf{e}_1, \mathbf{e}_2)\det(\mathbf{e}_3, \mathbf{e}_4)}{\det(\mathbf{e}_1, \mathbf{e}_4)\det(\mathbf{e}_3, \mathbf{e}_2)} = \frac{(a-b)(c-d)}{(a-d)(c-b)},$$

Man betecknar då förstås normalt detta som $R(a, b, c, d)$.

Övningar.

1. Visa att en allmän projektiv transformation av den projektiva linjen som ovan ges, i x-kartan, av (en så kallad Möbiustransformation)
$$x \mapsto \frac{ax + b}{cx + d}.$$
2. Läs och förstå beviset för Fyrpunktssatsen. Formulera och bevisa en Trepunktsats för $\mathbb{R}P^1$.

10.8 Projektiv klassificering av andragradskurvor.

En projektiv andragradskurva har utseendet
$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0.$$
Precis som i det affina fallet är det lämpligare att betrakta homogena andragradspolynom upp till projektiva transformationer, snarare än kurvor.

Sats. Varje homogent polynom av grad 2 över $\mathbb{R}$ är projektivt ekvivalent med exakt en av följande. Dess nollställesmängd beskrivs i parentes.

(a) $x^2 + y^2 - z^2$ (cirkeln)

(b) $x^2 - y^2$ (linjekorset)

(c) $x^2 + y^2$ (punkten)

(d) x^2 ('dubbellinjen')

(e) $x^2 + y^2 + z^2$ (tomma mängden)

Bevis. Detta är omedelbart från klassificeringen av kvadratiska former i tre variabler. De möjliga signaturerna är $\pm(1, 1, 1)$ (e), $\pm(1, 1, -1)$ (a), $\pm(1, 1, 0)$ (c), $\pm(1, -1, 0)$ (b) eller $\pm(1, 0, 0)$ (d). Varje kvadratisk form är ekvivalent med en av dessa enligt Sylvesters tröghetssats. Vi kan annars utgå ifrån vår affina klassificering och notera att redan de inledande exemplen i teorin för projektiva planet visar att de tre irreducibla kurvorna ellips, hyperbel och parabel är projektivt ekvivalenta samt att kurvan som består av två parallella linjer är projektivt ekvivalent med ett linjekors.

10.9 Skärningstalet återbesökt.

Vi definierar skärningstalet $I_P(f, g)$ mellan två projektiva kurvor i en punkt P som det affina skärningstalet i någon affin karta. Vi ersätter härvid Axiom 0 med invarians under projektiva transformationer så att vi är säkra på att valet av affin karta inte spelar någon roll.

Övningar.

1. Beräkna skärningstalet mellan de två projektiva kurvorna $F(x,y,z) = x+z$ och $G(x,y,z) = x+2z$ i de punkter där de skär varandra.

2. Beräkna skärningstalet mellan de två projektiva kurvorna $F(x,y,z) = x^2 + yz = 0$ och $g(x,y,z) = z$ i de projektiva punkter där de skär varandra.

11 Komplex projektiv geometri

11.1 Projektiva rum över $\mathbb{C}$

Vi definierar komplexa projektiva planet precis som det reella, men med $\mathbb{R}$ ersatt med $\mathbb{C}$ överallt.

Definition. Det projektiva planet $\mathbb{C}P^2$ är mängden av alla komplexa linjer genom origo i $\mathbb{C}^3$. Med andra ord är det mängden av ekvivalensklasser av nollskilda punkter i $\mathbb{C}^3$ under ekvivalensrelationen $(x,y,z) \sim (tx,ty,tz)$ (som identifierar två punkter omm de ligger på samma komplexa linje genom origo).

Definition. Vi betecknar punkter i projektiva planet med s.k. *homogena koordinater*, vilket helt enkelt är komponenterna (x,y,z) av någon punkt i ekvivalensklassen ifråga. En ekvivalensklass kallas en *projektiv punkt*.

Definition. Vi definierar *den affina xy-standardkartan* på $\mathbb{C}P^2$ som mängden av alla projektiva punkter vars homogena z-koordinat är nollskild. Eftersom varje sådan punkt har en unik representant av formen $(x,y,1)$ kan denna mängd naturligt identifieras med det komplexa $xy1$-planet i $\mathbb{C}^3$ (och därför med $\mathbb{C}^2$). *Linjen i oändligheten* sedd från den affina xy-standardkartan är komplementet av den i $\mathbb{C}P^2$, dvs mängden av alla projektiva punkter med $z = 0$.

Anmärkning. På samma sätt definieras de affina yz- och $xz-$standardkartorna och deras linjer i oändligheten.

Anmärkning. $\mathbb{C}P^2$ är en fyrdimensionell glatt kompakt Hausdorffmångfald. Beviset är rättframt, men utelämnas. Vänta på din kurs i topologi.

Anmärkning. Givet ett homogent polynom $F(x,y,z)$ är dess nollställesmängd $V(F)$ i $\mathbb{C}P^2$ väldefinierad.

Definition. $V(F)$ i föregående anmärkning kallas *en plan projektiv kurva*.

Anmärkning. Snittet mellan $V(F)$ och standardkartorna utgör affina kurvor i dessa. Varje projektiv kurva har alltså flera affina representationer.

Exempel 1/Definition. $ax + by + cz = 0$ kallas en projektiv linje. I de affina standardkartorna ser den ut som någon av de affina linjerna $ax + by + c = 0$, $ax + b + cz = 0$ eller $a + by + cz = 0$. (I undantagsfall kan den resulterande affina linjen vara tom - nämligen om två

av koefficienterna är 0, så att linjen är linjen i oändligheten för den kartan.)

Definition. Om F är som ovan och $F(P) = 0$ och $\nabla F(P) \neq 0$ så kallas

$$\frac{\partial F}{\partial x}(P)x + \frac{\partial F}{\partial y}(P)y + \frac{\partial F}{\partial z}(P)z = 0$$

för *tangentlinjen* i P . (Notera att denna linje är homogeniseringen av den affina tangentlinjen som tidigare definierat.)

11.2 Komplexa projektiva linjen $\mathbb{C}P^1$.

Det enklaste exemplet på ett komplext projektivt rum är den komplexa projektiva linjen, $\mathbb{C}P^1$. Den är betydligt intressantare i sig själv än sin reella kusin. Den är av central betydelse i komplex analys, där den oftast går under beteckningen "riemannsfären". Nedan kommer ordagranna repetitioner av definitionerna i reella fallet, för fullständighetens skull.

Definition. Den projektiva linjen $\mathbb{C}P^1$ är mängden av alla komplexa linjer genom origo i $\mathbb{C}^2$. Med andra ord är det mängden av ekvivalensklasser av nollskilda punkter (x, y) i $\mathbb{C}^2$ under ekvivalensrelationen $(x, y) \sim (tx, ty)$, $t \in \mathbb{C} \setminus \{0\}$.

Definition. Vi betecknar punkter i projektiva linjen med *homogena koordinater*, vilket helt enkelt är komponenterna (x, y) av någon punkt i ekvivalensklassen ifråga. En ekvivalensklass kallas en *projektiv punkt*.

Vi har även här affina kartor, i vilka man kan se de punkter där en viss koordinat är nollskild. T.ex. innehåller x-kartan alla projektiva punkter $(x, 1)$ med nollskild y-koordinat. Dessa kan betecknas med ett unikt komplext tal x och utgör därför en kopia av $\mathbb{C}$. Notera att oändligheten här bara består av en enda projektiv punkt (linjen $y = 0$) och att $\mathbb{C}P^1$ därför topologiskt ser ut som en sfär. Som vanligt är punkten i oändligheten är inte speciell sedd från ett projektivt perspektiv, det är ju bara att byta karta.

En *projektiv transformation* av $\mathbb{C}P^1$ ges av en inverterbar linjär avbildning på $\mathbb{C}^2$, dvs. en inverterbar matris

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

11.2.1 Dubbelförhållandet.

Ordagrant samma definition som i reella fallet kan användas för att definiera dubbelförhållandet av fyra punkter på $\mathbb{C}P^1$. Det är väldefinierat och projektivt invariant av samma skäl, nämligen linjär algebra.

Definition. Låt P_1, P_2, P_3 och P_4 vara projektiva punkter på $\mathbb{C}P^1$ och låt $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ och $\mathbf{e}_4$ vara vektorrepresentanter i $\mathbb{C}^2 \setminus \{0\}$ för dessa punkter. *Dubbelförhållandet* $R(P_1, P_2, P_3, P_4) \in \mathbb{C}$ definieras som

$$R(P_1, P_2, P_3, P_4) = \frac{\det(\mathbf{e}_1, \mathbf{e}_2)\det(\mathbf{e}_3, \mathbf{e}_4)}{\det(\mathbf{e}_1, \mathbf{e}_4)\det(\mathbf{e}_3, \mathbf{e}_2)}.$$

Anmärkning. Det komplexa fallet är geometriskt mycket intressantare än det reella, eftersom de fyra punkterna nu ligger på en reellt tvådimensionell sfär $\mathbb{C}P^1$ istället för på en cirkel $\mathbb{R}P^1$.

I övningarna nedan ser vi att projektiva transformationer av $\mathbb{C}P^1$ ges av så kallade Möbiustransformationer. Dessa, tillsammans med dubbelförhållandet, kommer att återkomma i kursen i komplex analys. I den kursen kommer man att huvudsakligen befinna sig i en fixerad karta $\mathbb{C}$ och det är inte ens säkert att någon talar om för er att de kommer från projektiva transformationer, utan istället introduceras de som konforma (vinkelbevarande) avbildningar från $\mathbb{C}$ till $\mathbb{C}$.

Övningar.

1. Visa att en allmän projektiv transformation av den projektiva linjen som ovan ges, i x-kartan, av (en så kallad Möbiustransformation)

$$x \mapsto \frac{ax + b}{cx + d}.$$

2. Visa att möbiustransformationen ovan kan skrivas som sammansättningen $F_4 \circ F_3 \circ F_2 \circ F_1$, där $F_1(x) = x + d/c$, $F_2(x) = 1/x$, $F_3(x) = (bc - ad)z/c^2$ och $F_4(x) = x + a/c$.

3. I x-kartan i $\mathbb{C}P^1$ som ju är ett reellt tvådimensionellt plan $\mathbb{C}$, finns förstås en massa vanliga reella linjer och euklidiska cirklar. Visa att bilden av en cirkel eller linje under en möbiustransformation är en cirkel eller en linje (använd förra uppgiften - påståendet bör vara uppenbart för allt utom F_3.).

11.3 Projektiva transformationer över $\mathbb{C}$

. **Definition.** En inverterbar linjär avbildning $F : \mathbb{C}^3 \to \mathbb{C}^3$ inducerar en avbildning $F_P : \mathbb{C}P^2 \to \mathbb{C}P^2$ eftersom F tar komplexa linjer genom origo till komplexa linjer genom origo. En sådan avbildning F_P kallas en *projektiv transformation* och vi betecknar ofta $F_P = F$ om inga missförstånd riskerar att uppstå.

Linjära avbildningar $F : \mathbb{C}^3 \to \mathbb{C}^3$ ges av 3×3-matriser på samma sätt som i reell linjär algebra och av samma skäl - de är bestämda av sina värden på tre linjärt oberoende vektorer. En linjär avbildning är inverterbar om och endast om dess determinant är nollskild. Två linjära avbildningar som skiljer sig åt på en komplex skalär multipel inducerar samma avbildning på den projektiva planet: $F_P = (\lambda F)_P$.

Övningar.

1. Gå igenom exemplen på reella projektiva transformationer och fundera på om något allvarligt händer ifall koefficienterna är komplexa istället.

2. Gå igenom beviset av fyrpunktssatsen och försäkra dig om att den fortfarande gäller om koefficienterna är komplexa.

11.4 Projektiv klassificering av andragradskurvor.

Sats. Varje homogent polynom av grad 2 över $\mathbb{C}$ är projektivt ekvivalent med exakt en av följande. Värt att notera är att (a) är irreducibelt, medan (b) och (c) är reducibla.

(a) $x^2 + y^2 + z^2$ (Cirkel.)

(b) $x^2 + y^2$ (Linjekors.)

(c) x^2 (Dubbellinje.)

Bevis. Detta är omedelbart från den komplexa klassificeringen av kvadratiska former i tre dimensioner. Varje sådan är ekvivalent med $Q(\mathbf{r}) = \mathbf{r}^T A\mathbf{r}$ där A är en av en av följande matriser: $\mathrm{diag}(1,1,1)$, $\mathrm{diag}(1,1,0)$ eller $\mathrm{diag}(1,0,0)$.

Anmärkning. Vi ser att "cirkeln" är den enda icke-singulära komplexa projektiva andragradskurvan.

Övningar.

1. Bestäm de komplexa projektiva punkter $P \in \mathbb{C}P^2$ där de två kurvorna f, g nedan skär varandra. Ange homogena koordinater för dem. Rita också illustrativa figurer som visar hur realdelarna av kurvorna ser ut i $\mathbb{R}P^2$.

   (a) $f(x,y) = 2x^2 + 4y^2 - 1$, $g(x,y) = x^2 - 4y^2 - 2$.
   (b) $f(x,y) = y - x^3$, $g(x,y) = y^2 - x^4$.

2. Låt A, B, C, D vara fyra punkter på en projektiv linje. Visa att det finns en projektiv transformation som byter plats på A och C samt på B och D.

3. Betrakta den komplexa plana projektiva kurva som i den affina xy-kartan ges av ekvationen

$$x^3 + y^3 + 3xy + y^2 = 0.$$

   (a) Ange kurvans singulära punkter.
   (b) Bestäm de generaliserade tangentlinjerna.
   (c) Bestäm homogena koordinater för de punkter där kurvan skär linjen i ∞, L_∞.
   (d) Bestäm skärningstalet mellan C och L_∞ i dessa punkter.

12 Bezouts sats, formulering och bevis.

I detta avsnitt bevisar vi en av de grundläggande satserna i denna kurs.

Sats (Bezout) Låt F och G vara två homogena polynom i tre variabler, utan gemensamma faktorer. Då är

$$I(F,G) = \deg F \cdot \deg G.$$

Beviset av Bezouts sats organiseras i ett antal Lemman. Det första gör explicit vad skärningstalet är då en av de inblandade kurvorna är en graf till en polynomfunktion $p(x)$. De utspelar sig helt i det affina planet.

Det första lemmat visar att Bezouts sats är sann då den ena kurvan är en projektiv linje, given av ett homogent polynom L, av grad 1. Eftersom det finns en projektiv transformation som tar L till linjen $y = 0$ så räcker det att visa påståendet i detta speciella fall, där räkningarna blir lätta. Notera att $y = 0$ är en graf till polynomfunktionen $p(x) = 0$, så vi kan använda Lemma 1 med $p(x) = 0$.

Lemma 1. Låt $G(x, y, z)$ vara ett homogent polynom av grad n och låt L vara av grad 1 (en linje). Då är $I(G, L) = n$.

Bevis. Genom en projektiv transformation kan L transformeras till y. Detta transformerar även G till ett nytt polynom av grad n som vi för enkelhets skull också kallar G. Eftersom projektiva transformationer bevarar skärningstalet räcker det att visa påståendet i Lemmat för $L = y$. Även detta kan göras genom en direkt räkning. Först beräknar vi bidraget till $I(G, y)$ från skärningspunkter med ändliga koordinater i xy-kartan, sedan från linjen i oändligheten $z = 0$. Vi skriver alltså först

$$G(x,y,z) = \sum_{i,j} c_{ij} x^i y^j z^{n-i-j}$$

och låter

$$g(x,y) = G(x,y,1) = \sum_{i,j} c_{ij} x^i y^j$$

vara motsvarande affina kurva i xy-kartan. Enligt en sats i avsnitt 9.2 är bidraget till det totala skärningstalet $I(G, y)$ från skärningspunkter $(a_i, 0)$ i denna karta detsamma som graden $d = s_1 + ... + s_\nu$ av polynomet

$$g(x,p(x)) = g(x,0) = G(x,0,1) = \sum_i c_{i0} x^i = c_{d0}(x-a_1)^{s_1} \cdot ... \cdot (x-a_\nu)^{s_\nu}$$

(Alla termer där $j \neq 0$ försvinner.) Observera att ett sätt att beskriva d är som det största värdet på index i sådant att $c_{i0} \neq 0$. Nu behöver vi se vad som eventuellt händer i ∞. Eftersom $y = 0$ är en linje har den bara en punkt i oändligheten, nämligen $P = [1 : 0 : 0]$. Vi ska alltså

beräkna skärningstalet $I_P(G, y)$ och detta gör vi i yz-kartan, där $P = (0, 0)$. Kurvan G har i denna karta utseendet

$$\hat{g}(y, z) = G(1, y, z) = \sum_{i,j} c_{ij} y^j z^{n-i-j}.$$

Vi har att

$$I_P(G, y) = I_{(0,0)}(\hat{g}, y) = \text{mult}_0(\hat{g}(0, z))$$

och

$$\hat{g}(0, z) = G(1, 0, z) = \sum_i c_{i0} z^{n-i}.$$

Den lägsta nollskilda potensen av z som förekommer motsvarar det största värdet på i sådant att $c_{i0} \neq 0$. Detta värde är d enligt ovan, så $I_{(0,0)}(G, y) = \text{mult}_0(\hat{g}(0, z)) = n - d$.

Det totala skärningstalet är nu $I(G, y) = d + (n - d) = n$, vilket skulle bevisas.

Vårt nästa lemma visar att faktorer som bara beror av två variabler kan ignoreras när vi ska bevisa Bezouts sats. Detta beror på att sådana kan faktoriseras i linjära faktorer, för vilka Bezouts sats gäller enligt Lemma 1. Låt B$ez(f, g)$ vara påståendet $I(f, g) = \deg(f) \deg(g)$.

Lemma 2. Låt F, G, H vara homogena polynom av grad m, n, p. Antag att $H = H(x, z)$ är oberoende av y och att G och H saknar gemensamma faktorer. Då gäller

$$\text{B}ez(FH, G) \iff \text{B}ez(F, G).$$

Bevis. $H(x, z)$ är homogent i två variabler och kan därför faktoriseras i p linjära faktorer: $H(x, z) = L_1 \cdot ... \cdot L_p$. Då har vi

$$I(H, G) = I(L_1 \cdot ... \cdot L_p, G) = I(L_1, G) + ... + I(L_p, G) = pn,$$

enligt Lemma 2. Vidare har vi

$$I(FH, G) = I(F, G) + I(H, G) = I(F, G) + pn.$$

Vi ser direkt från detta att

$$I(FH, G) = (m + p)n \iff I(F, G) = mn,$$

dvs.

$$\text{B}ez(FH, G) \iff \text{B}ez(F, G),$$

vilket var vad ville bevisa.

Lemma 3. Låt F, G vara homogena polynom utan gemensamma faktorer, sådana att

$$\deg_y G = t \leq \deg_y F = s.$$

Då finns homogena polynom F_1, G_1 utan gemensamma faktorer, sådana att

$$\deg_y F_1 < \deg_y F,$$
$$\deg_y G_1 = \deg_y G$$

och

$$\mathrm{B}ez(F,G) \iff \mathrm{B}ez(F_1,G_1).$$

Bevis. Vi definierar G_1 genom att bryta ut den maximala y-oberoende faktorn $H = H(x,z)$ ur G, dvs vi skriver $G = HG_1$ där H är oberoende av y och G_1 inte innehåller någon y-oberoende faktor. Vi noterar att

(a) G_1 har inte någon gemensam faktor med F (eftersom då G och F skulle ha gemensam faktor.)

(b) $\deg_y G_1 = \deg_y G = t$.(eftersom $\deg_y H = 0$.)

För att definiera F_1 betraktar vi G_1 och F som polynom i y och skriver

$$G_1 = y^t Q(x,z) + \text{termer med lägre } y\text{-grad.}$$
$$F = y^s P(x,z) + \text{termer med lägre } y\text{-grad.}$$

Vi vill eliminera högsta y-termen i F så vi multiplicerar G_1 med Py^{s-t} och F med Q och subtraherar. Då får vi

$$F_1 = QF - Py^{s-t}G_1.$$

Vi ser nu att

(i) F_1 har lägre y-grad än F per konstruktion.

(ii) F_1 och G_1 saknar gemensamma faktorer: Om K vore en gemensam irreducibel faktor skulle K också vara en faktor i $QF = F_1 + Py^{s-t}G_1$ och alltså i antingen Q eller F. Men om $K|Q$ skulle K vara y-oberoende och alltså inte en faktor i G_1. Om $K|F$ skulle det motsäga (a).

Slutligen, genom användning av Lemma 2 och räknereglerna för skärningstal har vi

$$\mathrm{B}ez(F,G) = \mathrm{B}ez(F,G_1H) \iff \mathrm{B}ez(F,G_1) \iff$$
$$\iff \mathrm{B}ez(QF,G_1) \iff \mathrm{B}ez(QF - Py^{s-t}G_1, G_1) \iff \mathrm{B}ez(F_1,G_1).$$

vilket var vad ville bevisa.

Bevis av satsen. Låt F och G vara givna som i satsen. Genom upprepad användning av Lemma 3 kan vi anta att G är oberoende av y. Men då kan G faktoriseras i $\deg G$ linjära faktorer och vi har med hjälp av Lemma 1,

$$I(F,G) = I(F, L_1 \cdot \ldots \cdot L_{\deg G}) = \sum_{1 \le k \le \deg G} I(F,L_k) = \deg G \cdot \deg F.$$

Detta avslutar beviset av satsen.

13 Några tillämpningar av Bezouts sats

13.1 En kommentar om dimensionsräkning och en sats om andragradskurvor.

Alla polynom i detta avsnitt är homogena trevariabelpolynom om vi inte säger annat, men principerna är helt allmänna. Ett homogent förstagradspolynom

$$F(x, y, z) = ax + by + cz,$$

är helt bestämt av sina tre koefficienter. Med andra ord är rummet

$$V_1 = \{\text{homogena linjära polynom av grad } 3\} \cup \{0\},$$

ett linjärt rum av dimension 3, isomorft med $\mathbb{C}^3$. Om vi är intresserade av projektiva kurvor snarare än polynom, ger de två koefficientvektorerna (a, b, c) och (ka, kb, kc) samma projektiva linje, så rummet av projektiva linjer är $\mathbb{C}P^2$.[7] Låt $P_0 = (x_0, y_0, z_0)$. Om vi ställer kravet att F ska vara noll i P_0, ger detta ett linjärt homogent villkor på de tre koefficienterna (a, b, c):

$$x_0a + y_0b + z_0c = 0,$$

vilket minskar dimensionen till två, dvs. det linjära rummet

$$V_1(P_0) = \{F \in V_1 | F(P_0) = 0\} \cup \{0\},$$

är tvådimensionellt. Kravet på att ytterligare en punkt $P_1 = (x_1, y_1, z_1)$ ska vara nollställe, definierar en ekvation till och minskar lösningsrummets

$$V_1(P_0, P_1) = \{F \in V_1 | F(P_0) = F(P_1) = 0\} \cup \{0\},$$

dimension till ett (under förutsättning att P_0 och P_1 inte ligger på samma linje genom origo): Betraktar vi kurvor istället för polynom är dimensionen minskad till 0, dvs. det finns exakt en linje genom två projektiva punkter (som vi har sett tidigare). Andragradspolynom definieras av sex koefficienter. Med samma sorts resonemang som ovan, borde alltså fem punkter definiera en unik andragradskurva. Det är det ungefärliga innehållet i följande sats. För att varje punkt ska tillföra en linjärt oberoende ekvation, tillför vi ett ytterligare villkor.

Sats. Fem distinkta punkter $P_1, ..., P_5$ i $\mathbb{C}P^2$ är givna, sådana att det inte finns tre av dem som ligger på samma räta linje. Då finns en unik andragradskurva C som passerar genom dem alla, och denna kurva är irreducibel.

Bevis. Låt $L_{ij} = 0$ vara den linje som går genom P_i och P_j. Bilda andragradspolynomen $L_{12}L_{34}$ och $L_{13}L_{24}$. Då är $L_{12}(P_5)L_{34}(P_5) \neq 0$ och $L_{13}(P_5)L_{24}(P_5) \neq 0$, eftersom annars P_5 skulle ligga på samma linje som två andra punkter. Sätt

$$r = \frac{L_{12}(P_5)L_{34}(P_5)}{L_{13}(P_5)L_{24}(P_5)},$$

[7] Så rummet av projektiva linjer är detsamma som rummet av projektiva punkter! Kan du konstruera ett naturligt sätt att identifiera varje projektiv linje med en projektiv punkt och omvänt?

och definiera

$$Q = L_{12}L_{34} - rL_{13}L_{24}.$$

Det följer att $Q(P_i) = 0$ för $i = 1, ..., 5$. Vidare följer direkt från Bezouts sats att det inte kan finnas två olika andragradskurvor C, C' som går igenom $P_1, ..., P_5$, ty då skulle $4 = I(C, C') \geq 5$. Eftersom en reducibel andragradskurva består av en eller två linjer, kan den bara gå igenom $P_1, ..., P_5$ om en av linjerna innehåller minst tre punkter, vilket inte är fallet. Detta visar att Q är irreducibelt och avslutar beviset.

13.2 Singulära kurvor

Här ger vi ett par första tillämpningar på Bezouts sats och singulära punkter. Eftersom vi nu kommer att arbeta mestadels med projektiva kurvor omformulerar vi först definitionen på singulär punkt från tidigare.

Definition. Låt $F(x, y, z)$ vara ett homogent polynom. Om $F(a, b, c) = 0$ och $\nabla F(a, b, c) = 0$ kallas (a, b, c) en singulär punkt till kurvan $V(F)$.

Anmärkning. En projektiv punkt är singulär om och endast om den är singulär i någon karta enligt tidigare definition. T.ex. för en punkt som ligger i xy-kartan, $P = (a, b, 1)$ har vi enligt Eulers lemma:

$$\frac{\partial F}{\partial z}(a, b, 1) = dF(a, b, 1) - a\frac{\partial F}{\partial x}(a, b, 1) - b\frac{\partial F}{\partial y}(a, b, 1) =$$

$$= 0 - a\frac{\partial f}{\partial x}(a, b) - b\frac{\partial f}{\partial y}(a, b).$$

Sats. Varje icke-singulär kurva är irreducibel.

Bevis. Vi visar kontrapositionen: Varje reducibel kurva är singulär. Låt F vara ett homogent polynom som beskriver kurvan och antag att $F = GH$ där varken G eller H är konstant. Då är enligt Bezouts sats $I(G, H) \geq 1$ så det finns någon punkt P där $G(P) = H(P) = 0$. Men då är $\nabla F(P) = G(P)\nabla F(P) + F(P)\nabla G(P) = 0$, så P är en singulär punkt för F.

Kom ihåg satsen från tidigare, att skärningstalet är 1 precis om båda kurvorna är glatta i P och skär varandra transversellt i P. Det betyder speciellt att:

Sats. Om $F(P) = G(P) = 0$ och P är en singulär punkt för F eller G så är $I_P(F, G) > 1$.

Nästa sats ger en begränsning på hur många singulära punkter en kurva av grad d kan ha. Beviset sker genom dimensionsräkning.

Sats. En irreducibel projektiv kurva C av grad d har som mest

$$\binom{d-1}{2} = \frac{(d-1)(d-2)}{2}$$

singulära punkter.

Bevis. Fallen $d = 1, 2$ är kända som icke-singulära enligt tidigare. Låt $d \geq 3$. Vi antar, för att sedermera nå en motsägelse, att C har fler singulära punkter än angett, dvs minst

$$\frac{(d-1)(d-2)}{2} + 1$$

stycken. Markera nu ytterligare $d-3$ punkter på C, så att vi totalt har att göra med

$$\frac{(d-1)(d-2)}{2} + 1 + (d-3) = \binom{d}{2} - 1$$

speciella punkter på C.

Vi hävdar nu att det finns en kurva C' av grad $d-2$ som går igenom alla dessa punkter.

Mängden av homogena polynom i (x, y, z) av grad $d-2$ är nämligen ett vektorrum av dimension $\binom{d}{2}$ (= antalet koefficienter)[8]. Var och en av de ovannämnda punkterna ger en linjär homogen ekvation för de obekanta koefficienterna. Eftersom antalet ekvationer är lägre än antalet obekanta så finns icke-trivial lösning vilken ger den sökta kurvan C'. Låt oss nu beräkna totala skärningstalet mellan C och C'. Om C och C' skulle ha gemensamma faktorer, skulle C behöva vara en irreducibel komponent av C'. Men C' har lägre grad än C så det är omöjligt. Enligt Bezout är då $I(C, C') = d(d-2)$. Men eftersom varje singulär punkt i C kommer att motsvara ett bidrag till skärningstalet på minst 2 (enligt satsen som nämndes ovan) är

$$I(C, C') \geq 2(\binom{d-1}{2} + 1) + d - 3 = d(d-2) + 1,$$

vilket är en motsägelse.

13.3 Reella algebraiska kurvor och deras ovaler. Ej skrivet än.

Sats.(Harnack)

[8] Detta lämnar vi till studenten som en liten övning.

14 Tredjegradskurvor

14.1 Hessianen och inflexionspunkter.

Definition. Låt $F(x,y,z)$ vara ett polynom av grad d. Beteckna med $F_{xy} = \dfrac{\partial^2 F}{\partial x \partial y}$ osv. *Hessianen* $H(x,y,z)$ definieras som polynomet

$$H(x,y,z) = \det \begin{bmatrix} F_{xx} & F_{xy} & F_{xz} \\ F_{yx} & F_{yy} & F_{yz} \\ F_{zx} & F_{zy} & F_{zz} \end{bmatrix}.$$

Notera att H har grad $3(d-2)$.

Definition. En (projektiv) punkt $P = (a,b,c)$ på kurvan $F(x,y,z) = 0$ kallas *inflexionspunkt (eller flex)* om $H(a,b,c) = 0$.

Att detta är en rimlig generalisering av inflexionspunkter i envariabelanalys ska vi se efter beviset av följande Tekniska Lemma, som jag har hämtat från boken Complex Algebraic Curves av Frances Kirwan. Vi kommer även att använda det senare för klassificering av glatta tredjegradskurvor.

Tekniskt Lemma. Låt $F(x,y,z)$ vara ett homogent polynom av grad $d > 1$. Då är

Bevis. Eulers lemma om homogena funktioner säger att[9]

$$dF(x,y,z) = xF_x(x,y,z) + yF_y(x,y,z) + zF_z(x,y,z). \tag{1}$$

Eftersom F_x, F_y, F_z är homogena av grad $d-1$ har vi också

$$(d-1)F_x = xF_{xx} + yF_{xy} + zF_{xz} \tag{2}$$
$$(d-1)F_y = xF_{yx} + yF_{yy} + zF_{yz} \tag{3}$$
$$(d-1)F_z = xF_{zx} + yF_{zy} + zF_{zz} \tag{4}$$

Betrakta

$$zH(x,y,z) = \det \begin{bmatrix} F_{xx} & F_{xy} & F_{xz} \\ F_{yx} & F_{yy} & F_{yz} \\ zF_{zx} & zF_{zy} & zF_{zz} \end{bmatrix}.$$

Addera nu x gånger rad 1 och y gånger rad 2 till rad 3. Då får vi, med hjälp av ekvationerna (2)-(4)

$$zH(x,y,z) = \det \begin{bmatrix} F_{xx} & F_{xy} & F_{xz} \\ F_{yx} & F_{yy} & F_{yz} \\ (d-1)F_x & (d-1)F_y & (d-1)F_z \end{bmatrix} = (d-1)\det \begin{bmatrix} F_{xx} & F_{xy} & F_{xz} \\ F_{yx} & F_{yy} & F_{yz} \\ F_x & F_y & F_z \end{bmatrix}$$

[9]Beviset är en rättfram övning: En funktion $F(x,y,z)$ är homogen av grad d om $F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x,y,z)$. Derivera båda sidor m.a.p. λ och sätt sedan $\lambda = 1$. Eftersom vi i vår kurs bara har att göra med *polynom* kan vi förstås också göra detta explicit, genom att skriva $F = \sum_{i,j} c_{ij} x^i y^j z^{d-i-j}$ och beräkna båda sidor.

Om detta nu multipliceras med z får vi

$$z^2H(x,y,z) = (d-1)\det\begin{bmatrix} F_{xx} & F_{xy} & zF_{xz} \\ F_{yx} & F_{yy} & zF_{yz} \\ F_x & F_y & zF_z \end{bmatrix}$$

Addera nu x gånger kolumn 1 och y gånger kolumn 2 till kolumn 3. Då får vi på samma sätt som ovan

$$z^2H(x,y,z) = (d-1)\det\begin{bmatrix} F_{xx} & F_{xy} & (d-1)F_x \\ F_{yx} & F_{yy} & (d-1)F_y \\ F_x & F_y & dF \end{bmatrix}$$

I zz-luckan har vi utnyttjat ekvation (1). Bryter vi nu ut $(d-1)$ ur sista kolumnen har vi visat påståendet.

Med hjälp av detta kan vi nu se den utlovade relationen till vanliga inflexionspunkter. Betrakta en projektiv kurva i xy-kartan: $F(x,y,1) = 0$. Antag att $F_y \neq 0$ och derivera två gånger implicit m.a.p. x. Då får vi först $F_x + y'F_y = 0$ och sedan $F_{xx} + 2y'F_{xy} + y''F_y + (y')^2F_{yy} = 0$. Löser vi ut y' ur den första av dessa ekvationer och sätter in i den andra kan vi skriva (efter en del förenklingar)

$$y''(x) = \frac{2F_xF_yF_{xy} - (F_y)^2F_{xx} - (F_x)^2F_{yy}}{(F_y)^3} = \frac{1}{(F_y)^3}\det\begin{bmatrix} F_{xx} & F_{xy} & F_x \\ F_{yx} & F_{yy} & F_y \\ F_x & F_y & 0 \end{bmatrix} = \frac{H(x,y,1)}{(F_y)^3(d-1)^2}.$$

Vi ser att $y''(x) = 0$ om och endast om $H(x,y,1) = 0$.

Sats. En irreducibel kurva av grad $d \geq 3$ har minst en och som mest $3d(d-2)$ inflexionspunkter.

Bevis. Eftersom $\deg(F) = d$ och $\deg(H) = 3(d-2)$ är enligt Bezouts sats $I(F,H) = 3d(d-2)$ om F och H saknar gemensamma faktorer och påståendet följer direkt från detta. Eftersom F är irreducibel, gäller att om F och H har en gemensam faktor måste $F|H$. Men då är $H = 0$ längs hela $F = 0$ och alla punkter på F är inflexionspunkter. Men då är F en linje[10] vilket är en motsägelse.

Sats. Låt F vara ett homogent polynom av grad d. Beteckna med $T_P(F)$ tangentlinjen i punkten P. Då gäller P är en inflexionspunkt till $F \iff I_P(F, T_PF) \geq 3$.

Bevis. Formeln från vårt tekniska lemma uträknad i en punkt P på kurvan $F(x,y,z) = 0$ visar att

$$0 = \det\begin{bmatrix} F_{xx} & F_{xy} & F_x \\ F_{yx} & F_{yy} & F_y \\ F_x & F_y & 0 \end{bmatrix} = -F_{xx}F_y^2 - F_{yy}F_x^2 + 2F_{yx}F_xF_y,$$

[10]Detta är väl lätt att tro på. Skiss till ett noggrant bevis: Derivera $F = 0$ implicit m.a.p x efter att ha garanterat $F_y \neq 0$ genom en lämplig projektiv transformation och få en ekvation $y'' = 0$ vilket bara har lösningen $y(x) = kx + m$.

om och endast om P är en inflexionspunkt. Efter en projektiv transformation kan vi anta att P motsvarar punkten $(0,0)$ i xy-kartan. Med notationen $F(x,y,1) = f(x,y)$ har vi alltså

$$f_{xx}f_y^2 + f_{yy}f_x^2 - 2f_{yx}f_xf_y = 0,$$

där alla derivator är uträknade i $(0,0)$. Taylorutvecklar vi $f(x,y)$ får vi nu

$$f(x,y) = f_x x + f_y y + \frac{1}{2}\begin{bmatrix} x & y \end{bmatrix}\begin{bmatrix} f_{xx} & f_{xy} \\ f_{yx} & f_{yy} \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} + \text{termer av högre grad},$$

(åter är alla derivator underförstått uträknade i $(0,0)$). T_PF ges av $f_x x + f_y y = 0$. Vi kan anta att $f_y \neq 0$. Då får vi med en rättfram räkning

$$f(x, -\frac{f_x}{f_y}x) = \frac{1}{2}\begin{bmatrix} x & -\frac{f_x}{f_y}x \end{bmatrix}\begin{bmatrix} f_{xx} & f_{xy} \\ f_{yx} & f_{yy} \end{bmatrix}\begin{bmatrix} x \\ -\frac{f_x}{f_y}x \end{bmatrix} + ... = \frac{1}{2}x^2\frac{(f_{xx}f_y^2 + f_{yy}f_x^2 - 2f_{yx}f_xf_y)}{f_y^2} + ...$$

Eftersom $I_{(0,0)}(f, y + \frac{f_x}{f_y}x) = \text{mult}_0 f(x, -\frac{f_x}{f_y}x)$ ser vi nu att skärningstalet är större än 3 om och endast om P är en inflexionspunkt. Detta var vad vi ville bevisa.

14.2 Klassificering av glatta projektiva tredjegradskurvor

Vi inför härmed beteckningen *glatt* kurva som en stavelsebesparande synonym till *icke-singulär* kurva. Vi har redan sett att glatta andragradskurvor alla är projektivt ekvivalenta.[11] Följande sats är motsvarande påstående för kurvor av grad 3.

Sats. Låt C vara en glatt projektiv tredjegradskurva i $\mathbb{C}P^2$. Då finns en projektiv transformation som tar C till kurvan given av

$$y^2z = x(x-z)(x-\lambda z)$$

för något $\lambda \in \mathbb{C} \setminus \{0,1\}$.

Bevis. (från Kirwan, Complex algebraic curves). C har en inflexionspunkt enligt en sats i förra kapitlet. Den kan vi anta ligger i $(0,1,0)$ efter en lämplig projektiv transformation[12]. Efter en rotation av xz-planet kan vi anta att tangentlinjen till C är linjen $z = 0$. Då ges C av $F(x,y,z) = 0$, där $F(0,1,0) = 0 = F_x(0,1,0) = F_y(0,1,0) = H(0,1,0)$. Från vårt tekniska lemma i förra kapitlet följer (vi måste byta plats på y och z och sätta $d = 3$).

$$y^2H(x,y,z) = 4\det\begin{bmatrix} F_{xx} & F_x & F_{xz} \\ F_x & \frac{3}{2}F & F_z \\ F_{zx} & F_z & F_{zz} \end{bmatrix}$$

[11] I fallet med andragradskurvor är alla irreducibla kurvor glatta, vilket inte är fallet för kurvor av högre grad.
[12] Projektiva transformationer avbildar inflexionspunkter till inflexionspunkter: En övning till en senare lektion.

Om vi nu sätter $(x, y, z) = (0, 1, 0)$ får vi

$$0 = H(0,1,0) = 4 \det \begin{bmatrix} F_{xx} & 0 & F_{xz} \\ 0 & 0 & F_z \\ F_{xz} & F_z & F_{zz} \end{bmatrix} = -4(F_z)^2 F_{xx}.$$

Men $F_z(0,1,0) \neq 0$, eftersom $(0,1,0)$ annars vore en singulär punkt, så vi måste ha $F_{xx}(0,1,0) = 0$. Detta betyder att det linjära polynomet F_{xx} saknar y-term:

$$F_{xx}(x, y, z) = Ax + Cz.$$

Integrerar vi m.a.p. x får vi ett polynom på formen

$$F_x(x, y, z) = Ax^2 + Bxz + Cyz + Dz^2.$$

Ingen y^2-term dyker upp här eftersom $F_x(0,1,0) = 0$. Ytterligare en integration ger ett polynom på formen:

$$F(x, y, z) = Ax^3 + Bx^2 z + axyz + Cxz^2 + cyz^2 + Dz^3 + by^2 z.$$

Ingen y^3-term, eftersom $F(0,1,0) = 0$. Vi skriver detta lite lämpligare och utnyttjar att $b = F_z(0,1,0) \neq 0$.

$$F(x, y, z) = yz(ax + by + cz) + h(x, z) = bz(y^2 + y\frac{ax + cz}{b}) + h(x, z).$$

Kvadratkomplettering i y ger nu:

$$F(x, y, z) = bz((y + \frac{ax + cz}{2b})^2 - (\frac{ax + cz}{2b})^2) + h(x, z).$$

Den projektiva transformationen $x \mapsto x$, $y + \dfrac{ax + cz}{2b} \mapsto y$ och $z \mapsto z$ ger oss nu $F(x, y, z) = bzy^2 + h(x, z)$, där $h(x, z)$ kan faktoriseras i tre linjära faktorer eftersom det är ett homogent polynom av två variabler. Om koefficienten framför x^3 vore noll så skulle z vara en faktor i $F(x, y, z)$ vilket motsäger dess irreducibilitet. Alltså kan vi efter en omskalning av variablerna x, y, z skriva $F = 0$ som

$$zy^2 = (x - az)(x - bz)(x - cz),$$

där a, b, c är olika eftersom kurvan annars är singulär (Varför?).

Nu ger transformationen $(x, y, z) \mapsto (x + az), y, z)$ ekvationen

$$zy^2 = x(x - (b - a)z)(x - (c - a)z),$$

som efter ytterligare en diagonal transformation $(x, y, z) \mapsto (x, \eta y, \dfrac{z}{b - a})$ ger det önskade resultatet

$$y^2 z = x(x - z)(x - \lambda z)$$

med $\lambda = \dfrac{c - a}{b - a}$. Här är η valt som någon rot till $\eta^2 = b - a$. Detta avslutar beviset.

Denna sats visar att man alltid kan reducera en icke-singulär tredjegradskurva till denna standardform för något värde på parametern λ. Man kan också beskriva exakt vilka av dessa λ som beskriver ekvivalenta kurvor, men detaljerna för detta lämnar vi till fritt sökande på nätet. Ett nyckelord är Kleins J-invariant. Det visar sig att två kurvor svarande mot parametervärdena λ och μ är projektivt ekvivalenta om och endast om μ har ett av värdena

$$\lambda,\ \frac{1}{\lambda},\ 1-\lambda,\ \frac{1}{1-\lambda},\ \frac{\lambda-1}{\lambda},\ \frac{\lambda}{\lambda-1}.$$

Sats. En glatt tredjegradskurva i $\mathbb{C}P^2$ har exakt nio inflexionspunkter.

Bevis. Bezouts sats garanterar att antalet inflexionspunkter inte är mer än nio. Beviset av satsen ovan visar att en inflexionspunkt P kan flyttas till $(0,1,0)$ med en projektiv transformation så att kurvan sedan har formen

$$F(x,y,z) = y^2z - x(x-z)(x-\lambda z) = 0.$$

Direkta räkningar (övning) visar då $\nabla F(0,1,0) = (0,0,1)$ och $\nabla H_F(0,1,0) = (24,0,8(\lambda-1))$. Dessa är inte parallella, så tangentlinjerna till $F=0$ och $H=0$ är olika i $(0,1,0)$. Med andra ord skär kurvorna transversellt i varje inflexionspunkt P så att $I_P(F,H) = 1$. Det följer att antalet inflexionspunkter inte kan vara mindre än nio.

14.3 Klassificering av singulära tredjegradskurvor.

Vi såg i förra kapitlet att det finns en familj av glatta tredjegradskurvor parametriserad av en komplex parameter λ. När det gäller singlära kurvor är situationen annorlunda. Det finns exakt två stycken sådana upp till projektiva transformationer. Det är innebörden av huvudsatsen i detta kapitel. I beviset kommer vi att utnyttja följande lilla hjälpsats om att skriva om kubiska polynom.

Lemma. (*Kubikkomplettering.*) Låt $p(x,y)$ vara ett homogent tredjegradspolynom, moniskt i x.

(a) Det finns A, B, β sådana att

$$p(x,y) = (x+\beta y)^3 + y^2(Ax+By).$$

(b) Det finns A, B, β sådana att

$$p(x,y) = (x+\beta y)^3 + xy(Ax+By).$$

Bevis. Bevisen för båda påståendena följer direkt från binomialutvecklingen. Låt

$$p(x,y) = x^3 + bx^2y + cxy^2 + dy^3,$$

vara givet.

(a) Låt vidare β vara sådant att $3\beta = b$. Då kan vi skriva

$$p(x,y) = x^3+bx^2y+cxy^2+dy^3 = x^3+bx^2y+(3\beta^2xy^2+\beta^3y^3)-(3\beta^2xy^2+\beta^3y^3)+cxy^2+dx^2y =$$

$$(x+\beta y)^3 + y^2((c-3\beta^2)x + (d-\beta^3)y) = (x+\beta y)^3 + y^2(Ax+By).$$

(b) Låt nu istället β vara sådant att $\beta^3 = d$. Då kan vi skriva

$$p(x,y) = x^3+bx^2y+cxy^2+dy^3 = x^3+(3\beta x^2y+3\beta^2xy^2)+dy^3-(3\beta x^2y+3\beta^2xy^2)+bx^2y+cxy^2$$

$$= (x+\beta y)^3 + xy((b-3\beta)x + (c-3\beta^2)y) = (x+\beta y)^3 + xy(Ax+By).$$

Sats. Låt C vara en singulär irreducibel tredjegradskurva i $\mathbb{C}P^2$. Då finns en projektiv transformation som tar C till kurvan given av antingen ekvationen

$$y^2z = x^2(x+z),$$

eller ekvationen

$$y^2z = x^3.$$

Bevis. Enligt satsen om singulära punkter i förra kapitlet har C exakt en singulär punkt. Efter en projektiv transformation kan vi anta att den singulära punkten är $(0,0,1)$. Då ges C av en ekvation utan z^3-term och utan termer som är linjära i x och y (detta inses t.ex. genom att Maclaurinutveckla i xy-kartan). Den högsta förekommande z-graden är därför 1 och vi kan skriva

$$q(x,y)z = p(x,y),$$

där $p(x,y)$ har grad 3 och $q(x,y)$ har grad 2. Efter en rotation och en skalning kan vi anta att q är moniskt i y. $q(x,y)$ kan faktoriseras i två linjära faktorer enligt $q(x,y) = (ax+y)(bx+y)$. Vi har nu två fall. Antingen är $a = b$ (Fall A) eller $a \neq b$ (Fall B).

Fall A. Vi gör variabelbytet $x \to x, ax+y \to y, z \to z$ och ekvationen får formen

$$y^2z = p(x,y).$$

Notera att koefficienten framför x^3 i $p(x,y)$ är nollskild, ty annars är kurvan reducibel (den innehåller då linjen $y = 0$). Vi kan genom att skala om x anta att p är moniskt i x. Nu noterar vi att Lemmats del (a) ovan tillåter oss att skriva

$$y^2z = (x+\beta y)^3 + y^2(Ax+By) \iff y^2(-Ax-By+z) = (x+\beta y)^3$$

Nu kan vi göra variabelbytet $-Ax-By+z \to z$ så att ekvationen får utseendet $y^2z = (x+\beta y)^3$. Sätter vi nu bara $x+\beta y \to x$ så har vi ekvationen

$$y^2z = x^3.$$

Fall B. I det andra fallet gör vi variabelbytet

$$bx + y \to x, ax + y \to y, z \to z,$$

vilket ger en ekvation på formen

$$xyz = p(x, y).$$

Återigen måste koefficienten framför x^3 i p vara nollskild för att kurvan ska kunna vara irreducibel. Lemmats del (b) ovan tillåter oss att skriva ekvationen som:

$$xyz = (x + \beta y)^3 + xy(Ax + By) \iff xy(z - Ax - By) = (x + \beta y)^3.$$

Vi gör sedan variabelbytet $(x, y, z) \to (x, y, z - Ax - By)$ som ger ekvationen formen

$$xyz = (x + \beta y)^3.$$

Här kan vi göra variabelbytet $(x, y, z) \to (x, y/\beta, \beta z)$ ($\beta \neq 0$ av irreducibilitetsskäl) och få

$$xyz = (x + y)^3.$$

Nu gör vi variabelbytet $(x, y, z) \to (\frac{x+y}{2}, \frac{x-y}{2}, -4z)$, vilket ger

$$\frac{1}{4}(y + x)(y - x)4z = x^3 \iff y^2 z = x^2(x + z).$$

15 Elliptiska kurvor.

15.1 Additionslagen.

Låt C vara en glatt projektiv kurva av grad 3 och låt $O \in C$ vara en fixerad punkt. Låt $P, Q \in C$ vara två godtyckliga punkter. Betrakta den linje som går igenom P och Q. Om P och Q råkar vara samma punkt låter vi detta betyda tangentlinjen i P. Enligt Bezouts sats skär linjen kurvan C i en tredje punkt. Kalla denna punkt för $P * Q$. Tag nu den linje som går igenom O och $P * Q$ [13]. Denna linje skär C i en tredje punkt, som vi kallar $P + Q$. Att denna konstruktion ger en vettig additionslag på C är innehållet i följande sats.

Sats. Den ovanstående additionen på C ger C strukturen av en abelsk grupp, med additiv identitet O, dvs.

(a) O är additiv identitet: $P + O = P$.

(b) För varje P finns en punkt $-P$ sådan att $P + (-P) = O$.

(c) Additionen är kommutativ: $P + Q = Q + P$.

[13] Om $O = P * Q$ menar vi här återigen tangentlinjen.

(d) Additionen är associativ: $(P+Q)+R = P+(Q+R)$.

Definition. C med gruppstrukturen ovan kallas en *elliptisk kurva.*

Anmärkning. Namnet kommer inte från att dessa kurvor är ellipser (de är ju av grad tre) utan från att intresset för dessa kurvor dök upp i studiet av vissa integraler som inte lät sig beräknas med elementära metoder, t.ex. båglängden av en ellips.

Anmärkning. Valet av O är inte så viktigt. Om O' är ett annat val är det lätt att visa att $P \mapsto P + (O' - O)$ en gruppisomorfism från (C, O) till (C, O').

Bevis för (a)-(c) Det underlättar att rita figurer nedan.

(a) $P + O = (P * O) * O = P$. De två linjerna i konstruktionen av + sammanfaller här.

(b) Betrakta $S = O * O$, dvs den andra punkt i vilken tangentlinjen i O skär C. Vi definierar $-P = P * S$, ty då $P * -P = S$ så $(P * -P) * O) = S * O = O$.

(c) Detta är uppenbart. Konstruktionen gör ingen skillnad på P och Q.

Beviset av associativiteten i (d) är mer komplicerat. Vi tar itu med det i nästa avsnitt.

15.2 Bevis av associativiteten i det generiska fallet.

Kom ihåg att att rummet V_3 som består av homogena polynom av grad $d-2$ är av dimension $\binom{d}{2}$. Om graden är 3 är dimensionen alltså $\binom{5}{2} = 10$. Åtta oberoende villkor bör alltså minska dimensionen till $10 - 8 = 2$. Detta är innebörden av följande sats, vars detaljerade bevis vi utelämnar. Kom också ihåg att när vi tänker på polynom istället för kurvor får vi en dimension extra, så motsvarande rum av kurvor är av dimension 1, dvs. det är en enparameterfamilj av kurvor.

Lemma 1. Låt åtta punkter $P_1, ..., P_8$ vara givna. Definiera vektorrummet

$$V_3(P_1, ..., P_8) = \{F \in \mathbb{C}[x, y, z] \mid F \text{ homogent av grad } 3, F(P_i) = 0, i = 1, ..., 8\}.$$

Antag att dessa punkter har följande egenskaper:

(a) Det finns inte fyra av dessa punkter som ligger på samma linje.

(b) Det finns inte sju av dessa punkter som ligger på samma irreducibla andragradskurva.

Då är rummet $V_3(P_1, ..., P_8)$ tvådimensionellt.

Bevis. Premisserna (a) och (b) är till för att garantera att alla punkterna tillför oberoende ekvationer. Det detaljerade beviset använder Bezouts sats, och kan hittas i t.ex. Miles Reid, Undergraduate Algebraic Geometry (som ligger online på författarens hemsida).

Lemma 2. Låt C vara en irreducibel tredjegradskurva och C_1 och C_2 vara två tredjegradskurvor i $\mathbb{C}P^2$. Antag att C_1 och C_2 skär varandra i nio distinkta punkter: $C_1 \cap C_2 = \{P_1, ..., P_9\}$, $P_i \neq P_j$. Antag att C går igenom $P_1, ..., P_8$. Då går C också genom P_9.

Bevis. Låt C ges av $F = 0$, C_1 ges av $F_1 = 0$, och C_2 ges av $F_2 = 0$. Om fyra av $P_1, ..., P_9$ ligger på samma linje L, så måste enligt Bezout, $I(C_i, L) \geq 4$ för $i = 1, 2$, så både C_1 och C_2 innehåller L och deras snitt innehåller då oändligt många punkter. Av samma skäl kan inte sju av punkterna ligga på samma kägelsnitt. Det följer från Lemma 1 att rummet $V_3(P_1, ..., P_8)$ är av dimension 2. Uppenbarligen tillhör F, F_1 och F_2 alla detta rum.

Betrakta

$$U = \{aF_1 + bF_2 | a, b \in \mathbb{C}\}.$$

Detta är ett underrum av dimension 2 till $V_3(P_1, ..., P_8)$, eftersom $(aF_1 + bF_2)(P_i) = 0, i = 1, ..., 8$ och F_1 och F_2 inte är multipler av varandra. Alltså är $U = V_3(P_1, ..., P_8)$ och det finns α, β så att $F = \alpha F_1 + \beta F_2$. Men då ser vi genast att $F(P_9) = \alpha F_1(P_9) + \beta F_2(P_9) = 0$. Detta avslutar beviset av Lemma 2.

Bevis av (d). För att bevisa associativiteten räcker det att visa att punkterna $(P + Q) * R$ och $P * (Q + R)$ är samma punkt. Konstruktionen av dessa från P, Q och R involverar följande åtta punkter: O, P, Q, R, $P*Q$, $Q*R$, $P+Q$, $Q+R$ och sex linjer, tre streckade och tre heldragna, enligt följande figur (ur Silverman/Tate, Rational Points on Elliptic Curves). De streckade linjerna utgör tillsammans en tredjegradskurva C_1 och de heldragna en annan, C_2. *Vi antar först att alla de åtta punkterna ovan är olika.* De två linjerna genom R och $P + Q$, respektive genom P och $Q + R$ skär varandra i en punkt Π. Vi ska visa att $\Pi = (P + Q) * R = P * (Q + R)$.

Vi noterar först att C, C_1 och C_2 alla går igenom de åtta punkterna ovan och att C_1 och C_2 dessutom går igenom Π. Då kommer C att gå igenom Π enligt Lemma 2. Men Π måste då vara $(P + Q) * R$ eftersom $C \cap C_1 \ni (P + Q) * R$. På samma sätt måste $\Pi = P * (Q + R)$. Detta avslutar beviset i det fall att alla de nio punkterna i konstruktionen är olika.

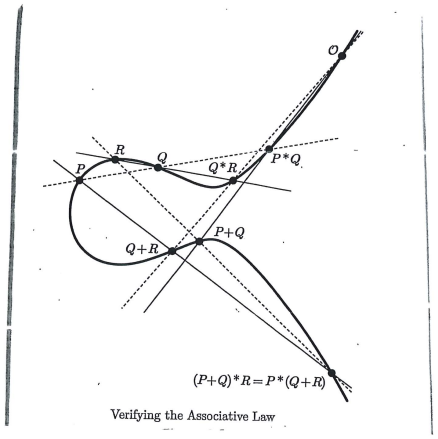
15.3 Topologisk slutkläm på beviset av associativiteten.

För att avsluta argumentet i fallet då vissa av punkterna sammanfaller använder vi följande lemma. Beviset är rättframt för någon som kan lite topologi. (Man kan också göra ett rent algebraiskt argument. Ett sådant bevis skulle inte behöva anta att vi arbetar över $\mathbb{C}$).

Lemma 3.

(a) Avbildningarna $C \times C \to C$ givna av $(P, Q) \mapsto P * Q$ respektive $(P, Q) \mapsto P + Q$ är kontinuerliga.

(b) De två avbildningarna $C \times C \times C \to C$ givna av $(P, Q, R) \mapsto (P + Q) + R$, respektive $(P, Q, R) \mapsto P + (Q + R)$ är kontinuerliga.



Verifying the Associative Law

(c) Mängden av tripler $(P, Q, R) \in C \times C \times C$ sådana att punkterna $P, Q, R, P * Q, R * Q, R + Q, P + Q, O, \Pi$ alla är olika är en tät delmängd av $C \times C \times C$.

Bevis. Detaljerna utelämnas, men idéerna är följande.

(a) Påståendet innebär att små ändringar av P och Q längs C bara kommer att leda till små förändringar i $P + Q$. Det bör vara intuitivt uppenbart att detta är fallet.

(b) Funktionerna är givna av sammansättningar av kontinuerliga avbildningar enligt (a).

(c) Detta påstående innebär att de punkttripplar som är sådana att några av de åtta punkterna sammanfaller, kan approximeras godtyckligt väl med punkttripplar som ger åtta distinkta punkter.

Nu kan vi slutföra beviset av associativiteten. De två avbildningarna i (b) sammanfaller enligt vårt tidigare argument på en tät delmängd av $C \times C \times C$. Eftersom de är kontinuerliga sammanfaller de överallt. Detta avslutar beviset för grupplagen.

15.4 Elliptiska kurvor på normalform.

Om vi arrangerar vår kurva på normalform med hjälp av en projektiv transformation så får additionslagen och inversen en enkel och tillfredsställande geometrisk beskrivning.

Sats. Om $C \subset \mathbb{C}P^2$ är på formen

$$y^2z = x(x-z)(x-\lambda z)$$

skär C linjen $z = 0$ i en unik punkt, som är en inflexionspunkt. Om O väljs som denna punkt, så har grupplagen följande egenskaper.

(a) Inversoperationen $P \to -P$ motsvarar reflektionen $(x, y, z) \mapsto (x, -y, z)$.

(b) $P + Q + R = O$ om och endast om P, Q och R är de tre skärningspunkterna av C med en linje L.

Bevis. Den enda lösningen då $z = 0$ är uppenbarligen $x = 0$, som motsvarar den projektiva punkten $O = (0, 1, 0)$. Enligt Bezout är $I(C, z) = 3$ så $I_{(0,0)}(C, z) = 3$. Detta innebär dels att $z = 0$ är tangentlinjen till C i $O = (0, 1, 0)$ dels att O är en inflexionspunkt. Vi har alltså $O * O = O$ (alla tre skärningarna mellan tangentlinjen i O och C ligger i O). Betrakta kurvan i xy-kartan. O är då den punkt i oändligheten där vertikala linjer skär varandra. Detta innebär att inversoperationen ges av spegling i x-axeln: $P * O * O = P * O = -P$. Det följer att $P + Q = -P * Q$. Så $P + Q + R = 0 \iff P + Q = -R \iff R = P * Q$ och vi är klara.

16 Mer algebra.

16.1 Radikalideal och reducerade ringar.

Definition. *Radikalen* $\sqrt{I}$ till ett ideal I är

$$\sqrt{I} = \{f \in R \,|\, \exists m : f^m \in I\}.$$

Definition. Ett *radikalideal* $I \neq R$ är ett ideal sådant att $\sqrt{I} = I$.

Med andra ord har ett radikalideal egenskapen: Om det finns $m \in \mathbb{N}$ så att $f^m \in I$ så är $f \in I$.

Sats. Varje primideal är ett radikalideal.
Bevis. Direkt från definitionerna.

Exempel.

(i) Radikalen av ett ideal $m\mathbb{Z} \subset \mathbb{Z}$ är $r\mathbb{Z}$, där r är den största kvadratfria faktorn i m. Med andra ord, om m har primtalsfaktoriseringen $m = p_1^{r_1} \cdot ... \cdot p_n^{r_n}$ så är $r = p_1 \cdot ... \cdot p_n$. T.ex. är $6\mathbb{Z}$ radikalt men $4\mathbb{Z}$ är det inte. (Dess radikal är $2\mathbb{Z}$).

(ii) Radikalen av ett ideal $(f(x)) \subset \mathbb{C}[x]$ är på samma sätt $(r(x))$ där $r(x)$ är produkten av de distinkta irreducibla faktorerna i $f(x)$. T.ex. är $\sqrt{(x(x+1)^2)} = (x(x+1))$

(iii) Radikalen av ett huvudideal $(f(x,y)) \subset \mathbb{C}[x,y]$ är på samma sätt som i förra exemplet genererat av det polynom som har samma irreducibla faktorer som f men där alla har multiplicitet 1. T.ex. $\sqrt{(x^2y)} = (xy)$.

De tre exemplen ovan kan ses i ljuset av följande sats. T.ex. (x) och (y) är de primideal som innehåller (x^2y) och $(xy) = (x) \cap (y)$.

Sats. Radikalen $\sqrt{I}$ är snittet av de primideal $\mathfrak{p}$ som innehåller I.

$$\sqrt{I} = \bigcap_{I \subset \mathfrak{p}} \mathfrak{p}.$$

Bevis. $\subseteq$-riktningen är lätt att visa. För $\supseteq$ behöver vi använda Zorns Lemma. Beviset utelämnas.

Kom ihåg att ett element f i en ring R kallas *nilpotent* om någon potens av det är 0.

Sats. I är ett radikalideal $\iff$ R/I saknar nilpotenta nollskilda element.

Bevis. Övning. Det handlar bara om att tolka definitionen i kvotringen.

Definition. En ring som inte har några nollskilda nilpotenter kallas *reducerad*.

Notera att ringen av komplexvärda funktioner på en godtycklig mängd M är reducerad.

Exempel.

(i) $\mathbb{Z}/6\mathbb{Z}$ är reducerad. I $\mathbb{Z}/4\mathbb{Z}$ är dock $2^2 = 0$ så den är inte reducerad.

(b) $\mathbb{C}[x]/(x(x+1))$ är reducerad. Däremot har $\mathbb{C}[x]/(x(x+1)^2)$ nilpotenten $x(x+1)$, eftersom $x^2(x+1)^2 = 0$ i denna ring (men $x(x+1)$ inte är det).

(c) I $\mathbb{C}[x,y]/(x^2y)$ är xy nilpotent, men $\mathbb{C}[x,y]/(xy)$ är reducerad.

17 Algebraiska mängder. Funktioner och avbildningar.

17.1 Algebraiska mängder.

Vi utvidgar studieobjekten något i detta kapitel, främst för att bland dem inkludera enstaka punkter. Vi ger också en orientering till några grundläggande satserna i högre algebraisk ge-

ometri utan bevis.

Definition. Låt $F \subset \mathbb{C}[x_1, ..., x_n]$. Vi skriver

$$V(F) = \{\mathbf{x} = (x_1, ..., x_n) \in \mathbb{C}^n \,|\, \forall f \in F : f(\mathbf{x}) = 0\}.$$

Mängder $V(F)$ av detta slag kallas *algebraiska mängder*.

Faktum. Det är lätt att se att om $I = (F)$ betecknar idealet genererat av elementen i F gäller $V(F) = V(I)$. Detta betyder att algebraiska mängder inte primärt är associerade med mängder av polynom utan snarare med ideal genererade av dessa polynom . En sats av Hilbert[14] säger dessutom att varje ideal I i en polynomring är *ändligt genererat*[15] så faktiskt är varje algebraisk mängd av formen $V(f_1, ..., f_n)$, dvs. algebraiska mängder definieras av *ändliga* ekvationssystem.

Definition. Låt V vara en algebraisk mängd. Vi betecknar med $I(V)$ mängden av alla polynom som är identiskt noll på V:

Det är lätt att se att $I(V)$ är ett ideal. Dessutom är $V = \bigcap_{f \in I(V)} V(f) = V(I(V))$. [16].

Vi har alltså en korrespondens som tillordnar ett ideal $I(V)$ till varje algebraisk mängd V och en algebraisk mängd $V(I)$ till varje ideal I. Denna uppfyller $V(I(V)) = V$ enligt ovan, men i allmänhet är $I(V(I)) \neq I$ som nedanstående exempel i dimension 1 visar.

Exempel. Idealet $I = (x^2) \subset \mathbb{C}[x]$ har $V(I) = \{0\}$ och $I(V(I)) = (x) \neq (x^2)$. Men (x) är radikalen till (x^2). Detta illustrerar den allmänna situationen. Vi har nämligen nedanstående sats som är utgångspunkten för algebraisk geometri i högre dimensioner.

Hilberts Nullstellensatz.[17] Den nämnda korrespondensen ovan ger en bijektion mellan de algebraiska mängderna i $\mathbb{C}^n$ och radikalidealen i $\mathbb{C}[x_1, ..., x_n]$.

Exempel. Irreducibla algebraiska mängder motsvarar under denna korrespondens primideal och enstaka punkter motsvarar sådana primideal som är maximala. I det tvådimensionella fallet betyder detta att en irreducibel algebraisk kurva $f(x, y) = 0$ i $\mathbb{C}^2$ motsvarar sådana primideal som är huvudideal $(f) \subset \mathbb{C}[x, y]$. En enstaka punkt $P = (a, b) \in \mathbb{C}^2$ svarar mot det maximala idealet $\mathfrak{m}_P = ((x - a), (y - b))$. Detta är en uttömmande lista över de nollskilda primidealen i $\mathbb{C}[x, y]$.

[14] Hilberts bassats

[15] Ringar i vilka alla ideal är ändligt genererade kallas Noetherska ringar, efter Emmy Noether (1882-1935).

[16] Beviset av de flesta (inte alla) av påståendena som är utströdda i detta kapitel kan betraktas som övningar (dock överkurs).

[17] David Hilbert (1862-1943)

17.2 Koordinatringen.

Betrakta en affin kurva V definierad av ett irreducibelt polynom $p \in \mathbb{C}[x,y]$. Varje polynom $f \in \mathbb{C}[x,y]$ definierar en funktion på V genom restriktionen

$$f|_V : V \subset \mathbb{C}^2 \to \mathbb{C}.$$

Två polynom f och g definierar samma funktion om och endast om $(f-g)|_V = 0$, dvs. $f - g \in I(V)$. Enligt Hilberts Nullstellensatz är $I(V) = (p)$ så detta betyder att $p|f-g$.

Definition. Kvotringen

$$\mathbb{C}[V] := \mathbb{C}[x,y]/(p)$$

kallas *koordinatringen för* V och kan alltså tänkas som rummet av polynomfunktioner (*reguljära funktioner*) definierade på V.

Notera att om p är irreducibelt är (p) primideal och koordinatringen $\mathbb{C}[V]$ ett integritetsområde. För allmänna algebraiska mängder $V(I) \subset \mathbb{C}^n$ definieras koordinatringen på motsvarande sätt.

Definition. Om I är ett radikalideal $I \subset \mathbb{C}[x_1, ..., x_n]$ som motsvarar $V = V(I)$ är *koordinatringen för* V definierad som

$$\mathbb{C}[V] = \mathbb{C}[x_1, ..., x_n]/I.$$

Om f är reducibelt är inte koordinatringen ett integritetsområde. Se exemplet (iv) nedan.

Exempel. Vi använder Noethers isomorfisats för att beräkna några koordinatringar nedan.

(i) Koordinatringen på x-axeln $y = 0$ är

$$\mathbb{C}[x,y]/(y) \cong \mathbb{C}[x].$$

Definiera nämligen en surjektiv ringhomomorfi $\phi : \mathbb{C}[x,y] \to \mathbb{C}[x]$ genom $\phi(1) = 1, \phi(x) = x$, $\phi(y) = 0$. Kärnan $\ker \phi = (y)$, så ϕ inducerar den angivna isomorfin. Detta verkar rimligt, eftersom ringen av polynomfunktioner på $\mathbb{C}$ bör vara $\mathbb{C}[x]$.

(ii) Koordinatringen för linjen $y = x$ är

$$\mathbb{C}[x,y]/(y-x) \cong \mathbb{C}[x],$$

isomorfin här är här inducerad av $\phi : \mathbb{C}[x,y] \to \mathbb{C}[x]$, given av $\phi(1) = 1, \phi(x) = x, \phi(y) = x$. Kärnan $\ker \phi = (x-y)$ eftersom $p(x,y) \in \ker \phi \iff p(x,x) = 0 \iff (y-x)|p(x,y)$. Detta är väl också rimligt - linje som linje.

(iii) Detta exempel generaliserar de två ovan. Koordinatringen för en polynomgraf

$$\mathbb{C}[x,y]/(y - p(x)) \cong \mathbb{C}[x],$$

isomorfin här ges av $\phi(1) = 1, \phi(x) = x$, $\phi(y) = p(x)$. Att $f(x,y)$ ligger i $\ker(\phi)$ här är detsamma som att $f(x,p(x)) = 0$ dvs. $y - f(x)$ delar $f(x,y)$.

(iv) Koordinatringen för en disjunkt union V av n punkter $(a_1, b_1), ..., (a_n, b_n)$ är isomorf med $\mathbb{C}^n$ (produkt och addition i varje lucka separat). Betrakta ringhomomorfismen

$$\phi : \mathbb{C}[x, y] \to \mathbb{C}^n,$$

som ges av $\phi(f) = (f(a_1, b_1), ..., f(a_n, b_n))$. Den är surjektiv och har $\ker \phi = (x - a_1, y - b_1) \cap ... \cap (x - a_n, y - b_n) = I(V)$. Alltså är $\mathbb{C}[V]/I(V) = \mathbb{C}^n$. Med andra ord, en funktion på n st punkter bestäms av n st tal - funktionens värden i punkterna. Notera att $(1, 0, 0...0)(0, 1, 0...0) = (0, 0, ..., 0)$ så den här ringen har nolldelare om $n \geq 2$.

Vi noterar att alla de ovanstående ringarna är reducerade och att alla utom den sista är integritetsområden.

Anmärkning. Detta ger ett annat sätt att tala om Hilberts nollställessats: Algebraiska mängder är i bijektion med ändligt genererade reducerade $\mathbb{C}$-algebror. Det är mycket mer än en bijektion, det är en ekvivalens av kategorier. Det här är ett exempel på en viktig princip i modern matematik: Geometriska objekt kan ofta alternativt beskrivas med sina funktionsrum, som är av mer algebraisk natur.

Nedan är ett exempel på en $\mathbb{C}$-algebra som *inte* är reducerad och som alltså inte är koordinatring till någon algebraisk mängd, men som ändå kommer att vara mycket viktig för oss.

Exempel. $R = \mathbb{C}[x]/(x^2)$. I denna ring är x nilpotent, ty $x^2 = 0$. Eftersom (x^2) inte är ett radikalideal är R inte koordinatring till någon algebraisk mängd, men vi kommer att se att den ändå dyker upp som behållare för geometrisk information nedan.

17.3 Rationella funktioner

Definition. Låt $R = \mathbb{C}[x_1, ..., x_n]$. Som vi redan diskuterat i tidigare avsnitt, kallas ett element av $Q(R)$ en *rationell funktion.* Vi använder beteckningen $\mathbb{C}(x_1, ..., x_n)$ för mängden av alla sådana.

Om V är en irreducibel algebraisk mängd är $I(V)$ ett primideal i $\mathbb{C}[x, y]$ genererat av ett irreducibelt polynom $p(x, y)$ och ringen $\mathbb{C}[V] = \mathbb{C}[x, y]/(p(x, y))$ är alltså ett integritetsområde. Således har den en fraktionskropp.

Definition. Fraktionskroppen $Q(\mathbb{C}[V])$ betecknar vi $\mathbb{C}(V)$ och kallar för *funktionskroppen* till V. Elementen i $\mathbb{C}(V)$ kallar vi *rationella funktioner* (notera dock att de vanligen endast är partiellt definierade funktioner - nämnaren kan vara 0).

Notera att olika representanter för en rationell funktion kan ha olika definitionsområden. Om $\mathbb{C}[V]$ är en faktoriell ring (t.ex. om $V = \mathbb{C}^n$), så kan vi använda ett maximalt förkortat bråk som kanonisk representant, men normalt har vi inte sådan tur.

Definition. En rationell funktion $F \in \mathbb{C}(V)$ sägs vara *reguljär i* P om den har en representant f/g där $g(P) \neq 0$.

Övning. Om en rationell funktion är reguljär i P har den ett väldefinierat värde $f(P)/g(P) \in \mathbb{C}$ där.

Sats. Om en rationell funktion är reguljär i alla punkter på V är den en reguljär funktion.

Bevis. Utelämnas här. Se senare kurser i algebraisk geometri.

17.4 Reguljära avbildningar

Koordinatringen ger oss alltså en ring av polynomfunktioner på vår kurva. Vi kan också definiera *reguljära (polynomiella) avbildningar* mer allmänt som sådana som har komponenter som är polynomfunktioner.

Definition. En reguljär avbildning $f : V \to \mathbb{C}^n$ är en avbildning sådan att den kan beskrivas med komponenter $(f_1, ...f_n)$ där $f_1, ..., f_n \in \mathbb{C}[V]$.

Exempel:

(i) Låt $p(t)$ vara ett polynom. Avbildningen $f : \mathbb{C} \to \mathbb{C}^2$, given av $f(t) = (t, p(t))$ är en reguljär avbildning vars bild är grafen Γ till p. Projektionen på x-axeln definierar en reguljär invers $g : \Gamma \to \mathbb{C}$, $g(x, y) = x$. Vi säger då att Γ är *isomorf* med $\mathbb{C}$.

(ii) Avbildningen $f : \mathbb{C} \to \mathbb{C}^2$, given av $f(t) = (t^2, t^3)$ är en reguljär avbildning vars bild är den singulära tredjegradskurvan $y^2 = x^3$. Avbildningen $g(x, y) = y/x$ är dess invers, men den är inte reguljär i $(0, 0)$, så den givna avbildningen är inte en isomorfi (det finns ingen sådan isomorfi).

(iii) Affina avbildningar ges av polynom och är därför reguljära.

17.5 Rationella avbildningar

Definition. En rationell avbildning $f : V \to \mathbb{C}^n$ är en (partiellt definierad) avbildning som kan beskrivas med komponenter $(f_1, ...f_n)$ där $f_1, ..., f_n \in \mathbb{C}(V)$. Vi kallar f *reguljär* i $\mathbf{x}$ om alla f_i är reguljära i $\mathbf{x}$. Bilden $f(V)$ av V under f är bilden av mängden av alla punkter där f är reguljär.

Exempel.

(i) Låt $V = \{(x, y) \in \mathbb{C}^2 \mid x^2 + y^2 = 1\}$. Avbildningen $f : \mathbb{C} \to \mathbb{C}^2$ given av

$$f(t) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right)$$

är en rationell avbildning som är definierad för alla $t \neq \pm i$ och vars bild är $V \setminus \{(-1, 0)\}$. Denna avbildning ges geometriskt av konstruktionen i nedanstående figur. En linje genom $(-1, 0)$ med vinkel $\theta/2$ mot x-axeln skär y-axeln i t och V i $f(t)$.

(ii) Avbildningen $g : \mathbb{C}^2 \to \mathbb{C}$ given av $g(x, y) = y/x$ är en rationell avbildning. Låt V beteckna kurvan $V = \{y^2 = x^3\}$. Då är g definierad på $V \setminus \{(0, 0)\}$ och ger där en invers till $f : \mathbb{C} \setminus \{0\} \to V \setminus \{(0, 0)\}$, given av $t \mapsto (t^2, t^3)$. Vi säger att $\mathbb{C}$ och V är *birationellt ekvivalenta*[18].

(iii) De två ovanstående exemplen är mer generella än de ser ut. Alla kägelsnitt och singulära tredjegradskurvor kan parametriseras med rationella funktioner på detta sätt. De är alltså birationellt ekvivalenta med $\mathbb{C}$. Sådana kurvor kallas *rationella kurvor*.

(iv) Avbildningen

$$F : \mathbb{C}^2 \to \mathbb{C}^2,$$

given av

$$F(x, y) = (\frac{ax + by + c}{gx + hy + k}, \frac{dx + ey + f}{gx + hy + k}),$$

är en rationell avbildning. Den är framställningen av en allmän projektiv transformation i xy-kartan (Kolla detta!). Med andra ord, projektiva transformationer ges av rationella avbildningar i de affina kartorna.

18 Lokalisering.

18.1 Fraktionskroppar.

Fraktionskroppen $Q(R)$ till ett integritetsområde R är vad vi får om vi tillåter alla nollskilda element i R att ha en invers. Den konstrueras på samma sätt oavsett vilket R vi börjar med, och ni bör känna igen konstruktionen från specialfallet $\mathbb{Z} \subset \mathbb{Q}$.

Definition. Låt R vara ett integritetsområde. Vi definierar *fraktionskroppen Q(R)* genom följande konstruktion. Introducera följande relation på $R \times (R \setminus \{0\})$:

$$(p, q) \sim (r, s) \iff ps = qr.$$

Att visa att detta är en ekvivalensrelation är rättframt. Vi definierar

$$Q(R) = R \times (R \setminus \{0\})/\sim .$$

Ekvivalensklassen till (a, b) betecknar vi med $\frac{a}{b}$. Dessa bråk kan då adderas och multipliceras som 'förväntat', dvs.

$$\frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs} \quad \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs},$$

och detta gör $Q(R)$ till en kropp.

Exempel:

[18]En rationell avbildning $f : X \to Y$ är en *birationell ekvivalens* om $f(X)$ är tät i Y och det finns en rationell avbildning $g : Y \to X$ sådan att $f(Y)$ är tät i X och g och f är inverser överallt där sammansättningen av dem är väldefinierad. Detta kommer inte att vara en central del av denna kurs dock. Man kan visa att birationella avbildningar $X \to Y$ är i ett-ett-korrespondens med isomorfier mellan kropparna $k(Y) \to k(X)$.

(i) Heltalen $\mathbb{Z}$ är ett integritetsområde. Konstruktionen ovan ger $Q(\mathbb{Z}) = \mathbb{Q}$.

(ii) En polynomring över en kropp $k[x]$ är ett integritetsområde. Konstruktionen ovan ger kroppen av rationella funktioner $Q(k[x]) = k(x)$. Ett element i denna är en kvot av polynom $\frac{p(x)}{q(x)}$ och en annan sådan kvot $\frac{r(x)}{s(x)}$ motsvarar samma element i $k(x)$ om $p(x)s(x) = r(x)q(x)$. Till exempel är $\frac{(x-1)}{x^2} = \frac{(x-1)^2}{x^3-x^2}$. Notera att element i $k(x)$ inte riktigt är funktioner, eftersom de inte är definierade för alla x. (Dessutom kan olika representanter av samma ekvivalensklass ha olika definitionsområden. I exemplet ovan är det ena bråket definierat i $x = 1$ medan det andra inte är det.)

(iii) I $\mathbb{C}[x, y]$ kan vi förstås bilda ringen av rationella funktioner $\mathbb{C}(x, y)$ med samma konstruktion som i (*ii*). Här kan de rationella funktionerna vara odefinierade längs hela kurvor (nollställen till nämnaren).

Sats. Den naturliga avbildningen $R \to Q(R)$ given av $p \mapsto \frac{p}{1}$ är en injektiv ringhomomorfi, dvs. vi kan betrakta R som en delring av $Q(R)$.

Anmärkning. I de välbekanta fallen har vi $\mathbb{Z} \subset \mathbb{Q}$, $k[x] \subset k(x)$ och $\mathbb{C}[x, y] \subset \mathbb{C}(x, y)$.

18.2 Lokalisering av integritetsområde.

Konstruktioner som ger oss fraktionskroppen för ett integritetsområde $Q(R)$ kan generaliseras. Istället för att ta våra nämnare ur $R \setminus \{0\}$ kan vi ta dem ur vilken s.k. multiplikativ mängd som helst.

Definition. $S \subset R$ kallas en *multiplikativ mängd* om $1 \in S$ och S är sluten under multiplikation.

Definition. Låt R vara ett integritetsområde. Lokaliseringen av R med avseende på S är

$$S^{-1}R = (R \times S)/\sim,$$

där $(x, s) \sim (y, t) \iff xt - ys = 0$. (x, s) betecknas $\frac{x}{s}$.

Vi kommer nedan att generalisera denna definition till allmänna ringar R, men fallet då R saknar nolldelare är ett viktigt specialfall och konstruktionen är då är helt och hållet parallell med konstruktionen av fraktionskroppar (som ni är bekanta med).

Sats. Låt R vara ett integritetsområde och $S \subseteq R$ en multiplikativ mängd som inte innehåller 0.

(a) $S^{-1}R$ är ett integritetsområde, med addition och multiplikation definierade på samma sätt som i fraktionskroppen.

(b) Funktionen $R \to S^{-1}R$ given av $r \mapsto r/1$ är en injektiv ringhomomorfi.

Bevisskiss. Att addition och multiplikation fungerar som de ska är exakt samma bevis som i fraktionskroppen. Eftersom $R \times S \subset R \times (R \setminus \{0\})$ och ekvivalensrelationerna som bildar $S^{-1}R$ resp. $Q(R)$ är desamma, är det klart att $S^{-1}R$ är kanoniskt isomorf med delringen

$$S^{-1}R \cong \{f \in Q(R) \mid f \text{ har en representant } p/q \text{ där } q \in S\} \subset Q(R).$$

Notation. Det viktigaste exemplet är när $\mathfrak{p} \subset R$ är ett primideal och $S = R \setminus \mathfrak{p}$[19]. Då kallas även $S^{-1}R$ *lokaliseringen i* $\mathfrak{p}$ och betecknas

$$R_{\mathfrak{p}} = S^{-1}R.$$

Notation. Det näst viktigaste exemplet är när $f \in R$ och $S = \{1, f, f^2 ...\}$. Då skriver vi

$$R_f = S^{-1}R.$$

Exempel.

(i) Om $R = \mathbb{Z}$ och $\mathfrak{p} = (3)$ så är lokaliseringen

$$\mathbb{Z}_{\mathfrak{p}} \cong \{p/q \in \mathbb{Q} \mid 3 \not| \, q\} \subset \mathbb{Q}$$

(ii) Om $R = \mathbb{Z}$ och $S = \{1, 3, 3^2, 3^3, ...\}$ så är lokaliseringen

$$\mathbb{Z}_3 \cong \{p/q \in \mathbb{Q} \mid \exists m \in \mathbb{N} : q = 3^m\} \subset \mathbb{Q}.$$

(ii) Om $R = \mathbb{C}[x]$ och primidealet det maximala idealet $\mathfrak{m} = (x)$ är

$$\mathbb{C}[x]_{(x)} \cong \{p/q \in \mathbb{C}(x) \mid x \not| \, q\} = \{p/q \in \mathbb{C}(x) \mid q(0) \neq 0\} \subset \mathbb{C}(x).$$

(iii) Om $R = \mathbb{C}[x, y]$ och primidealet det maximala idealet $\mathfrak{m} = (x - a, y - b)$ är

$$\mathbb{C}[x, y]_{\mathfrak{m}} \cong \{p/q \in \mathbb{C}(x, y) \mid q(a, b) \neq 0\} \subset \mathbb{C}(x, y).$$

(iv) Om $R = \mathbb{C}[x, y]$ och primidealet huvudidealet $\mathfrak{p} = (f)$ för ett irreducibelt polynom f är

$$\mathbb{C}[x, y]_{\mathfrak{p}} = \mathbb{C}[x, y]_{(f)} = \{p/q \in \mathbb{C}(x, y) \mid f \not| \, q\} \subset \mathbb{C}(x, y).$$

Definition. *Den lokala ringen i en punkt* $P = (a, b)$, $\mathcal{O}_P$, är lokaliseringen av $\mathbb{C}[x, y]$ till det maximala idealet $\mathfrak{m}_P = (x - a, y - b)$ som motsvarar P:

$$\mathcal{O}_P = \mathbb{C}[x, y]_{\mathfrak{m}_P}$$

$\mathcal{O}_P$ innehåller alltså inverser till alla element som inte är 0 i P och vi kan tänka på $\mathcal{O}_P \subset \mathbb{C}(x, y)$ som de rationella funktioner som är reguljära i P.

[19] Notera att definitionen av ett primideal säger precis att dess komplement är en multiplikativ mängd.

Exempel. Let $O = (0,0) \in \mathbb{C}^2$. $\mathcal{O}_O \subset \mathbb{C}(x,y)$ består av de rationella funktioner som kan skrivas f/g där g har icke-försvinnande konstantterm.

Anmärkning. Termen "lokalisering" kan förklaras på följande sätt. I en polynomring R är bara de nollskilda konstanterna inverterbara. Vi kan bara tvångsinvertera icke-konstanta polynom till priset av att resultatet (en rationell funktion) har diverse singulariteter. Då vi bildar fraktionskroppen av rationella funktioner struntar vi i denna kostnad. Men om vi bara är intresserade av geometri *lokalt*, säg i närheten av en speciell punkt P, så kan vi göra något mer sofistikerat. Polynom som inte är noll i P (dvs. ligger utanför motsvarande maximala ideal $\mathfrak{m}$) är då "kostnadsfria" att invertera (alla eventuella problem dyker upp långt bort från P och vi bryr oss inte om det). De rationella funktioner som vi får genom att invertera sådana polynom utgör lokaliseringen $R_{\mathfrak{m}}$.

Mer allmänt, om $V = V(\mathfrak{p})$ är en irreducibel algebraisk mängd så är de rationella funktioner vi får genom att invertera alla polynom som inte är noll på V lokaliseringen $R_{\mathfrak{p}}$. I den här kursen kommer vi dock bara att behöva lokalisera i punkter, dvs. i maximala ideal.

18.3 Lokalisering i allmänna fallet.

Noga taget fungerar definitionen av lokalisering som vi gav den i förra avsnittet så länge S inte innehåller nolldelare (R behöver inte vara ett integritetsområde.) Men om S innehåller nolldelare måste vi definiera lokaliseringen på följande sätt istället. Detta kommer inte att användas på något essentiellt sätt senare, men vi inkluderar det här för fullständighetens skull och för att det är viktigt i allmänhet. I detta avsnitt placerar jag också några ytterligare satser om lokalisering av ringar.

Definition. Låt R vara en ring. Lokaliseringen av R med avseende på S är

$$S^{-1}R = (R \times S)/\sim,$$

där $(x,s) \sim (y,t) \iff$ Det finns $u \in S : u(xt - ys) = 0$. Vi betecknar (x,s) med $\dfrac{x}{s}$.

Följande sats visar att definitionen ovan inte är nonsens.

Sats.

(a) $\sim$ är en ekvivalensrelation.

(b) $S^{-1}R$ är en ring och addition och multiplikation definieras som i fraktionskroppar.

(c) Den naturliga avbildningen $R \to S^{-1}R$ given av $r \mapsto \dfrac{r}{1}$ är en ringhomomorfi.

Bevis.

(a) Att $\sim$ är reflexiv och symmetrisk är uppenbart. Transitiviteten behöver bevis, som är standard: Låt $(x,s) \sim (y,t)$ så att $u(xt - ys) = 0$ och $(y,t) \sim (z,r)$ så att $v(yr - tz) = 0$.

Vi behöver visa att $(x,s) \sim (z,r)$. Multiplicera $u(xt-ys) = 0$ med rv. Vi får $urv(xt-ys) = 0 \iff urvxt - us(yrv) = 0 \iff urvxt - us(vtz) = 0 \iff uvt(xr - sz) = 0$. Eftersom $uvt \in S$ är $(x,s) \sim (z,r)$.

(b) Vi definierar summa och produkt på samma sätt som i fraktionskroppar. Det är rättframt att kolla att detta ger väldefinierade ringoperationer på $S^{-1}R$. Vi lämnar detta som övning.

(c) Detta påstående är också rättframt att kolla. (Till skillnad från i fallet utan nolldelare så kan vi dock inte garantera att avbildningen är injektiv.)

Sats. Låt R, R' vara ringar och $S \subset R$ en multiplikativ mängd. Om $f : R \to R'$ är en ringhomomorfi sådan att $f(S)$ består av inverterbara element i R' så är avbildningen $\tilde{f} : S^{-1}(R) \to R'$ given av $\tilde{f}\left(\frac{r}{s}\right) = \frac{f(r)}{f(s)}$ en ringhomomorfi.

Anmärkning. Om $\iota : R \to S^{-1}R$ är den kanoniska avbildningen $r \mapsto \frac{r}{1}$ så är alltså $\tilde{f} \circ \iota = f$. $\tilde{f}$ är då den enda ringhomomorfin med denna egenskap.

Bevis. Utelämnas, men det finns bara ett sätt att definiera $\tilde{f}$ så det är bara en fråga om att verifiera att den så definierade avbildningen har de önskade egenskaperna.

Om $I \subset R$ är ett ideal och $S \subset R$ är en multiplikativ mängd är

$$S^{-1}I = \{i/s \in S^{-1}R \,|\, i \in I,\, s \in S\}$$

ett ideal i $S^{-1}R$. Låt $\bar{S}$ vara bilden av S under den kanoniska homomorfin $R \to R/I$.

Sats. Avbildningen $\kappa : S^{-1}R/S^{-1}I \to \bar{S}^{-1}(R/I)$, given av

$$\kappa\left(\frac{r}{s} + S^{-1}I\right) = \frac{r+I}{s+I}$$

är en ringisomorfi.

Bevis. Utgå från sammansättningen av de kanoniska avbildningarna

$$k : R \to R/I \to \bar{S}^{-1}(R/I)\,.$$

Bilden av S är $\bar{S}$ så den innehåller bara inverterbara element. Därför ger den förra satsen en utvidgning till

$$\tilde{k} : S^{-1}R \to \bar{S}^{-1}(R/I)\,,$$

och om man bara följer definitionen så ser man

$$\tilde{k}\left(\frac{r}{s}\right) = \frac{r+I}{s+I}.$$

Det är uppenbarligen en surjektiv avbildning. Det är lätt att se att kärnan uppfyller $\ker \tilde{k} \supset S^{-1}I$, men eftersom också

$$\frac{r+I}{s+I} = 0 \iff \exists t + I \in \bar{S} : (t+I)(r+I) = 0 \in R/I \iff \exists t \in S : tr \in I \subset R.$$

Detta betyder att $\frac{r}{s} = \frac{tr}{ts} \in S^{-1}I$. Satsen följer nu från Noethers isomorfisats.

Exempel. I detta exempel undersöker vi effekten av lokalisering på en enkel koordinatring, nämligen koordinatringen för två punkter $V = \{\pm 1\}$ i $\mathbb{C}$, kvotringen $\mathbb{C}[V] = \mathbb{C}[x]/(x^2-1) \cong \mathbb{C}^2$. Den ena faktorn $\mathbb{C} \times \{0\}$ svarar mot funktionsvärdet i -1 och den andra $\{0\} \times \mathbb{C}$ mot funktionsvärdet i $+1$.) Vi genomför samma räkning på två sätt för att illustrera satsen ovan, och visar:

$$\mathbb{C}[x]_{(x+1)}/(x^2-1)_{(x+1)} \cong \mathbb{C} \cong (\mathbb{C}[x]/(x^2-1))_{(x+1)}.$$

Vänsterledet: Här lokaliserar vi först polynomringen i idealet $(x+1)$ och får ringen $\mathbb{C}[x]_{(x+1)}$. Ett element i $\mathbb{C}[x]_{(x+1)}$ kan skrivas som en rationell funktion

$$\frac{a_0 + a_1(x+1) + a_2(x+1)^2 + ... + a_n(x+1)^n}{b_0 + b_1(x+1) + b_2(x+1)^2 + ... + b_m(x+1)^m},$$

där $b_0 \neq 0$. Idealet (x^2-1) blir efter lokalisering $(x^2-1)_{(x+1)} = ((x+1)(x-1))_{(x+1)} = (x+1)_{(x+1)}$ eftersom $x-1$ nu är inverterbart. I kvotringen modulo $(x+1)_{(x+1)}$ är ovanstående rationella funkton ekvivalent med $a_0/b_0 \in \mathbb{C}$ eftersom $(x+1)$ är en faktor i

$$b_0(a_0 + a_1(x+1) + a_2(x+1)^2 + ...a_n(x+1^n)) - a_0(b_0 + b_1(x+1) + b_2(x+1)^2 + ... + b_m(x+1)^m).$$

Det följer att

$$\mathbb{C}[x]_{(x+1)}/(x+1)_{(x+1)} \cong \mathbb{C}.$$

Högerledet: Vi kan också lokalisera koordinatringen för två punkter i $\mathbb{C}$ direkt, dvs. bilda

$$\left(\mathbb{C}[x]/(x^2-1)\right)_{(x+1)}.$$

Notera att här är ringen som ska lokaliseras inte ett integritetsområde. Om vi för läsbarhetens skull betecknar idealet (x^2-1) med J kan vi skriva ett allmänt element i denna ring som:

$$\frac{a_0 + a_1(x+1) + a_2(x+1)^2 + ... + a_n(x+1)^n + J}{b_0 + b_1(x+1) + b_2(x+1)^2 + ... + b_m(x+1)^m + J},$$

där $b_0 \neq 0$. Men detta är ekvivalent med a_0/b_0 eftersom $x - 1 \notin (x+1)$ och

$$(x-1)(b_0(a_0 + a_1(x+1) + ... + J) - a_0(b_0 + b_1(x+1) + ... + J) = 0.$$

Detta visar att

$$(\mathbb{C}[x]/(x^2-1))_{(x+1)} \cong \mathbb{C}.$$

18.4 Lite närmare skärningstalet.

Exempel. De två polynomen $f(x,y) = y - x^2 + 1$ och $g(x,y) = y$ definierar den algebraiska mängden $V \subset \mathbb{C}^2$ som består av punkterna $(0,1)$ och $(0,-1)$. Idealet som genereras av f och g är ett radikalideal och koordinatringen är

$$\mathbb{C}[V] = \mathbb{C}[x,y]/(y - x^2 + 1, y) \cong \mathbb{C}[x]/(x^2 - 1) \cong \mathbb{C}^2.$$

Samma resultat får vi om $f(x,y)$ ersätts med $f_\epsilon(x,y) = y - x^2 + \epsilon$, $\epsilon \neq 0$.

$$\mathbb{C}[V_\epsilon] = \mathbb{C}[x,y]/(y - x^2 + \epsilon, y) \cong \mathbb{C}[x]/(x^2 - \epsilon) \cong \mathbb{C}^2.$$

Exempel. Om vi i ovanstående exempel sätter $\epsilon = 0$ får vi V_0 givet av de två polynomen $f(x,y) = y - x^2$ och $g(x,y) = y$. Det ideal som genereras av f och g är här inte ett radikalideal: $(f,g) = (y - x^2, y) = (y, x^2)$ och $\sqrt{(f,g)} = (x,y)$. Motsvarande algebraiska mängd är $V_0 = \{(0,0)\}$. Koordinatringen är alltså

$$\mathbb{C}[V_0] = \mathbb{C}[x,y]/(x,y) \cong \mathbb{C}.$$

Vi har alltså följande diskontinuerliga beteende:

$$\lim_{\epsilon \to 0} \dim_{\mathbb{C}} \mathbb{C}[V_\epsilon] = 2 \neq 1 = \dim_{\mathbb{C}} \mathbb{C}[V_0].$$

Nu observerar vi att om vi istället i högerledet betraktar kvotringen med det (icke-radikala) idealet (f_0, g) får vi

$$\mathbb{C}[x,y]/(f_0, g) = \mathbb{C}[x,y]/(y - x^2, y) \cong \mathbb{C}[x]/(x^2) \cong \mathbb{C}^2.$$

Vi har alltså det behagligare beteendet

$$\lim_{\epsilon \to 0} \dim_{\mathbb{C}}(\mathbb{C}[x,y]/(f_\epsilon, g)) = 2 = \dim_{\mathbb{C}}(\mathbb{C}[x,y]/(f_0, g)).$$

Från synvinkeln att skärningspunkten mellan f och g bara är en punkt utan någon relation till de två kurvorna f och g är det lämpligt att tänka på koordinatringen som det algebraiska objekt som naturligt motsvarar den. Men f och g innehåller mer information. Punkten i sig (radikalen till idealet) kan förstås inte säga någonting intressant om *hur* f och g skär varandra. Men idealet (f,g) kan!

Vi kan få mer detaljerad information om vi lokaliserar i de olika skärningspunkterna. Låt oss t.ex. visa att

$$\mathbb{C}[x,y]_{\mathfrak{m}_{(\sqrt{\epsilon},0)}}/(f_\epsilon, g)) \cong \mathbb{C},$$

om $\epsilon \neq 0$. Här är $f_\epsilon = y - x^2 + \epsilon$ och $\mathfrak{m}_{(\sqrt{\epsilon},0)} = (x - \sqrt{\epsilon}, y)$. Vi kan börja med att notera att $(f_\epsilon, g) = (y - x^2 + \epsilon, y) = (x^2 - \epsilon, y) = (x - \sqrt{\epsilon}, y)$, där den sista likheten är för att $x + \sqrt{\epsilon}$ är

inverterbart i lokala ringen.

Betrakta ett allmänt element $\frac{p(x,y)}{q(x,y)}$ i $\mathbb{C}[x,y]_{\mathfrak{m}_{(\sqrt{\epsilon},0)}}$. Om täljare och nämnare Taylorutvecklas i variablerna $x-\sqrt{\epsilon}$ och y får vi

$$\frac{p(x,y)}{q(x,y)} = \frac{p(\sqrt{\epsilon},0)+(x-\sqrt{\epsilon})A(x,y)+yB(x,y)}{q(\sqrt{\epsilon},0)+(x-\sqrt{\epsilon})C(x,y)+yD(x,y)},$$

där $q(\sqrt{\epsilon},0)\neq 0$. Vi påstår nu att $\frac{p(x,y)}{q(x,y)} = \frac{p(\sqrt{\epsilon},0)}{q(\sqrt{\epsilon},0)}$ i kvotringen $\mathbb{C}[x,y]_{\mathfrak{m}_{(\sqrt{\epsilon},0)}}/(f_\epsilon,g))$. Vi undersöker

$$\frac{p(\sqrt{\epsilon},0)+(x-\sqrt{\epsilon})A(x,y)+yB(x,y)}{q(\sqrt{\epsilon},0)+(x-\sqrt{\epsilon})C(x,y)+yD(x,y)} - \frac{p(\sqrt{\epsilon},0)}{q(\sqrt{\epsilon},0)} =$$

$$= \frac{q(\sqrt{\epsilon},0)p(\sqrt{\epsilon},0)+(x-\sqrt{\epsilon})E(x,y)+yF(x,y)-p(\sqrt{\epsilon},0)q(\sqrt{\epsilon},0)}{q(\sqrt{\epsilon},0)(q(\sqrt{\epsilon},0)+(x-\sqrt{\epsilon})C(x,y)+yD(x,y))} =$$

$$= \frac{(x-\sqrt{\epsilon})E(x,y)+yF(x,y)}{q(\sqrt{\epsilon},0)(q(\sqrt{\epsilon},0)+(x-\sqrt{\epsilon})C(x,y)+yD(x,y))} \in (x-\sqrt{\epsilon},y).$$

Det följer att varje element är ekvivalent med ett komplext tal så

$$\mathbb{C}[x,y]_{\mathfrak{m}_{(\sqrt{\epsilon},0)}}/(f_\epsilon,g)) \cong \mathbb{C}.$$

Med hjälp av ovanstående ser vi att

$$\dim_{\mathbb{C}}(\mathbb{C}[x,y]/(f_\epsilon,g)) = \dim_{\mathbb{C}}(\mathbb{C}[x,y]_{\mathfrak{m}_{(\sqrt{\epsilon},0)}}/(f_\epsilon,g)) + \dim_{\mathbb{C}}(\mathbb{C}[x,y]_{\mathfrak{m}_{(-\sqrt{\epsilon},0)}}/(f_\epsilon,g)) = 1+1 = 2.$$

Liknande räkning visar också att

$$\mathbb{C}[x,y]_{\mathfrak{m}_{(0,0)}}/(y-x^2,y) \cong \mathbb{C}^2.$$

Exempel. Betrakta kurvorna $f = y-x^2(x-1)$ och $f=0$. Det är lätt att se att

$$\mathbb{C}[x,y]_{\mathfrak{m}_{(0,0)}}/(y-x^2(x-1),y)) = \mathbb{C}[x,y]_{\mathfrak{m}_{(0,0)}}/(x^2(x-1),y) = \mathbb{C}[x,y]_{\mathfrak{m}_{(0,0)}}/(x^2,y),$$

där den sista likheten är för att lokalisering i $(x,y)=(0,0)$ gör $x-1$ inverterbart.

Ett allmänt element i $\mathbb{C}[x,y]_{\mathfrak{m}_{(0,0)}}$ kan skrivas

$$\frac{p(x,y)}{q(x,y)} = \frac{a_0+a_1x+x^2B(x,y)+yC(x,y)}{b_0+b_1x+x^2D(x,y)+yE(x,y)},$$

där $b_0\neq 0$. Det är inte svårt att bestämma c_0 och c_1 så att $\frac{p(x,y)}{q(x,y)} = c_0+c_1x$ modulo (x^2,y). (Gör det. Facit i fotnoten.[20]) Detta visar att

$$\mathbb{C}[x,y]_{\mathfrak{m}_{(0,0)}}/(y-x^2(x-1),y)) \cong \mathbb{C}^2.$$

[20] $c_0 = \frac{a_0}{b_0}$ och $c_1 = \frac{a_1b_0-a_0b_1}{{b_0}^2}$.

Man kan också lätt visa att

$$\mathbb{C}[x,y]_{\mathfrak{m}_{(1,0)}}/(y-x^2(x-1),y)) \cong \mathbb{C}.$$

Vi har alltså även här

$$\mathbb{C}[x,y]_{\mathfrak{m}_{(1,0)}}/(y-x^2(x-1),y)) \oplus \mathbb{C}[x,y]_{\mathfrak{m}_{(0,0)}}/(y-x^2(x-1),y)) = \mathbb{C}[x,y]/(y-x^2(x-1),y)).$$

Man kan mer allmänt visa följande sats.

Sats. Låt $I \subset \mathbb{C}[x,y]$ vara ett ideal sådant att $V(I)$ har ändligt många punkter $P_1,...,P_n$. Då gäller

$$\mathbb{C}[x,y]/I = \bigoplus_{i=1}^{n} O_{P_i}/IO_{P_i}.$$

Allt det ovanstående ger oss ledtrådar till hur vi ska definiera skärningsmultipliciteten.

19 Ett par saker till från linjär algebra.

19.1 Direkt summa.

Definition. Om U och W är delrum av V sådana att varje $v \in V$ kan skrivas $v = u + w$ för $u \in U$ och $v \in W$ och dessutom $U \cap W = \{0\}$ kallas V *den direkta summan* av U och W.

Exempel.

Exempel.

19.2 Exakta följder.

Definition. En följd av linjära rum och linjära avbildningar

$$V_0 \xrightarrow{f} V_1 \xrightarrow{g} V_2,$$

kallas *exakt vid* V_1 om $\ker g = \mathrm{im} f$.

Exempel.

$$V_0 \xrightarrow{f} V_1 \to 0^{21}$$

är exakt vid $V_1 \iff f$ är surjektiv.

Exempel.

$$0 \to V_1 \xrightarrow{f} V_2$$

[21] Här betecknar 0 nollvektorrummet och den omärkta pilen den enda möjliga linjära avbildningen.

är exakt vid $V_1 \iff f$ är injektiv.

Definition.

$$0 \to V_0 \xrightarrow{f} V_1 \xrightarrow{g} V_2 \to 0$$

kallas en *kort exakt följd* om den är exakt vid V_i för alla $i = 0, 1, 2$.

19.3 Dimensionssatsen.

Från grundläggande linjär algebra minns ni dimensionssatsen som säger att om $\Psi : V \to W$ är en linjär avbildning gäller

$$\dim V = \dim \ker \Psi + \dim \operatorname{im} \Psi.$$

Här följer en generalisering av denna sats. Vi ska använda den i beviset av att $I_P(f, gh) = I_P(f, g) + I_P(f, h)$ i nästa avsnitt, men den är av stor betydelse i sig själv och används jämt och ständigt i allehanda sammanhang.

Sats. Låt

$$0 \to U \xrightarrow{\Phi} V \xrightarrow{\Psi} W \to 0$$

vara en kort exakt följd av linjära rum och linjära avbildningar. Då finns delrum U' och W' till V sådana att $U' \cong U$, $W' \cong W$ och

$$V = U' \oplus W'.$$

Bevis. Eftersom Ψ är surjektiv finns en injektiv linjär avbildning $s : W \to V$ så att $\Psi \circ s = id_W$. (Låt en bas $\{e_i\}$ vara given i W. Tag ett element w_i i $\Psi^{-1}(e_i)$ för varje baselement e_i och definiera s genom $s(e_i) = w_i$.) Beteckna sammansättningen $\Pi = s \circ \Psi$. Då är $\Pi^2 = s \circ (\Psi \circ s) \circ \Psi = \Pi$. Varje element v i V kan skrivas $v = (v - \Pi(v)) + \Pi(v)$. Men $\Pi(v - \Pi(v)) = \Pi(v) - \Pi \circ \Pi(v) = 0$. Detta innebär att $v - \Pi(v) \in \ker(s \circ \Psi) = \ker(\Psi) = \operatorname{im}(\Phi)$, så v kan skrivas som en summa av ett element ur $\operatorname{im}(\Phi) \cong U$ och ett ur $\operatorname{im}(\Pi) = \operatorname{im}(s) \cong V$. Det återstår att se att $\operatorname{im}(s) \cap \operatorname{im}(\Phi) = \{0\}$. Ett element i detta snitt kan skrivas på två sätt $s(w) = \Phi(u)$. Applicerar vi Ψ på denna identitet får vi $w = (\Psi \circ s)(w) = (\Psi \circ \Phi)(u) = 0$. Detta visar Lemmat.

20 Skärningstalet.

20.1 Definition av skärningstalet och formulering av satsen.

Kom ihåg att om $P = (a, b) \in \mathbb{C}^2$ och motsvarande maximala ideal $\mathfrak{m}_P = (x - a, y - b)$, definierar vi den lokala ringen

$$\mathcal{O}_P = \mathbb{C}[x, y]_{\mathfrak{m}_P},$$

vari varje element kan tänkas som en rationell funktion som är reguljär i P. Två polynom genererar ett ideal $(f, g)_{\mathfrak{m}} \subset \mathcal{O}_P$. När det är klart från kontexten att idealet som f och g genererar på detta sätt ligger i $\mathcal{O}_P$ skriver vi ibland bara (f, g) för att göra notationen mindre belastad. Notera att de ingående ringarna och idealen också alla är vektorrum över $\mathbb{C}$.

Vi definierar skärningstalet mellan f och g i P på följande sätt:

Definition.

$$I_P(f,g) = \dim_{\mathbb{C}} \mathcal{O}_P/(f,g)_{\mathfrak{m}_P}.$$

Sats. Skärningstalet som definierat ovan har följande egenskaper.

(o) Skärningstalet är projektivt invariant.

(i) $I_P(f,g) \in \mathbb{N} \cup \{\infty\}$.

(ii) $I_P(f,g) = I_P(g,f)$.

(iii) Låt $O = (0,0) \in \mathbb{C}^2$. Då är $I_O(x,y) = 1$.

(iv) $I_P(f,g) = 0 \iff f(P) \neq 0$ eller $g(P) \neq 0$.

(v) $I_P(f,g) = I_P(f, g+fh)$.

(vi) $I_P(f,gh) = I_P(f,g) + I_P(f,h)$.

20.2 Bevis av skärningstalets egenskaper.

Bevis.

(o) En projektiv transformation ges i lämpliga kartor av en birationell ekvivalens $F : \mathbb{C}^2 \to \mathbb{C}^2$. Denna inducerar en $\mathbb{C}$-algebraisomorfi $F^* : \mathbb{C}(x,y) \to \mathbb{C}(x,y)$, genom $F^*(\frac{p}{q}) = \frac{p \circ F}{q \circ F}$. Denna uppfyller uppenbarligen

$$F^*(\mathcal{O}_P) = \mathcal{O}_{F^{-1}(P)} \text{ och } \phi((f,g)_{\mathfrak{m}_P}) = (f \circ F, g \circ F)_{\mathfrak{m}_{F^{-1}(P)}}$$

F^* inducerar därför en isomorfi $\mathcal{O}_P/(f,g)_{\mathfrak{m}_P} \cong \mathcal{O}_{F^{-1}(P)}/(f \circ F, g \circ F)_{\mathfrak{m}_{F^{-1}(P)}}$.

(i) och (ii) är uppenbara. För läsbarhetens skull skriver vi idealet $(f,g) = (f,g)_{\mathfrak{m}_P}$ utan angivelse av att det är lokaliserat nedan.Kolla detta ovanstående igen map F^*:s def

(iii)

$$I_O(f,g) = \dim_{\mathbb{C}} \mathcal{O}_O/(x,y) = \dim_{\mathbb{C}} \mathbb{C}[x,y]_{(x,y)}/(x,y) = \dim_{\mathbb{C}} \mathbb{C} = 1.$$

(iv) $I_P(f,g) = 0 \iff \mathcal{O}_P = (f,g) \iff 1 \in (f,g) \iff 1 = af + bg$. Om den sista likheten gäller kan uppenbarligen inte både f och g vara 0 i P. Om å andra sidan $f(P) \neq 0$, säg, är f inverterbar i $\mathcal{O}_P$ och $1 \in (f,g)$.

(v) $I_P(f,g) = I_P(f, g+fh)$ eftersom de berörda idealen är lika: $(f,g) = (f, g+fh)$

(vi) Detta kräver betydligt mer arbete. Vi delar upp i två fall.

Fall 1. Antag att f och g saknar gemensamma icke-konstanta faktorer. Betrakta följande vektorrum och linjära avbildningar.

$$\mathcal{O}_P/(f,h) \xrightarrow{\Phi} \mathcal{O}_P/(f,gh) \xrightarrow{\Psi} \mathcal{O}_P/(f,g),$$

där $\Phi(z) = gz + (f,gh)$ och $\Psi(x) = x + (f,g)$. Vi vill visa att Φ är injektiv, Ψ är surjektiv och att $\ker\Psi = \Phi(\mathcal{O}_P/(f,h))$. Då följer det från Lemmat att

$$\mathcal{O}_P/(f,gh) \cong \mathcal{O}_P/(f,h) \oplus \mathcal{O}_P/(f,g),$$

så att

$$I_P(f,gh) = \dim_{\mathbb{C}}(\mathcal{O}_P/(f,gh)) = \dim_{\mathbb{C}}(\mathcal{O}_P/(f,g)) + \dim_{\mathbb{C}}(\mathcal{O}_P/(f,h)) = I_P(f,g) + I_P(f,h).$$

Att Ψ är surjektiv är uppenbart.

Vi börjar med att visa $\ker\Psi = \Phi(\mathcal{O}_P/(f,h))$. Låt x vara ett element i $\mathcal{O}_P/(f,gh)$. Vi har att (för några a och b i $\mathcal{O}_P$):

$$\Psi(x) = 0 \iff x = af + bg \iff x = bg \iff x \in \Phi(\mathcal{O}_P/(f,h)),$$

så $\ker\Psi = \Phi(\mathcal{O}_P/(f,h))$.

Beviset för att Φ är injektiv är lite mer involverat. Antag att $z \in \ker\Phi$. Då har vi

$$gz = af + bgh,$$

där $f,g,h \in \mathbb{C}[x,y]$ är polynom, men där a, b och $z \in \mathcal{O}_P$[22]. Låt $S \in \mathbb{C}[x,y]$ vara produkten av nämnarna i a,b och z. Då är $S(P) \neq 0$. Vi gör oss av med nämnarna i ekvationen ovan genom att multiplicera med S:

$$g(Sz) = (Sa)f + (Sb)gh.$$

Sätt $A = Sa$, $B = Sb$ och $C = Sz$. Då kan vi skriva ekvationen som följer, med alla ingående element i $\mathbb{C}[x,y]$:

$$Cg = Af + Bhg \iff Af = g(C - Bh).$$

Eftersom f och g saknar gemensamma faktorer måste f dela $C - Bh$, dvs. $C - Bh = Df$, för något $D \in \mathbb{C}[x,y]$. Men $C = Sz$, så detta kan skrivas som

$$Sz = Df + Bh$$

och alltså

$$z = \frac{D}{S}f + \frac{B}{S}h,$$

vilket innebär att $z = 0 \in \mathcal{O}_P/(f,h)$, vilket skulle visas.

[22] Dessa har därför nämnare (som är nollskilda i P).

Fall 2. Antag att f och g har en gemensam irreducibel faktor q, $q(P) = 0$. Då är avbildningen $x + (f, g) \mapsto x + (q)$ en surjektiv linjär avbildning

$$\mathcal{O}_P/(f, g) \to \mathcal{O}_P/(q) = \mathbb{C}[x, y]_{\mathfrak{m}_P}/(q)_{\mathfrak{m}_P}.$$

Det följer att vi måste ha:

$$\dim_{\mathbb{C}} \mathcal{O}_P/(f, g) \geq \dim_{\mathbb{C}} \mathcal{O}_P/(q).$$

Vi ska nu visa att högerledet är ∞.

Låt $\pi : \mathbb{C}[x, y] \to \mathbb{C}[x, y]/(q)$ vara den kanoniska projektionen. Sätt $S = \mathbb{C} \setminus \mathfrak{m}_P$ och $\bar{S} = \pi(S)$. Då är $0 \notin \bar{S}$ eftersom annars det finns ett $f \in (q)$ så att $f(P) \neq 0$ vilket är en motsägelse.

Avbildningen

$$\mathcal{O}_P/(q) = \mathbb{C}[x, y]_{\mathfrak{m}_P}/(q)_{\mathfrak{m}_P} \to \bar{S}^{-1}(\mathbb{C}[x, y]/(q)),$$

som tar $\dfrac{r}{s} + (q)_{\mathfrak{m}_P} \mapsto \dfrac{r + (q)}{s + (q)}$ är en isomorfi.

Eftersom $\mathbb{C}[x, y]/(q)$ är ett integritetsområde och $0 \notin \bar{S}$ så är den naturliga avbildningen en injektion av $\mathbb{C}[x, y]/(q)$ i lokaliseringen $\bar{S}^{-1}(\mathbb{C}[x, y]/(q))$. Det följer att

$$\dim_{\mathbb{C}} \bar{S}^{-1}(\mathbb{C}[x, y]/(q)) \geq \dim_{\mathbb{C}} \mathbb{C}[x, y]/(q).$$

Vi ska nu visa att $\mathbb{C}[x, y]/(q)$ inte har ändlig dimension. Vi vet sedan tidigare att det finns oändligt många punkter som uppfyller $q(x, y) = 0$. Låt $n \in \mathbb{N}$ vara givet. Tag $P_1, ..., P_n$ sådana att $q(P_i) = 0, \forall\, 0 \leq i \leq n$. Då kan vi konstruera $f_1, ..., f_n \in \mathbb{C}[x, y]$ s.a. $f_i(P_j) = 0$ om $i \neq j$ och $f_i(P_i) = 1$ för alla i [23]. Om

$$\sum_i \lambda_i f_i = mq,$$

ser vi genom att räkna ut båda sidor i P_j att $\lambda_j = 0$ för alla j. Detta betyder att $f_1, ..., f_n$ är linjärt oberoende i $\mathbb{C}[x, y]/(q)$ så att dimensionen för $\mathbb{C}[x, y]/(q) \geq n$. Men n var ett godtyckligt naturligt tal, så

$$\dim_{\mathbb{C}}(\mathbb{C}[x, y]/(q)) = \infty.$$

Därför har vi till sist

$$\dim_{\mathbb{C}} \mathcal{O}_P/(f, g) \geq \dim_{\mathbb{C}} \mathcal{O}_P/(q) = \dim_{\mathbb{C}} \mathbb{C}[x, y]_{\mathfrak{m}_P}/(q) =$$

$$= \dim_{\mathbb{C}}(\mathbb{C}[x, y]/(q))_{\mathfrak{m}_P} \geq \dim_{\mathbb{C}} \mathbb{C}[x, y]/(q) = \infty.$$

Eftersom f och gh har en gemensam faktor om f och g har det, gäller också

$$\dim_{\mathbb{C}} \mathcal{O}_P/(f, gh) = \infty.$$

Båda sidorna i (vi) är alltså oändliga i detta fall.

Detta avslutar beviset och dessa föreläsningsanteckningar.

[23] Övning!

21 Referenser

1. Robert Bix, *Conics and Cubics*, A Concrete Introduction to Algebraic Curves, Springer.
2. Frances Kirwan, *Complex Algebraic Curves*, London Mathematical Society.
3. William Fulton, *Algebraic Curves*, Addison-Wesley.
4. Miles Reid, *Undergraduate Algebraic Geometry*, London Mathematical Society.