

Affin och projektiv geometri

Magnus Jacobsson

October 17, 2022

Contents

1	Introduktion och Varning.	3
2	Repetition: Algebra.	4
2.1	Ringar och kroppar.	4
2.2	Faktorisering och irreducibilitet.	5
2.3	Ideal och kvotringar.	8
2.4	Ringhomomorfismer.	9
2.5	Fraktionskroppar.	11
3	Repetition: Linjär algebra.	12
3.1	Grundläggande satser om linjära rum.	12
3.2	Kvadratiske former.	13
3.3	Reella kvadratiske former.	13
3.4	Direkt summa.	14
3.5	Exakta följder.	15
3.6	En generalisering av dimensionssatsen.	15
4	Repetition: Lite flervariabelanalys.	16
4.1	Nivåkurvor, gradient, linjarisering och Taylorutveckling.	16
4.2	Implicita funktionssatsen.	17
5	Reell affin geometri.	18
5.1	Reella algebraiska kurvor.	18
5.2	Begreppet klassificering.	20
5.3	Affina och euklidiska transformationer	21
5.4	Klassificering av reella förstgradspolynom i planet.	25
5.5	Klassificering av reella andragradspolynom upp till affina transformationer.	26
6	Algebraiska kurvor.	30
6.1	Irreducibilitet hos kurvor.	30
6.2	En sats om algebraiska kurvor.	30
6.3	Något om algebraiska kurvor över andra kroppar än \mathbb{C} . Inte skrivet än.	32

7	Bezouts sats, diskussion	32
8	Komplex affin geometri.	33
8.1	Komplexa affina linjer och kurvor.	33
8.2	Generaliserade tangentlinjer.	35
8.3	Komplexa affina transformationer.	35
8.4	Komplexa kvadratiske former.	36
8.5	Klassificering av komplexa andragradspolynom upp till affin ekvivalens.	36
8.6	Två satser till om komplexa kurvor.	37
8.7	Komplex analys och geometri.	38
8.8	Några geometriska exempel.	40
9	Skärningsmultiplicitet	41
9.1	Axiomen	41
9.2	Preliminära konsekvenser av axiomen.	43
10	Reell projektiv geometri	47
10.1	Historia.	47
10.2	Motiverande diskussion.	47
10.3	Det reella projektiva planet.	48
10.4	Homogena polynom och projektiva plana algebraiska kurvor	49
10.5	Den sfäriska modellen av $\mathbb{R}P^2$. Skivmodellen.	54
10.6	Projektiva transformationer och fyrpunktssatsen.	54
10.7	Den reella projektiva linjen och dess transformationer.	58
10.8	Projektiv klassificering av andragradskurvor.	60
11	Komplex projektiv geometri	61
11.1	Projektiva rum över \mathbb{C}	61
11.2	Komplexa projektiva linjen $\mathbb{C}P^1$	62
11.3	Projektiva transformationer över \mathbb{C}	63
11.4	Komplex projektiv klassificering av andragradskurvor.	64
11.5	Skärningstalet återbesökt.	64
12	Bezouts sats, formulering och bevis.	66
12.1	Lemma 1. Fallet då en av kurvorna är en linje.	66
12.2	Lemma 2. y -oberoende faktorer kan ignoreras.	67
12.3	Lemma 3. Reduktion av y -graden.	68
12.4	Beviset avslutas.	69
13	Några tillämpningar av Bezouts sats	69
13.1	En kommentar om dimensionsräkning och en sats om andragradskurvor.	69
13.2	Singulära kurvor	71
13.3	Reella algebraiska kurvor och deras ovaler. (Överkurs.) Ej skrivet än.	73

14 Tredjegradskurvor	73
14.1 Hessianen och inflexionspunkter.	73
14.2 Klassificering av glatta projektiva tredjegradskurvor	76
14.3 Klassificering av singulära tredjegradskurvor.	79
15 Elliptiska kurvor.	81
15.1 Additionslagen.	81
15.2 Bevis av associativiteten i det generiska fallet.	82
15.3 Topologisk slutkläm på beviset av associativiteten. (Överkurs.)	84
15.4 Elliptiska kurvor på normalform.	86
15.5 Något om elliptiska kurvor över andra kroppar än \mathbb{C} . Ej skrivet än.	86
16 Mer algebra.	86
16.1 Radikalideal och reducerade ringar.	86
17 Algebraiska mängder. Funktioner och avbildningar.	88
17.1 Algebraiska mängder.	88
17.2 Koordinatringen.	89
17.3 Reguljära avbildningar	91
17.4 Rationella funktioner	92
17.5 Rationella avbildningar	93
18 Lokalisering och skärningstalets definition.	94
18.1 Lokalisering av integritetsområde.	94
18.2 Lokalisering i allmänna fallet. (Mestadels överkurs.)	96
18.3 Exempel på lokalisering i algebraisk geometri.	98
18.4 Skärningstalets definition och exempel.	100
18.5 Relationen till koordinatringen.	101
19 Skärningstalet uppfyller axiomen.	102
19.1 Formulering av satsen.	102
19.2 Bevis av att $I_P(f, g)$ uppfyller axiomen.	103
20 En alternativ definition av skärningstalet. (Överkurs.)	106
20.1 Formella potensserier och parametrisering av kurvor.	106
20.2 Alternativ definition av skärningstalet.	108
20.3 Bevis för axiomen för denna definition.	109
21 Referenser	109

1 Introduktion och Varning.

Det här är mer föreläsningssanteckningar än en bok än så länge, så det finns garanterat fel och slarvigheter i dem. Vissa avsnitt 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} .

¹En 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 $k[x_1, \dots, x_n]$ 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

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

Definition. En ring som dessutom är ett k -vektorrum och sådant att regeln ovan gäller kallas en (*kommutativ*) k -*algebra*.

Vi kommer i fortsättningen att referera till $k[x_1, \dots, x_n]$ 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 $p = p(x_1, \dots, x_n) \in k[x_1, \dots, x_n]$. 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 entydig primtalsfaktorisering. Motsvarande påstående om polynom är följande. Det torde vara bekant i envariabelfallet $n = 1$.

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

Definition. Egenskapen som beskrivs i satsen kan uttryckas genom att säga att $k[x_1, \dots, x_n]$ 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 kurser².

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 $k[x_1, \dots, x_n]$ är irreducibla. (Notera att graden av en produkt är summan av graderna.)

²Ett 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.

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 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 entydiga 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

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

Då kan vi skriva om som följer:

$$\begin{aligned} f(x, y) &= a_n(x)y^n + \dots + a_1(x)y + a_0(x) = \\ &= (y - p(x))(a_n(x)y^{n-1} + \dots + a_1(x)) + p(x)(a_n(x)y^{n-1} + \dots + a_1(x)) + a_0(x) = \\ &= (y - p(x))q_1(x, y) + r_1(x, y), \end{aligned}$$

där vi har använt beteckningarna

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

och

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

Eftersom $\deg_y r_1 < n$ är enligt induktionsantagandet

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

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, med ett likartat men lite mer omständligt bevis.

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

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

Bevis. Utelämnas.

Anmärkning. Beviset för satsen ovan fungerar mer allmänt, nämligen då element f, g är element i en polynomringar $R[y]$ med koefficienter i en allmän ring R . Satsen motsvarar fallet $R = k[x]$.

Övningar.

1. Kontrollera att polynomringen $k[x, y]$ är en k -algebra, genom att gå igenom alla axiom.
2. Är $k[x, y]$ en kropp?

2.3 Ideal och kvotringar.

Definition. En icke-tom delmängd $I \subseteq R$ 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 ändliga linjärbinationer

$$r_1s_1 + \cdots + r_ns_n,$$

av element s_i ur S med koefficienter r_i i R ett ideal i R , som vi betecknar med (S) och kallar för idealet genererat av S .

Anmärkning. För k -algebraer kräver vi också att I är ett delvektorrum.

Exempel.

- (i) Varje ideal i \mathbb{Z} genereras av ett enda element k : $(k) = \{nk \mid n \in \mathbb{Z}\}$ (det minsta positiva elementet i I genererar I , använd divisionsalgoritmen). Detta ideal betecknas också $k\mathbb{Z}$.
- (ii) Varje ideal i $k[x]$ genereras av ett enda polynom $p(x)$, och består av alla polynom som har p som faktor: $(p) = \{mp \mid m \in k[x]\}$.
- (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 (algebra) 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 (kvotalgebra). Namnet motiveras av följande sats.

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

2.4 Ringhomomorfismer.

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

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

- $f(1) = 1$

Anmärkning. Om R och S är k -algebror, kräver vi också k -linjaritet, så att $f(\lambda \cdot x) = \lambda f(x)$, och får definitionen för en k -algebrahomomorfism.

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

$$\text{ev}_a : k[x_1, \dots, x_n] \rightarrow k,$$

definierad genom $\text{ev}_a(f) = f(a_1, \dots, a_n)$ kallas *evalueringshomomorfismen* i punkten a . Detta är en k -algebrahomomorfism.

Sats. Om $f : R \rightarrow S$ är en ringhomomorfism (algebrahomomorfism) 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 och är mycket användbar. Motsvarande sats gäller även för k -algebror.

Sats. Om $f : R \rightarrow S$ är en surjektiv ringhomomorfism 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 $\pi : R \rightarrow R/I$ som ges av $r \mapsto r + I$ är en surjektiv homomorfism.

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.

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 $xy = 0$.

2.5 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:

- (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 (nollställena till nämnaren).

Sats. Den naturliga avbildningen $R \rightarrow Q(R)$ given av $p \mapsto \frac{p}{1}$ är en injektiv ringhomomorfism, 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 $\mathbb{C}[x, y] \subset \mathbb{C}(x, y)$.

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. **Vektorrum över k .**

Låt V vara ett vektorrum över k .

Definition. Vektorer $\mathbf{v}_1, \dots, \mathbf{v}_m$ i V kallas *linjärt oberoende* om

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

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

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

Sats. Varje bas för V har samma kardinalitet.

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

Definition. En funktion $F : V \rightarrow W$ 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 entydigt bestämd av sina värden på elementen i en bas.

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 $\text{char } k \neq 2$.

Definition. En funktion $q : V \rightarrow k$ 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, \dots, 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 kvadratiske 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 kvadratiske formen av den diagonala matrisen $T^t Q T$. I dessa koordinater har den då formen

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

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 kvadratiske 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

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

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

3.4 Direkt summa.

Följande definition ingår möjligen inte i Linjär algebra II.

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 $v \in W$ kallas V summan av U och W och vi skriver $V = U + W$. Om dessutom $U \cap W = \{0\}$ kallas V den direkta summan av U och W , vilket betecknas $V = U \oplus W$.

Exempel. \mathbb{R}^2 är den direkta summan av x -axeln och y -axeln. Det är också den direkta summan av y -axeln och linjen $y = ax$, $a \in \mathbb{R}$ t.ex.

Exempel. \mathbb{R}^3 är den direkta summan av x -axeln och yz -planet. Den är summan, men inte direkta summan av xz -planet och yz -planet.

Exempel. Om V är ett vektorrum och F är en diagonaliserbar linjär operator på V , så är V den direkta summan av egenrummen till F ,

$$V = \bigoplus_{\lambda} E_{\lambda}.$$

3.5 Exakta följder.

Definition. En följd av linjära rum och linjära avbildningar

$$U \xrightarrow{f} V \xrightarrow{g} W,$$

kallas *exakt vid* V_1 om $\ker g = \operatorname{im} f$.

Exempel.

$$V \xrightarrow{f} W \rightarrow 0.$$

är exakt vid $W \iff f$ är surjektiv. Här betecknar 0 vektorrummet med bara en enda vektor i och den omärkta pilen den enda möjliga linjära avbildningen, $0 \mapsto 0$.

Exempel.

$$0 \rightarrow U \xrightarrow{f} V$$

är exakt vid $U \iff f$ är injektiv.

Definition.

$$0 \rightarrow U \xrightarrow{f} V \xrightarrow{g} W \rightarrow 0$$

kallas en *kort exakt följd* om den är exakt vid U, V, W för alla $i = 0, 1, 2$.

Exempel.

$$0 \rightarrow \mathbb{R} \xrightarrow{f} \mathbb{R}^2 \xrightarrow{g} \mathbb{R} \rightarrow 0,$$

där $f(x) = (x, 0)$, $g(x, y) = y$ är en kort exakt följd.

3.6 En generalisering av dimensionssatsen.

Från grundläggande linjär algebra minns ni dimensionssatsen som säger att om $\Psi : V \rightarrow W$ är en linjär avbildning mellan ändligdimensionella vektorrum 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 skärningstalet uppfyller axiomen i ett av bokens sista avsnitt, men den är av stor betydelse i sig själv och används jämt och ständigt i allehanda sammanhang.

Sats. Låt

$$0 \rightarrow U \xrightarrow{\Phi} V \xrightarrow{\Psi} W \rightarrow 0$$

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 $s : W \rightarrow V$ så att $\Psi \circ s = id_W$. Låt nämligen en bas $\{e_i\}$ vara given i W . För varje baselement e_i , kan vi ta w_i i $\Psi^{-1}(e_i)$ och definiera s genom $s(e_i) = w_i$. Då är uppenbarligen $(\Psi \circ s)(e_i) = \Psi(w_i) = e_i$.

Betrakta nu den omvända sammansättningen $\Pi = s \circ \Psi$. Då är $\Pi^2 = s \circ (\Psi \circ s) \circ \Psi = \Pi$.

Varje element v i V kan förstås skrivas

$$v = (v - \Pi(v)) + \Pi(v).$$

Uppenbarligen är

$$\Pi(v) \in \text{im}(\Pi) = \text{im}(s).$$

Eftersom $\Pi(v - \Pi(v)) = \Pi(v) - \Pi \circ \Pi(v) = 0$ så är $v - \Pi(v) \in \ker \Pi = \ker s \circ \Psi$. Men eftersom s är injektiv och följd exakt, har vi $\ker(s \circ \Psi) = \ker(\Psi) = \text{im}(\Phi)$. Kallar vi nu $\text{im}(\Phi)$ för U' och $\text{im}(s)$ för W' , så har vi

$$V = U' + W' \cong U + W.$$

Det återstår att se att

$$U' \cap W' = \text{im}(s) \cap \text{im}(\Phi) = \{0\}.$$

Ett element i detta snitt kan skrivas på två sätt, nämligen som $s(w) = \Phi(u)$. Applicerar vi Ψ på denna identitet får vi $w = (\Psi \circ s)(w) = (\Psi \circ \Phi)(u) = 0$, så $s(w) = s(0) = 0$. Detta visar satsen.

4 Repetition: 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 C^∞ .

4.1 Nivåkurvor, gradient, linjarisering och Taylorutveckling.

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

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

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 $f : \mathbb{R}^n \rightarrow \mathbb{R}$ är vektorfältet

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

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 $\frac{\partial f}{\partial y}(a, b) \neq 0$ 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 nivå mängder 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.

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

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.

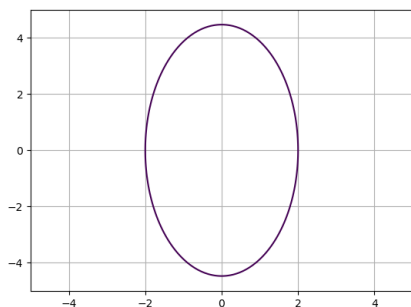


Figure 1: $\frac{x^2}{4} + \frac{y^2}{20} = 1$.

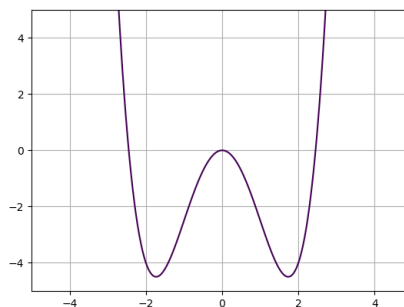


Figure 2: $y = \frac{x^4}{4} - 3x^2$.

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, polnomekvationen $x^2 + y^2 + 1 = 0$ 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.
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.

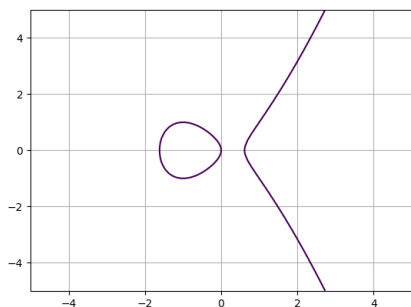


Figure 3: Kurvan $y^2 = x^3 - x$.



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

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 $\frac{\partial}{\partial x} x^n y^m = n x^{n-1} y^m$, 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 $x^2 y^3 + x^2 + y^2 = 0$.

5.2 Begreppet klassificering.

Låt

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

vara en andragsgradskurva. 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 ofta 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. Detta är då en ekvivalensrelation på klassen av ändliga mängder.

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 (isomorfism) 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 kvadratiske former, som nämns i repetitionskapitlet för linjär algebra ovan. Ett sätt att klassificera dessa är med hjälp av ortogonala avbildningar. Då är två kvadratiske former "desamma" om deras matriser har samma egenvärden. Alternativt kan vi klassificera reella kvadratiske former upp till allmänna linjära inverterbara avbildningar och då betrakta två kvadratiske 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 $\mathbf{T}_{\mathbf{a}} : \mathbb{R}^n \rightarrow \mathbb{R}^n$ given av $\mathbf{T}_{\mathbf{a}}(\mathbf{r}) = \mathbf{r} + \mathbf{a}$, kallas *translation* med \mathbf{a} .

Notera att om $\mathbf{a} \neq 0$ så är $\mathbf{T}_{\mathbf{a}}$ 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 $\mathbf{F}(\mathbf{r}) = \mathbf{L}(\mathbf{r}) + \mathbf{a}$ ($= (\mathbf{T}_{\mathbf{a}} \circ \mathbf{L})(\mathbf{r})$), där \mathbf{L} är linjär och \mathbf{a} är en vektor kallas en *affin avbildning*. Om \mathbf{L} är bijektiv kallas \mathbf{F} en *affin transformation*.

Anmärkning. Observera att derivatan $D\mathbf{F}(\mathbf{r})$ av en affin avbildning som ovan är konstant lika med \mathbf{L} .

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

Exempel: Avbildningen

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

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

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

Sats. Några algebraiska egenskaper hos affina avbildningar.

- (a) Sammansättningen av två affina (euklidiska) avbildningar är affin (euklidisk).
- (b) Affina (euklidiska) transformationer är inverterbara och inversen är affin (euklidisk).

Bevis.

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

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

som är affin. (Och euklidisk om \mathbf{F}, \mathbf{G} är det.)

- (b) Övning. Ange en formel för inversen.

Anmärkning. Påståendena i satsen tillsammans med det uppenbara faktum att identitetsavbildningen är en affin transformation och att sammansättning är en associativ operation, 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 $\text{Aff}(n)$.

Sats. Några geometriska egenskaper hos affina avbildningar.

- (a) Bilden av en linje under en affin transformation är en linje.
- (b) Affina transformationer bevarar parallellitet.
- (c) Affina transformationer bevarar transversalitet. (Euklidiska transformationer bevarar dessutom vinkeln mellan transversella kurvor.)

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

Bevis.

- (a) Om linjen framställs på parameterform som $\mathbf{r}(t) = \mathbf{r}_0 + t\mathbf{v}$ får vi

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

vilket också är en linje på parameterform.

- (b) Jämför med (c) i förra satsen. Om två linjer har parallella riktningsvektorer \mathbf{v} och \mathbf{v}' har deras bilder det också (nämligen, $\mathbf{L}(\mathbf{v})$ och $\mathbf{L}(\mathbf{v}')$).
- (c) Antag att två kurvor C, C' skär varandra i en punkt \mathbf{r} och att deras tangentvektorer där är \mathbf{v} och \mathbf{v}' . Då skär bilderna $\mathbf{F}(C)$ och $\mathbf{F}(C')$ varandra i $\mathbf{F}(\mathbf{r})$ och tangentvektorerna är $D\mathbf{F}(\mathbf{r})(\mathbf{v}) = \mathbf{L}(\mathbf{v})$ respektive $D\mathbf{F}(\mathbf{r})(\mathbf{v}') = \mathbf{L}(\mathbf{v}')$. Om \mathbf{v} och \mathbf{v}' är linjärt oberoende är $\mathbf{L}(\mathbf{v})$ och $\mathbf{L}(\mathbf{v}')$ det också, eftersom \mathbf{L} är en linjär isomorfism. (Mer allmänt gäller påståendet (e) för diffeomorfismer.)

- (d) 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 $\frac{|\overline{AB}|}{|\overline{CD}|} = |\lambda|$. Vi får (med $\mathbf{F}(\mathbf{v}) = \mathbf{L}(\mathbf{v}) + \xi$):

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

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

$$\mathbf{F}^* : \mathbb{R}[x_1, \dots, x_n] \rightarrow \mathbb{R}[x_1, \dots, x_n]$$

via $\mathbf{F}^*(f) = f \circ \mathbf{F}$. Vi kallar \mathbf{F}^* den av \mathbf{F} inducerade avbildningen.

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 ett affint variabelbyte. Om t.ex. $\mathbf{F}(x, y) = (x + 2y, 3y + 1)$ och $f(x, y) = x^2 + y^2$ så är $\mathbf{F}^*(f)(x, y) = (x + 2y)^2 + (3y + 1)^2 = x^2 + 13y^2 + 4xy + 6y + 1$.

Definition. Två polynom f och g kallas *affint ekvivalenta* om det finns ett tal $\lambda \in \mathbb{R} \setminus \{0\}$ så att $\lambda g = \mathbf{F}^*(f)$ för någon affin transformation \mathbf{F} .

Anmärkning. Talet λ i definitionen kommer sig av att vi egentligen är mest 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.

Sats. Om f är ett polynom av grad k så är $\mathbf{F}^*(f)$ också av grad k . (Notera att detta innehåller det tidigare bevisade påståendet att \mathbf{F} bevarar linjer.)

Bevis. Eftersom \mathbf{F} 's komponenter är polynom av grad ≤ 1 så är det uppenbart att

$$\deg f(\mathbf{F}(x_1, \dots, x_n)) \leq \deg f(x_1, \dots, x_n).$$

Men eftersom inversen \mathbf{F}^{-1} också är affin har vi även

$$\deg f(x_1, \dots, x_n) = \deg f(\mathbf{F}^{-1}(\mathbf{F}((x_1, \dots, x_n)))) \leq \deg f(\mathbf{F}(x_1, \dots, x_n)),$$

så resultatet följer.

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

Bevis. Inversen ges förstås av $(\mathbf{F}^{-1})^*$. Vi behöver även visa $\mathbf{F}^*(f + g) = \mathbf{F}^*(f) + \mathbf{F}^*(g)$, $\mathbf{F}^*(fg) = \mathbf{F}^*(f)\mathbf{F}^*(g)$ och $\mathbf{F}^*(1) = 1$ samt $\mathbf{F}^*(\lambda f) = \lambda \mathbf{F}^*(f)$. Detta lämnas med varm hand till läsaren.

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

Sats. Avbildningen $(-)^* : \text{Aff}(n) \rightarrow \text{Aut}(\mathbb{R}[x_1, \dots, x_n])$ som ges av $\mathbf{F} \mapsto \mathbf{F}^*$ har följande egenskaper³.

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

Bevis. Rättframt.

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

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

är en ekvivalensrelation.

Bevis. Detta följer enkelt från de två föregående satserna. Antag t.ex. att $\lambda g = \mathbf{F}^*(f)$ och att $\mu h = \mathbf{G}^*(g)$. Då har vi

$$\mu h = \mathbf{G}^*\left(\frac{\mathbf{F}^*(f)}{\lambda}\right) \iff \mu \lambda h = (\mathbf{F} \circ \mathbf{G})^*(f),$$

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

vilket visar transitivitet. Reflexivitet och symmetri lämnas till läsaren.

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

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

Bevis. Uppenbart.

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 $\mathbf{T}_{\mathbf{a}}$ den affina avbildningen som är translation med vektorn \mathbf{a} . Låt \mathbf{F} vara en linjär inverterbar avbildning. Visa att $\mathbf{F} \circ \mathbf{T}_{\mathbf{a}} \circ \mathbf{F}^{-1} = T_{\mathbf{F}(\mathbf{a})}$.
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 $\mathbf{F}^{-1}(P)$ en singulär punkt på kurvan $\mathbf{F}^*(p) = p \circ \mathbf{F} = 0$.
6. Låt $f(x, y) = 2x^2 + 2xy + 13y^2 - 1$. och $\mathbf{F}(x, y) = \frac{1}{5}(2x + 3y, x - y)$. Beräkna $\mathbf{F}^*(f)$.
7. Utgå ifrån förra uppgiften. Skissa kurvorna $f(x, y) = 0$ och $\mathbf{F}^*(f)(x, y) = 0$.
8. Visa satsen ovan: Om $(x, y) \in V(f)$ så är $\mathbf{F}^{-1}(x, y) \in V(\mathbf{F}^*(f))$.

5.4 Klassificering av reella förstegradspolynom i planet.

Vi sticker emellan med ett uppenbart men viktigt påpekande, nämligen att det upp till affina transformationer bara finns en linje i planet.

Sats. Alla förstegradspolynom i $\mathbb{R}[x, y]$ är affint (rentav euklidiskt) ekvivalenta, t.ex. med x .

Bevis. Det är förstås geometriskt självklart att varje linje kan translateras och eller roteras, så att den hamnar på x -axeln. Vi ger ett algebraiskt bevis som uppvärmning för nästa avsnitt, där beviset vi ska genomföra är mindre geometriskt uppenbart. Betrakta ett allmänt linjärt polynom $f(x, y) = ax + by - c$ i $\mathbb{R}[x, y]$. Om $a \neq 0$ gör vi den affina transformationen $\mathbf{F}(x, y) = (x/a - (b/a)y + c/a, y)$. Då är

$$\mathbf{F}^*(f)(x, y) = a(x/a - (b/a)y + c/a) + by - c = x.$$

Om $a = 0$ kan vi betrakta $\mathbf{F}(x, y) = (y, x/b + c/b)$ så att

$$\mathbf{F}^*(f)(x, y) = b(x/b + c/b) - c = x + c - c = x.$$

(Med marginellt mer arbete kan du förstås rentav skriva ned en euklidisk transformation 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 2.⁴ 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 kvadratiske formen q i de nya koordinaterna, som vi också betecknar (x, y) , ges av en diagonalmatrix, 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

⁴Vi kan skriva uttrycket på matrisform om det känns mer bekant, enligt:

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

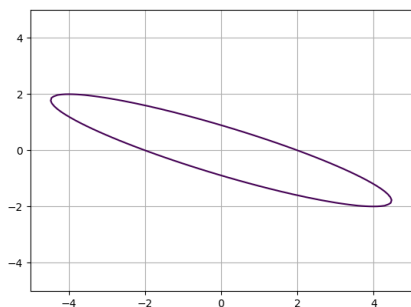


Figure 5: Kurvan $x^2 + 5y^2 - 4xy = 4$. En ellips.

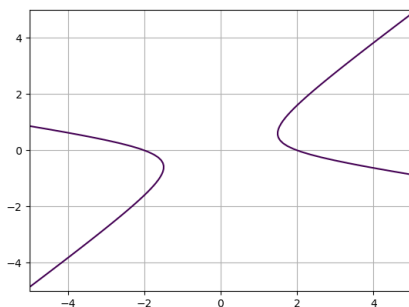


Figure 6: Kurvan $x^2 - 5y^2 - 4xy = 4$. En hyperbel.

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 analys i flera fall.

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

Vi kan då kvadratkomplettera

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

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

$$\mathbf{F}^*(p) = x^2 + \lambda y^2 + F.$$

Vi får nu dela upp i fall.

Fall A1. 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).

Fall A2. Om $F \neq 0$ kan vi göra transformationen $\mathbf{F}(x, y) = (\sqrt{|F|x}, \sqrt{|F|y})$. I fallet $\lambda = 1$ ger detta oss

$$\begin{aligned}\mathbf{F}^*(x^2 + y^2 + F) &= (\sqrt{|F|x})^2 + (\sqrt{|F|y})^2 + F = \\ &= |F|(x^2 + y^2 \pm 1) \sim x^2 + y^2 \pm 1,\end{aligned}$$

vilket är uttrycken i (a) respektive (i). I fallet $\lambda = -1$ får vi på liknande sätt

$$\begin{aligned}\mathbf{F}^*(x^2 - y^2 + F) &= (\sqrt{|F|x})^2 - (\sqrt{|F|y})^2 + F = \\ &= |F|(x^2 - y^2 \pm 1) \sim x^2 - y^2 \pm 1,\end{aligned}$$

vilket är uttrycket i (b) om den sista termen har ett minustecken. Om den har ett plustecken gör vi transformationen $(x, y) \mapsto (y, x)$ som är ekvivalent med (b) igen.

5.5.2 Fall B. $\lambda = 0$.

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

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

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 $\mathbf{F}(x, y) = (x - \frac{D}{2}, y - f/E + D^2/4E)$. Detta ger polynomet

$$Ey + x^2 = |E|(\pm y + \frac{x^2}{|E|}) \sim \pm y + \frac{x^2}{|E|},$$

som efter transformationen $\mathbf{F}(x, y) = (\sqrt{|E|x}, \mp y)$ ger uttrycket i (c).

Fall B2. $E = 0$. Om $E = 0$ är $p(x, y) = (x + D/2)^2 + F$, vilket om vi gör transformationen $\mathbf{F}(x, y) = (x - D/2, y)$ blir $x^2 + F$. Om $F = 0$ är detta polynom detsamma som i (g). Om $F \neq 0$ gör vi $\mathbf{F}(x, y) = (\sqrt{|F|x}, y)$ och får

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

I fallet med plustecken är detta (h). I fallet med minustecken kan det faktoriseras som $x^2 - 1 = (x + 1)(x - 1)$, som efter $\mathbf{F}(x, y) = (2x - 1, y)$ blir

$$2x(2x - 2) = 4x(x - 1) \sim x(x - 1),$$

vilket är uttrycket i (f).

Vi måste också visa att inga av dessa nio polynom är ekvivalenta med varandra. Först noterar vi att signaturen hos den kvadratiske formen q är oförändrad under affina transformationer. Alltså kan inte två polynom med olika signatur vara ekvivalenta.

Signaturen $(1, 1)$ förekommer i fallen (a), (e) och (i). Affina transformationer bevarar kardinaliteten hos nollställesmängden. (a) har oändligt många punkter, (e) har en och (i) har ingen. Alltså är dessa fall sinsemellan olika.

Signaturen $(1, -1)$ förekommer i fallen (b) och (d). Affina transformationer bevarar singulära punkter enligt en tidigare övningsuppgift. En singulär punkt 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. I (c) finns ingen linje, i (f) två och i (g) en. (h) är tom. Detta räcker för att skilja dessa fall åt och avslutar beviset.

Exempel. Om man vill förenkla ett kvadratisk polynom till någon av standardformerna till satsen är normalt det lättaste att börja med att genomföra en kvadratkomplettering och sedan göra ett lämpligt variabelbyte. Som exempel, låt $f(x, y) = x^2 + 2xy + 5y^2 + x + 9y$. Vi börjar med kvadratkompletteringen

$$x^2 + 2xy + 5y^2 + x + 9y = (x + y)^2 + 4y^2 + x + 9y.$$

Nu faller det sig naturligt att göra variabelbytet $x + y \rightarrow x$, $y \rightarrow y$ och få

$$x^2 + x + 4y^2 + 8y = (x + \frac{1}{2})^2 + (2y + 2)^2 - \frac{17}{4},$$

varefter ett till variabelbyte (en translation) $x + \frac{1}{2} \rightarrow x$, $2y + 2 \rightarrow y$ ger

$$x^2 + y^2 - \frac{17}{4} = \frac{17}{4} \left(\left(\frac{x}{\sqrt{\frac{17}{4}}} \right)^2 + \left(\frac{y}{\sqrt{\frac{17}{4}}} \right)^2 - 1 \right),$$

som efter en övergripande skalning $(x, y) \rightarrow (\sqrt{\frac{17}{4}}x, \sqrt{\frac{17}{4}}y)$ är en multipel av $x^2 + y^2 - 1$.

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.

Låt k vara vilken kropp som helst (även om vi i denna kurs håller oss till \mathbb{R} eller \mathbb{C}). Låt $f \in k[x, y]$.

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

Bevis. Övning.

Eftersom f har en entydig faktorisering i irreducibla faktorer (se repetitionskapitlet om algebra), är $V(f)$ unionen av nollställesmängderna till dessa faktorer.

Definition. 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 andragsgradskurvor 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 denna fråga i nästa avsnitt.

Övningar.

1. Låt $f(x)$ och $g(x)$ vara två polynom som saknar gemensamma faktorer (förutom konstanter). Visa att $f(x) + yg(x)$ är irreducibelt.
2. 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 .
3. 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 .

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 ten-

tan.

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 slutklämman. 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 (nollskilt⁵) polynom av en variabel och det finns bara ändligt många nollställena $x = a$ 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 skriva⁶

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

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

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

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

där alla d, e, g, h är polynom i y . Om vi alltså multiplicerar (**) med $a(y) = d_0(y)\dots d_m(y)e_0(y)\dots e_n(y)$ 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 formen⁷

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

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

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

⁵Om $f(x, b)$ vore nollpolynomet skulle $y - b$ dela $f(x, y)$ men f är ju irreducibelt.

⁶Här använder vi Bezouts lemma i polynomringen i en variabel över kroppen av rationella funktioner i y , $k(y)$.

⁷Jag återanvänder samma symboler som ovan men det är förstås inte samma funktioner!

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

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

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

Om f antas dela g i $k(y)[x]$ får vi:

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

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

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

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.

6.3 Något om algebraiska kurvor över andra kroppar än \mathbb{C} . **Inte skrivet än.**

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

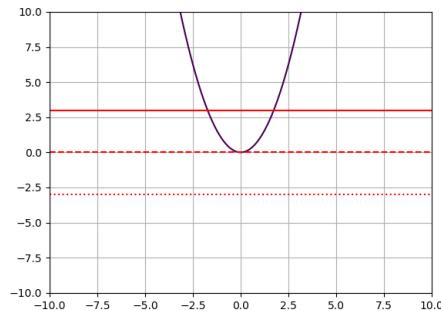


Figure 7: Tre olika konfigurationer av en parabel och en linje.

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 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 $\mathbf{r} = (z_1, \dots, z_n)$ som kan skrivas

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

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, motsvarande parametervärden t_i och s_i . Detta ger oss två ekvationer enligt nedan:

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

Subtraheras den andra ekvationen från den första får vi:

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

så att $\mathbf{w} = \frac{t_1 - t_2}{s_1 - s_2}\mathbf{v}$. 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

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

Vi har då visat att en godtycklig punkt på den ena av linjerna också ligger på den andra. Detta avslutar beviset.

Sats. Två linjer $L_1 \neq L_2$ i \mathbb{C}^2 som inte är parallella skär varandra i en entydig 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 $x \mapsto x, y \mapsto \frac{2 + i}{2i - 1}y$ 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 entydig faktorisering i linjära faktorer.

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

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

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

Definition. Vi kallar n för f 's *multiplicitet i P* och betecknar den understundom med $m_P(f)$.

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}^n , $\text{Aff}_{\mathbb{C}}(n)$, är en grupp och inducerar avbildningar på $\mathbb{C}[x_1, \dots, x_n]$ på samma sätt som i det reella fallet (och med samma bevis). 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 är alla komplexa linjer i \mathbb{C}^2 ekvivalenta.

Bevis. Övning.

8.4 Komplexa kvadratiske former.

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

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

Bevissskiss. Vad som behöver visas är att varje symmetrisk matris A med komplexa koefficienter är ekvivalent med en diagonal matris $D = T^t A T$ 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 $\text{diag}((\sqrt{a_{11}})^{-1}, \dots, (\sqrt{a_{kk}})^{-1}, 0, \dots, 0)$ eftersom vi arbetar över \mathbb{C} och kan hitta kvadratrötter. Här är k antalet nollskilda element på diagonalen.

Anmärkning. Notera att beviset här fungerar fram till sista steget för att bevisa motsvarande sats med reella koefficienter. Eftersom inte negativa reella tal har reella kvadratrötter är det bästa vi kan göra i reella fallet att skaffa ± 1 på diagonalelementen.

Anmärkning. Det enklaste sättet att finna denna form i både komplexa och reella fallen är normalt att göra 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 kvadratiske formen med hjälp av satsen ovan och sedan gör vi samma saker som i det reella beviset, förutom att vi alltså 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 affint 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 ('Dubbellingjen')

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. De 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 andragsgradskurvor 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 (överuppräknligt) 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 är 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 och geometri.

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. (Överkurs.)

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

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

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 $f : U \subset \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $f(z) = f(x + iy) = u(x, y) + iv(x, y) = (u(x, y), v(x, y)) = f(x, y)$. Detta framgår av följande sats.

Sats. Om f är komplext deriverbar uppfyller $u(x, y)$ och $v(x, y)$ Cauchy-Riemanns ekvationer $u_x = v_y$ och $u_y = -v_x$, dvs 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:

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

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

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 *geometrisk 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. $m = 2$:

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

Partiella derivator definieras på det uppenbara sättet.

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

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

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 $f: \mathbb{C}^2 \rightarrow \mathbb{C}$, men också som en funktion $f: \mathbb{R}^4 \rightarrow \mathbb{R}^2$. 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:

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

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 $\frac{\partial f}{\partial z} \neq 0$ eller $\frac{\partial f}{\partial w} \neq 0$ 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.

8.8 Några geometriska exempel.

Exempel. Betrakta kurvan C given av ekvationen $f(x, y) = 0$, där $f(x, y) = x - y^2$. Det är grafen till funktionen $x = p(y) = y^2$ och vi ska undersöka hur den beter sig. Gradienten är nollskild i alla punkter, så kurvan har inga singulariteter. Vi har två projektioner, en på varje koordinat, $p_1(x, y) = x$ och $p_2(x, y) = y$ och vi kommer att betrakta dem som funktioner från C till \mathbb{C} . p_2 är uppenbarligen en bijektion från C till \mathbb{C} . p_1 har egenskapen att Urbilden $p_1^{-1}(x)$ består av exakt två punkter om $x \neq 0$, men en punkt $(0, 0)$ om $x = 0$. Betrakta en cirkel $\gamma(t) = re^{it}$ kring origo i x -linjen. Föreställ dig att du vid tiden $t = 0$ befinner dig på C i (den reella) punkten (r, \sqrt{r}) och börjar gå på ett sådant sätt att du vid tiden t har x -koordinat $\gamma(t)$. Vid tiden $t = \pi/2$ är du i punkten $(re^{\pi/2}, \sqrt{re^{\frac{i\pi}{4}}})$, vid tiden $t = \pi$ i punkten

$(re^{i\pi}, \sqrt{r}e^{\frac{i\pi}{2}}) = (-r, i\sqrt{r})$ osv. När du har gått ett "varv", dvs. då $t = 2\pi$, är du inte tillbaka där du började utan i punkten $(r, -\sqrt{r})$. Du behöver gå ett helt varv till för att komma tillbaka till ändpunkten. Ytan är så att säga lindad "två varv" runt x -axeln. Betraktad på detta sätt brukar man referera till denna kurva som *Riemannytan* för den multipelvärdade "funktionen" \sqrt{x} .

Exempel. Betrakta följande tredjegradskurva C , $\lambda \in \mathbb{C} \setminus \{0, 1\}$:

$$y^2 = x(x-1)(x-\lambda).$$

Detta är $C = V(f)$ för $f(x, y) = y^2 - x(x-1)(x-\lambda)$. Beräknar vi $f_y = 2y$ så ser vi att eventuella singulära punkter på kurvan måste uppfylla $y = 0$ och därför ha $x = 0, x = 1$ eller $x = \lambda$. Men $f_x = (x-1)(x-\lambda) + x(x-\lambda) + x(x-1)$ som är nollskild i alla dessa punkter. Därför är denna kurva glatt. För de flesta punkter $x \in \mathbb{C}$ gäller att $\pi^{-1}(x)$ består av två punkter. Undantagen är $x = 0, x = 1$ och $x = \lambda$ som bara har en Urbild på C , nämligen $(0, 0), (1, 0)$ respektive $(\lambda, 0)$. För små värden på (x, y) nära $(0, 0)$ t.ex ser vi att $f(x, y) \approx y^2 - \lambda x$, vilket innebär att lokalt nära origo beter sig kurvan ungefär som grafen i förra exemplet. Detsamma gäller nära $(1, 0)$ respektive $(\lambda, 0)$. Projektionen p_2 på y -axeln har egenskapen att Urbilden $p^{-1}(y_0)$ i de flesta fall består av tre punkter. Undantagen är de punkter y_0 som är sådana att ekvationen

$$x(x-1)(x-\lambda) = y_0^2$$

har en multipelrot x .

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. T.ex. kommer vi att se att skärningsmultipliciteten mellan grafen $y = p(x)$ till ett envariabelpolynom $p(x)$ och x -axeln $y = 0$ i en punkt $(a, 0)$ är lika med multipliciteten hos a som ett nollställe till $p(x)$, så att detta nya begrepp generaliserar ett välkänt begrepp från inledande kurser i algebra. 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.

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 eller skärningstalet* mellan f och g i punkten P .

Axiom 0. Om $\mathbf{F} : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ är en affin transformation gäller

$$I_{\mathbf{F}^{-1}(P)}(f \circ \mathbf{F}, g \circ \mathbf{F}) = I_P(f, g).$$

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 för alla

typer av multipliciteter, transversella eller ej.

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.

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.

Anmärkning. Från och med nu kommer vi inte att hänvisa så noggrant till axiomnumren i våra argument. Vi lämnar åt läsaren att försäkra sig om att varje steg i härledningarna följer från axiomen.

Följande sats 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. Om a är ett nollställe av multiplicitet k kan vi skriva $p(x) = (x - a)^k v(x)$, där $v(a) \neq 0$. Vi har då

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

Nästa sats visar hur vi kan beräkna skärningstalet mellan två kurvor då en av kurvorna är en funktionsgraf. Beviset använder sig av satsen i slutet av 2.2, så passa på att lära dig beviset för denna nu.

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

Vi kommer understundom att använda beteckningen $\text{mult}_0 g(x, p(x))$ för nollställets multiplicitet.

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

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

Dessutom är $g(x, p(x)) = x^k v(x)$ där $v(0) \neq 0$. Vi kan nu beräkna skärningstalet som

$$\begin{aligned} I_0(f, g) &= I_0(y - p(x), q(x, y)(y - p(x)) + g(x, p(x))) = I_0(y - p(x), g(x, p(x))) = \\ &= I_0(y - p(x), x^k v(x)) = I_0(y - p(x), x^k) = k I_0(y, x) = k. \end{aligned}$$

Här har vi använt Axiom 5 för att eliminera $p(x)$. Detta är möjligt eftersom $p(0) = 0$ så alla termer innehåller en faktor x . Detta avslutar beviset.

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 . Faktoriserar

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

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. 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

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

där $h(0) = (a_1 - a_2)^{s_2} \cdot \dots \cdot (a_1 - a_\nu)^{s_\nu} \neq 0$, 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 . Om $a \neq a_i$ för alla i så blir $g(a, p(a)) \neq 0$, så $V(g)$ innehåller inte $(a, p(a))$ och skärningstalet är 0. I punkter utanför grafen $y = p(x)$ är förstås skärningstalet också 0. Detta avslutar beviset.

Anmärkning. Det är värt att notera att envariabelpolynomet $g(x, p(x))$ är g 's restriktion

till grafen till p .⁸ Meningen hos satsen är att skärningstalet återfås som multipliciteten hos nollställena till detta envariabelpolynom.

Vi bevisar nu att skärningstalet är entydigt om det existerar. Beviset innehåller en metod för beräkning av $I_P(f, g)$ i allmänhet.

Sats. Det finns maximalt en funktion $I_P(f, g)$ som uppfyller ovanstående axiom.

Bevis. Vi ska visa att axiomen är tillräckliga för att beräkna $I_P(f, g)$ för alla P, f, g . Beviset görs med induktion på $I_P(f, g)$.

Fallet då $I_P(f, g) = 0$ följer direkt från Axiom 2. Antag nu att $I_P(f, g)$ kan beräknas från axiomen om $I_P(f, g) < n$. Låt $I_P(f, g) = n > 0$. Då är $f(P) = g(P) = 0$. Efter en affin transformation kan vi anta att $P = (0, 0)$. Antag först att f innehåller faktorn y , så att $f(x, y) = yp(x, y)$. Då kan vi skriva

$$I_P(f, g) = I_P(yp, g) = I_P(y, g) + I_P(p, g).$$

Från satserna tidigare har vi att $I_P(y, g)$ kan beräknas som multipliciteten av 0 som nollställe till $g(x, 0)$. (Notera att $y = 0$ är grafen till nollpolynomet.) Denna är större än 0 eftersom $g(0, 0) = 0$. Om f inte har en faktor y så har f någon y -oberoende term. Antag att den högsta y -oberoende termen i f är x^r och att g 's högsta y -oberoende term är x^s . Vi kan anta att båda dessa är moniska (annars multiplicera polynomen med nollskilda tal) och att $r \leq s$ (annars byt roll på f och g i argumentet). Med axiom 5 har vi

$$I_P(f, g) = I_P(f, g - x^{s-r}f),$$

där den högsta y -oberoende termen i $h(x, y) = g(x, y) - x^{s-r}f(x, y)$ har grad $t < s$. Om denna process upprepas (vi kan behöva byta roll på f och g) så kommer till sist ett av polynomen att ha en faktor y och vi har bevisat att vi kan beräkna $I_P(f, g) = n$ från axiomen. Satsen följer nu från induktionsaxiomet.

Nästa sats bekräftar vad vi önskat oss, nämligen att skärningstalet 1 ska motsvara transversell skärning.

Sats. $I_P(f, g) = 1$ om och endast om f, g skär varandra transversellt i P .

Bevis. Vi kan anta att $P = (0, 0)$ efter en affin transformation och att $f(0, 0) = 0 = g(0, 0)$ eftersom motsatsen är ekvivalent med $I_P(f, g) = 0$.

Fall 1. Vi betraktar först fallet att något av polynomen har en faktor y . Vi kan anta att det är g så vi sätter $g(x, y) = yh(x, y)$. Då har vi från Axiom 4

$$I_P(f, g) = I_P(f, yh) = I_P(f, y) + I_P(f, h).$$

⁸Med standardparametriseringen $x \mapsto (x, p(x))$.

Vi vet att $I_P(f, y) \geq 1$ eftersom både $f(x, y)$ och y är 0 i P . Därför är $I_P(f, g) = 1$ ekvivalent med att både $I_P(f, h) = 0$ och $I_P(f, y) = 1$. Nu ska vi se att dessa villkor är ekvivalenta med transversalitet mellan f och g i P . Det första av dessa villkor är ekvivalent med att $h(P) \neq 0$, dvs. g kan skrivas

$$g(x, y) = h(P)y + \text{högre ordningens termer},$$

som är detsamma som att g är icke-singulär i P och har x -axeln som tangentlinje. $I_P(f, y) = 1$ är detsamma som att $x = 0$ är ett nollställe av multiplicitet 1 till $f(x, 0)$, vilket är ekvivalent med att f har en linjär del som är $ax + by$ där $a \neq 0$ (och alltså transversell mot x -axeln). Sammanfattningsvis är alltså påståendet

$$I_P(f, g) = 1 \iff f, g \text{ skär transversellt i } P$$

sant i fallet då ett av polynomen har en faktor y .

Fall 2. Antag nu att varken f eller g har en faktor y . Vi ska visa att vi kan ersätta f och g med, säg, f' och g' , så att

- (i) g' har en faktor y
- (ii) $I_P(f, g) = I_P(f', g')$
- (iii) f och g är transversella i $P \iff f'$ och g' är transversella i P .

Då kan vi använda Fall 1 och satsen följer på följande sätt. Om $I_P(f, g) = 1$ så är $I_P(f', g') = 1$ enligt (ii). Enligt Fall 1 är då f' och g' transversella i P och enligt (iii) gäller då detsamma f och g . Omvänt, om f och g är transversella i P så gäller enligt (iii) detsamma för f' och g' och enligt Fall 1 är $I_P(f', g') = 1$. Men enligt (ii) är då $I_P(f, g) = 1$.

Nu konstruerar vi f' och g' . Efter att möjligen ha multiplicerat f och g med nollskilda tal kan vi skriva $f(x, y) = x^m + p(x, y)$ där p inte innehåller några termer av typen ax^k där $k > m$, och $g(x, y) = x^n + q(x, y)$ på motsvarande sätt. Vi kan vidare u.f.a.a.⁹ anta att $m \leq n$. Notera nu att polynomet

$$k(x, y) = g(x, y) - x^{n-m}f(x, y) = x^n - x^{n-m}x^m + q(x, y) - x^{n-m}p(x, y) = q(x, y) - x^{n-m}p(x, y).$$

inte har några x -monom av grad n eller större. På grund av Axiom 5 gäller också

$$I_P(f, g) = I_P(f, g - x^{n-m}f) = I_P(f, k),$$

så vi kan ersätta g med k utan att förändra skärningstalet. Dessutom gäller att f är transversell med k om och endast om f transversell med g enligt diskussionen efter formuleringen av Axiom 5 i förra kapitlet. Upprepas denna process har vi till slut fått ett par av polynom f', g' där g' saknar y -oberoende termer och alltså har en faktor y . Vi kan därmed använda *Fall 1*. Detta avslutar beviset.

⁹Utan förlust av allmängiltighet. Jag medger att engelskans w.l.o.g., "without loss of generality", är mer vedertaget.

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:

- Beräkna skärningsmultipliciteten i origo, $I_0(f, g)$, av följande polynom. (Tagna ur [Bix]).
 - $f = y - x^3$ och $g = y^4 + 6x^3y + x^8$.
 - $f = y - x^2 - x$ och $g = y^2 - 3x^2y - x^2$.
 - $f = y^2 + x^2y - x^3$ och $g = y^2 + x^3y + 2x$
 - $f = y^5 - x^7$ och $g = y^2 - x^3$.
- 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.
 - $y = x^3 - 2x$, $s = 1$, $t = 1$.
 - $y^2 = x^3$, $s = 1$, $t = 1$.
 - $y^2 = x^4 + 4x^2$, $s = 2$, $t = 2$.
 - $y^2 = x^4 - 4x^2$, $s = 0$, $t = 2$.
- 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 rätta 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 $\mathbb{R}^3 \setminus \{0\}$.

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

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 parametreras 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 entydig 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 $(x, y) \rightarrow (x, y, 1)$.

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

Den del av $V(F)$ som ligger i en affin karta utgör en affin kurva i denna karta. Varje projektiv kurva har alltså flera affina representationer.

Definition. En *projektiv linje* är alla lösningar $(x, y, z) \in \mathbb{RP}^2$ 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 (entydiga) 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{RP}^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.

- (a) Givet två skilda projektiva punkter finns en entydig projektiv linje som går igenom dem.
- (b) Givet två skilda projektiva linjer finns en entydig projektiv punkt som ligger på båda.

Bevis.

- (a) Detta är en direkt omformulering av att två linjer genom origo bestämmer ett entydigt plan i \mathbb{R}^3 .
- (b) Detta är en direkt omformulering av att två plan genom origo skär varandra i en entydig linje i \mathbb{R}^3 .

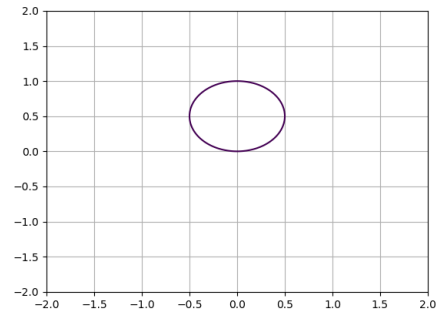
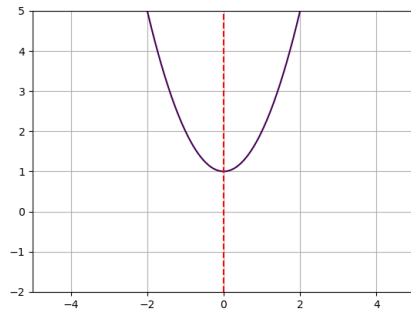


Figure 8: Den projektiva andragrad- Figure 9: Samma kurva betraktad skurvan $yz = x^2 + z^2$ i xy -kartan. Den i xz -kartan. Här syns alla kurvans streckade linjen indikerar punkten i ∞ . (reella) punkter.

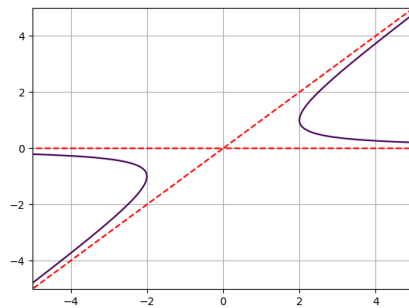


Figure 10: Och i yz -kartan. De streckade linjerna indikerar punkterna i ∞ , även om dessa inte syns i kartan.

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

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

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

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

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

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 linjär isomorfism

$$\mathbf{F} : \mathbb{R}^3 \rightarrow \mathbb{R}^3, (x, y, z) \mapsto \mathbf{F}(x, y, z)$$

inducerar en avbildning $F_P : \mathbb{R}P^2 \rightarrow \mathbb{R}P^2$ genom samma formel $F_P(x, y, z) = \mathbf{F}(x, y, z)$ applicerad på homogena koordinater. Denna avbildning är väldefinierad eftersom den linjära avbildningen \mathbf{F} saknar nollrum och därför tar linjer genom origo till linjer genom origo. En

avbildning $F_P : \mathbb{R}P^2 \rightarrow \mathbb{R}P^2$ som på detta sätt kommer från en linjär isomorfism kallas en *projektiv transformation* och vi betecknar ofta F_P med F om inga missförstånd riskerar att uppstå.

Exempel 1. Om \mathbf{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 \mathbf{F} ges av

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

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

$$(x, y) \mapsto (ax + bx, cx + dy),$$

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) :

$$(x, y) \mapsto (x + h, y + k)$$

Exempel 3. Beteckna med L_∞ den projektiva linjen $z = 0$. En projektiv transformation F given av matrisen

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

uppfyller $F(L_\infty) = L_\infty$ om och endast om $ex + fy = 0$ för alla x, y , så att $e = f = 0$, dvs. transformationen är affin i xy -kartan. Den fixerar L_∞ punktvis, dvs $F(a, b, c) = (a, b, c)$ för alla $(a, b, c) \in L_\infty$ om och endast om den i xy -kartan är sammansättning av en ren translation och en

homoteti, (dvs. en övergripande skalning $(x, y) \mapsto (\lambda x, \lambda y)$) . Att kontrollera dessa påståenden lämnas till läsaren. (Se övningarna nedan.)

Exempel 4. Om \mathbf{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 -koordinatplanen. 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 ut 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 $\text{Proj}(2)$ 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.(Fyrapunktssatsen.) Givet fyra projektiva punkter $z_1, z_2, z_3, z_4 \in \mathbb{R}P^2$ sådana att det inte finns tre av dem som är kolinjära, och givet $w_1, w_2, w_3, w_4 \in \mathbb{R}P^2$ med samma egenskap, finns en entydig projektiv transformation $F : \mathbb{R}P^2 \rightarrow \mathbb{R}P^2$ sådan att $F(z_i) = w_i$ för alla $i = 1, \dots, 4$.

Bevis. Representera de givna punkterna med vektorer i \mathbb{R}^3 , $\mathbf{z}_1, \dots, \mathbf{z}_4$ och $\mathbf{w}_1, \dots, \mathbf{w}_4$. Villkoret om kolinjaritet betyder att varje deltrippel av \mathbf{z}_i :n är linjärt oberoende, och detsamma gäller för \mathbf{w}_i . Därför utgör t.ex. $\mathbf{z}_1, \dots, \mathbf{z}_3$ en bas för \mathbb{R}^3 och \mathbf{z}_4 kan skrivas som en entydig linjärkombination

$$\mathbf{z}_4 = \sum_{i=1}^3 a_i \mathbf{z}_i.$$

På samma sätt kan \mathbf{w}_4 skrivas

$$\mathbf{w}_4 = \sum_{i=1}^3 b_i \mathbf{w}_i.$$

Notera att inga av a_i och b_i kan vara 0. Om t.ex. $a_1 = 0$ skulle vi nämligen ha $\mathbf{z}_4 = a_2 \mathbf{z}_2 + a_3 \mathbf{z}_3$ så $\mathbf{z}_2, \dots, \mathbf{z}_4$ skulle vara linjärt beroende. Definiera $\mathbf{F} : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ genom

$$\mathbf{F}(\mathbf{z}_i) = \frac{b_i}{a_i} \mathbf{w}_i, \quad i \in \{1, \dots, 3\}.$$

Då gäller

$$\mathbf{F}(\mathbf{z}_4) = \sum_{i=1}^3 a_i \mathbf{F}(\mathbf{z}_i) = \sum_{i=1}^3 a_i \frac{b_i}{a_i} \mathbf{w}_i = \sum_{i=1}^3 b_i \mathbf{w}_i = \mathbf{w}_4.$$

Detta visar att det finns en sådan projektiv transformation som efterfrågas. För att visa entydigheten, låt $\mathbf{G} : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ vara en annan linjär avbildning med den önskade egenskapen. Då är $\mathbf{G}(\mathbf{z}_i) = \lambda_i \mathbf{w}_i$ för några λ_i , $i = 1, \dots, 4$ och därför är, å ena sidan,

$$\mathbf{G}(\mathbf{z}_4) = \sum_{i=1}^3 a_i \mathbf{G}(\mathbf{z}_i) = \sum_{i=1}^3 a_i \lambda_i \mathbf{w}_i,$$

och å andra sidan är

$$\mathbf{G}(\mathbf{z}_4) = \lambda_4 \mathbf{w}_4 = \sum_{i=1}^3 \lambda_4 b_i \mathbf{w}_i.$$

Vi ser att detta medför att $\lambda_i = \lambda_4 \frac{b_i}{a_i}$, $i=1, \dots, 3$. Det följer att $\mathbf{G} = \lambda_4 \mathbf{F}$ och att \mathbf{F} och \mathbf{G} därför definierar samma projektiva transformation. Detta avslutar beviset av entydigheten.

Korollarium. Låt $P, Q \in \mathbb{R}P^2$. Då finns en projektiv transformation som tar P till Q . Låt $P, P', Q, Q' \in \mathbb{R}P^2$. Då finns en projektiv transformation som tar P till Q och P' till Q' . Låt $P, P', P'' \in \mathbb{R}P^2$ vara icke-kolinjära och låt detsamma gälla Q, Q', Q'' . 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 $\mathbb{R}_d^h[x, y, z] \subset \mathbb{R}[x, y, z]$ mängden av homogena polynom av grad d i tre variabler. (Notera att detta inte är en ring, eftersom summan av två homogena polynom av olika grad inte är ett homogent polynom.) En linjär transformation \mathbf{F} inducerar en ringisomorfism $\mathbf{F}^* : \mathbb{R}[x, y, z] \rightarrow \mathbb{R}[x, y, z]$ via $\mathbf{F}^*(f) = f \circ \mathbf{F}$, enligt avsnittet om affina transformationer.

Sats. Om $f \in \mathbb{R}_d^h[x, y, z]$ så $\mathbf{F}^*(f) \in \mathbb{R}_d^h[x, y, z]$.

Bevis. Eftersom \mathbf{F} är linjär och bijektiv bevarar den både grad och homogenitet.

Definition. Två homogena polynom $f, g \in \mathbb{R}_h[x, y, z]$ kallas *projektivt ekvivalenta* om det finns en linjär transformation $\mathbf{F} : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ så att $\mathbf{F}^*(f) = \pm g$.

Sats. Projektiv ekvivalens är en ekvivalensrelation på $\mathbb{R}_h[x, y, z]$.

Bevis. Följer från motsvarande påstående i affina fallet.

Övningar.

1. Skriv ned uttrycket för en allmän projektiv transformation i xy -kartan.
2. Visa påståendena i Exempel 3. om L_∞ .
3. Visa att polynomen $x^2 + yz$ och $4x^2 + 4yz$ är projektivt ekvivalenta.
4. Hur kan bilden av en kvadrat se ut under en affin transformation av planet?
5. Hur kan bilden av en kvadrat se ut under en projektiv transformation?
6. Ange en projektiv transformation som tar punkten $(1, 1, 1)$ till punkten $(0, 2, 3)$.
7. Ange en projektiv transformation som tar linjen $2x + 3y + z = 0$ till linjen $3x + y + z = 0$.
8. Beskriv alla projektiva transformationer som tar punkterna $(1, 1, 0)$, $(1, 0, 1)$, $(0, 1, 1)$ till punkterna $(1, 0, 0)$, $(0, 1, 0)$ resp. $(0, 0, 1)$.
9. Ange den projektiva 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+1} ger med liknande konstruktion som ovan projektiva rum $\mathbb{R}P^n$ 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 $(x, y) \in \mathbb{R}^2$ 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 entydigt 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 \mathbf{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. (Överkurs.)

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

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

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:

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

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 andragskurvor.

En projektiv andragskurva har utseendet

$$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0.$$

Precis som i det affina fallet är det lämpligare att betrakta homogena andragsgradspolynom 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 $(3, 0)$ (e), $(2, 1)$ (a), $(2, 0)$ (c), $(1, 1)$ (b) eller $(1, 0)$ (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 (exemplet $yz = x^2 + z^2$) visar att de tre irreducibla kurvorna ellips, hyperbel och parabel är projektivt ekvivalenta samt att kurvan $(x-c)(x+c)$ i xy -planet som består av två parallella linjer är projektivt ekvivalent med ett linjekors $(x-cz)(x+cz)$. Notera att ekvationen $x^2 + 1$ har en projektiv lösning i L_∞ och är projektivt ekvivalent med $x^2 + y^2$.

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{CP}^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 om 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{CP}^2 som mängden av alla projektiva punkter vars homogena z -koordinat är nollskild. Eftersom varje sådan punkt har en entydig representant av formen $(x, y, 1)$ kan denna mängd naturligt identifieras med det komplexa xy -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{CP}^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{CP}^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{CP}^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{CP}^1 .

Det enklaste exemplet på ett komplext projektivt rum är den komplexa projektiva linjen, \mathbb{CP}^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{CP}^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 entydigt 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{CP}^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{CP}^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. (Överkurs.)

Ordagrant samma definition som i reella fallet kan användas för att definiera dubbelförhållandet av fyra punkter på \mathbb{CP}^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{CP}^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{CP}^1 istället för på en cirkel \mathbb{RP}^1 .

I övningarna nedan ser vi att projektiva transformationer av \mathbb{CP}^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{CP}^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 $\mathbf{F} : \mathbb{C}^3 \rightarrow \mathbb{C}^3$ inducerar en avbildning $F_P : \mathbb{CP}^2 \rightarrow \mathbb{CP}^2$ eftersom \mathbf{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 $\mathbf{F} : \mathbb{C}^3 \rightarrow \mathbb{C}^3$ 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: $F_P = (\lambda F)_P$.

Sats. Det finns exakt en projektiv linje i \mathbb{CP}^2 upp till projektiva transformationer.

Bevis. Varje komplext plan genom origo kan tas till varje annat komplext plan genom en linjär isomorfism $\mathbb{C}^3 \rightarrow \mathbb{C}^3$.

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 Komplex 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 irreducibel och glatt, medan (b) och (c) är reducibla och har singulariteter.

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

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

(c) x^2 (Dubbellinge.)

Bevis. Detta är omedelbart från den komplexa klassificeringen av kvadratiske 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: $\text{diag}(1, 1, 1)$, $\text{diag}(1, 1, 0)$ eller $\text{diag}(1, 0, 0)$.

Anmärkning. Vi ser att det finns exakt en icke-singulär plan komplex projektiv andragradskurva.

11.5 Skärningstalet återbesökt.

Här redigerar vi axiomen för skärningstalet så att det fungerar väl för projektiva kurvor och deras transformationer.

Definition. Skärningstalet $I_P(F, G)$ mellan två projektiva kurvor i en punkt P definieras som det affina skärningstalet i någon affin karta som innehåller P .

Anmärkning. Det är inte klart apriori att detta är oberoende av valet av karta. För att råda bot på detta ersätter vi från och med nu Axiom 0 med invarianten under *projektiva transformationer*. Dvs.

Nytt Axiom 0. Om $\mathbf{F} : \mathbb{CP}^2 \rightarrow \mathbb{CP}^2$ är en projektiv transformation gäller

$$I_{\mathbf{F}^{-1}(P)}(F \circ \mathbf{F}, G \circ \mathbf{F}) = I_P(F, G).$$

Vi har redan sett att kartbyten ges av projektiva transformationer, så detta gör definitionen ovan meningsfull.

Problem. Betrakta den projektiva kurva $C \subset \mathbb{CP}^2$ som i xy -kartan ges av ekvationen

$$x^3 - 3x^2y + 2xy - 4y - 10 = 0$$

Bestäm de punkter där C skär L_∞ och bestäm skärningstalet i dessa.

Lösning. En homogen ekvation för C ges av homogeniseringen

$$x^3 - 3x^2y + 2xyz - 4yz^2 - 10z^3 = 0$$

Skärningspunkterna med L_∞ ges av $z = 0$ och

$$x^3 - 3x^2y = x^2(x - 3y) = 0.$$

Dessa ekvationer ger lösningarna $x = 0, y$ godtycklig respektive $x = 3y, y$ godtycklig är den andra. Homogena koordinater är $(0, 1, 0)$ respektive $(3, 1, 0)$. Båda dessa punkter ligger i xz -kartan, med koordinater $P_1 = (0, 0)$ respektive $P_2 = (3, 0)$ så vi väljer att beräkna skärningstalen där. I xz -kartan ser C ut som

$$g(x, z) = x^3 - 3x^2 + 2xz - 4z^2 - 10z^3 = 0$$

Vi behöver alltså beräkna $I_{P_i}(z, x^3 - 3x^2 + 2xz - 4z^2 - 10z^3)$. Notera att $z=0$ är grafen till envariabelpolynomet $p(x) = 0$. Enligt en sats i avsnitt 9.2 ges multipliciteterna av de olika multipliciteterna av nollställena till

$$g(x, 0) = x^2(x - 3).$$

Vi ser att $(0, 0)$ har multiplicitet 2 och $(3, 0)$ multiplicitet 1. Notera att alla skärningspunkter i \mathbb{CP}^2 faktiskt är i \mathbb{RP}^2 .

Övningar.

- 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.
- 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.
- Bestäm de komplexa projektiva punkter $P \in \mathbb{CP}^2$ 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{RP}^2 .
 - $f(x, y) = 2x^2 + 4y^2 - 1, g(x, y) = x^2 - 4y^2 - 2.$
 - $f(x, y) = y - x^3, g(x, y) = y^2 - x^4.$
- 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 .
- Betrakta den komplexa plana projektiva kurva som i den affina xy -kartan ges av ekvationen

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

- Ange kurvans singulära punkter.
- Bestäm de generaliserade tangentlinjerna.
- Bestäm homogena koordinater för de punkter där kurvan skär linjen i ∞, L_∞ .
- 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, nämligen Bezouts sats. Men först en definition.

Definition. Låt $F, G \in \mathbb{C}_h[x, y, z]$. Det *totala skärningstalet* $I(F, G)$ definieras som summan av alla skärningstal mellan kurvorna

$$I(F, G) = \sum_{P \in V(F) \cap V(G)} I_P(F, G).$$

Notera att summan är ändlig så länge kurvorna inte har någon gemensam faktor. Annars tolkar vi förstås summan som ∞ .

Sats (Bezout) Låt $F, G \in \mathbb{C}_h[x, y, z]$ 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.

12.1 Lemma 1. Fallet då en av kurvorna är en linje.

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 den sats som vi tidigare bevisade om skärningstalet då en av kurvorna är en graf.

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 $L = y$. 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

$d = s_1 + \dots + s_\nu$ av polynomet

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

(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.

12.2 Lemma 2. y -oberoende faktorer kan ignoreras.

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 (se kapitlet), för vilka Bezouts sats gäller enligt Lemma 1. Låt $\text{Bez}(F, G)$ 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

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

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

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

enligt Lemma 2. Vidare har vi

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

Vi ser direkt från detta följande ekvivalens mellan två påståenden:

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

dvs.

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

vilket var vad ville bevisa.

12.3 Lemma 3. Reduktion av y -graden.

Det sista lemmat låter oss successivt reducera y -graden tills ett av polynomen är y -oberoende.

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

$$\text{Bez}(F, G) \iff \text{Bez}(F_1, G_1).$$

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 räkneregler för skärningstal har vi

$$\begin{aligned} \text{Bez}(F, G) = \text{Bez}(F, G_1H) &\iff \text{Bez}(F, G_1) \iff \\ &\iff \text{Bez}(QF, G_1) \iff \text{Bez}(QF - Py^{s-t}G_1, G_1) \iff \text{Bez}(F_1, G_1). \end{aligned}$$

vilket var vad ville bevisa.

12.4 Beviset avslutas.

Nu är det bara slutklämman kvar.

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,

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

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 förstegradspolynom

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

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{CP}^2 .¹⁰ 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) :

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

¹⁰Så 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?

vilket minskar dimensionen till två, dvs. det linjära rummet

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

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 Lösningssrummets

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

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. Fem punkter innebär fem linjära ekvationer, så med samma sorts resonemang som ovan, borde fem punkter definiera en entydig andragradskurva. Det är det ungefärliga innehållet i följande sats. Det krävs även här ett geometriskt antagande för att garantera att villkoren är "tillräckligt oberoende".

Sats. Antag att $P_1, \dots, P_5 \in \mathbb{C}P^2$ är givna och att det inte finns fyra av dem som är kolinjära. Då finns en entydig andragradskurva C som går igenom dem alla. Om inte ens tre av dem är kolinjära är C irreducibel.

Bevis. Att det finns som mest en sådan andragradskurva följer från Bezouts sats. Om nämligen F, G är två sådana andragradskurvor utan gemensamma faktorer är $I(F, G) = 4$, men fem skärningspunkter skulle innebära $I(F, G) \leq 5$, vilket är en motsägelse. Om F, G skulle ha en gemensam faktor och inte sammanfalla, skulle de båda vara linjekors och alla fem punkterna måste ligga på den gemensamma linjen, vilket är en motsägelse.

Om tre av punkterna är kolinjära, ligger de på en entydig linje L . De övriga två ligger då på en annan linje L' så $C = L \cup L'$ är den önskade kurvan.

Antag nu att inte ens tre av punkterna är kolinjära. 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

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

och definiera

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

Det följer att $Q(P_i) = 0$ för $i = 1, \dots, 5$. Sätt $C = V(Q)$.

Eftersom en reducibel andragradskurva består av en eller två linjer, kan C bara gå igenom P_1, \dots, P_5 om en av linjerna innehåller minst tre punkter, vilket inte är fallet. Detta visar att C 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 $V(F)$.

Vi påminner här om följande användbara lemma.

Eulers lemma om homogena funktioner. Om $F(x, y, z)$ är en homogen funktion av grad d , gäller

$$a \frac{\partial F}{\partial x}(a, b, c) + b \frac{\partial F}{\partial y}(a, b, c) + c \frac{\partial F}{\partial z}(a, b, c) = dF(a, b, c)^{11}.$$

Anmärkning. En projektiv punkt är singulär om och endast om den är singulär i någon affin karta. För en punkt som t.ex. ligger i xy -kartan, $P = (a, b, 1)$ har vi nämligen enligt Eulers lemma

$$\begin{aligned} \frac{\partial F}{\partial z}(a, b, 1) &= dF(a, b, 1) - a \frac{\partial F}{\partial x}(a, b, 1) - b \frac{\partial F}{\partial y}(a, b, 1) = \\ &= 0 - a \frac{\partial f}{\partial x}(a, b) - b \frac{\partial f}{\partial y}(a, b). \end{aligned}$$

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 .

Nästa sats ger en begränsning på hur många singulära punkter en kurva av grad d kan ha. Beviset sker genom dimensionsräkning. Vi inleder med några exempel och visar sedan satsen i sin helhet.

Exempel. (*Grad 1 och 2.*) En irreducibel kurva av grad 1 är en linje så den har inga singulära punkter. En irreducibel andragsgradskurva är ekvivalent med cirkeln, så saknar också singulära punkter.

¹¹Beviset är en rättfram övning: En funktion $F(x, y, z)$ kallas 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.

Exempel. (*Grad 3.*) Det första intressanta exemplet är således i grad 3, där vi redan tidigare sett singulära irreducibla exempel. Om C är en irreducibel tredjegradskurva och P och Q är två singulära punkter på C så kan vi betrakta linjen L igenom P och Q . Eftersom C är irreducibel kan L och C bara ha gemensamma komponenter om $C = L$, men detta är förstas omöjligt (C och L har ju olika grad.) Bezouts sats säger då att $I(C, L) = 3$, men eftersom $I_P(C, L) \geq 2$ och $I(Q, L) \geq 2$ så är detta en motsägelse. Det kan alltså inte finnas mer än en singulär punkt på C .

Exempel. (*Grad 4.*) Antag att C är en irreducibel fjärdegradskurva och att den har 4 singulära punkter P_1, \dots, P_4 . Låt oss försöka med en metod liknande den i förra exemplet. Vi kan hitta en andragradskurva C' som går genom alla punkterna, eftersom rummet av andragradspolynom är sexdimensionellt och villkoren som punkterna ställer på koefficienterna utgör bara fyra homogena linjära ekvationer i sex obekanta. Återigen är $C \neq C'$ så Bezouts sats säger att $I(C, C') = 8$. Men nu ger detta inte en motsägelse, det skulle ju kunna vara möjligt att ha $I_P(C, C') = 2$ i alla skärningspunkterna. Vi kan dock modifiera vår approach. Notera att vi faktiskt har utrymme för att ställa ett villkor till. Vi hade sex variabler och fyra ekvationer och därför en icke-trivial lösning, men det hade funkat med fem ekvationer också. Vi plockar därför en punkt $P_5 \in C$, som nu inte nödvändigtvis är singulär. Då kommer vi att ha C' igen som ovan, men nu får vi även ett bidrag på minst 1 ifrån P_5 också. Detta ger den önskade motsägelsen: $8 = I(C, C') \geq 9$. Det kan alltså inte finnas mer än tre singulära punkter på C .

Nu bevisar vi den allmänna satsen.

Sats. En irreducibel projektiv kurva $C \subset \mathbb{C}^2$ 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 vektorrum¹² av dimension $\binom{d}{2}$ (= antalet koefficienter)¹³. 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 $C = C'$, eftersom C är irreducibel. Men C' och C har olika grad, 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

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

vilket är en motsägelse.

13.3 Reella algebraiska kurvor och deras ovaler. (Överkurs.) **Ej skrivet än.**

Sats.(Harnack)

14 Tredjegradskurvor

14.1 Hessianen och inflexionspunkter.

Definition. Låt $F(x, y, z)$ vara ett polynom av grad d . Beteckna med $F_{xy} = \frac{\partial^2 F}{\partial x \partial y}$ 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. Låt $F \in \mathbb{C}_h[x, y, z]$. En (projektiv) punkt $P = (a, b, c)$ på kurvan $F(x, y, z) = 0$ kallas en *inflexionspunkt* (eller *flex*) om den är icke-singulär och $H(a, b, c) = 0$.

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.

¹²Ätminstone om nollpolynomet tillfälligtvis får betraktas som homogent av varje grad.

¹³Detta lämnar vi till studenten som en liten övning.

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

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

Bevis. Eulers lemma om homogena funktioner säger att

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

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

$$(d-1)F_x = xF_{xx} + yF_{xy} + zF_{xz} \quad (2)$$

$$(d-1)F_y = xF_{yx} + yF_{yy} + zF_{yz} \quad (3)$$

$$(d-1)F_z = xF_{zx} + yF_{zy} + zF_{zz} \quad (4)$$

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)

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

Om denna ekvation nu multipliceras med z får vi

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

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

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

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

Anmärkning. Med hjälp av detta Lemma kan vi nu se den utlovade relationen till vanliga inflexionspunkter. Vi börjar med att beräkna följande determinant, som enligt vårt Lemma är proportionell mot Hessianen i en punkt på formen $(x, y, 1)$, på kurvan $F = 0$ enligt

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

Betrakta en projektiv kurva $F(x, y, 1) = 0$ i den affina xy -kartan. Antag att $F_y(P) \neq 0$, så att $y = y(x)$ lokalt kring P , enligt implicita funktionssatsen. 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 efter en del förenklingar skriva

$$y''(x) = \frac{2F_xF_yF_{xy} - F_y^2F_{xx} - F_x^2F_{yy}}{F_y^3}.$$

Men täljaren i detta uttryck är precis determinanten ovan, så vi får

$$y''(x) = \frac{H(x, y, 1)}{(F_y)^3(d-1)^2}.$$

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

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

Bevis. Antag först att F och H saknar gemensamma faktorer. Eftersom $\deg(F) = d$ och $\deg(H) = 3(d-2)$ så är antalet inflexionspunkter räknade med multiplicitet enligt Bezouts sats $I(F, H) = 3d(d-2)$. Påståendet i satsformuleringen följer direkt från detta. Om F och H har en gemensam faktor måste $F|H$, eftersom F är irreducibel. Det följer att $H(P) = 0$ så fort $F(P) = 0$ så alla punkter på F är inflexionspunkter. Men då måste F vara en linje, vilket vi kan se på följande sätt. Se till att $F_y(P) \neq 0$ genom en lämplig projektiv transformation. Då kommer det i xy -kartan finnas en öppen omgivning U av P där kurvan kan beskrivas som $y = y(x)$. Enligt anmärkningen ovan är för alla punkter i denna omgivning $y'' = 0$. Denna differentialekvation har lösningen $y(x) = kx + m$ i U så snittet mellan kurvan och U innehåller ett linjesegment. Men en irreducibel algebraisk kurva F som sammanfaller med en linje L i oändligt många punkter uppfyller $F = L$.

Sats. Låt $F \in \mathbb{C}_h[x, y, z]$ ha grad d . Beteckna med $T_P(F)$ tangentlinjen i punkten P ¹⁴. Då gäller:

$$P \text{ är en inflexionspunkt till } F \iff I_P(F, T_PF) \geq 3.$$

Bevis. Efter en projektiv transformation kan vi anta att P motsvarar punkten $(0, 0)$ i xy -kartan och att $F_y(0, 0) \neq 0$. Vi har redan sett i anmärkningen ovan att P är en inflexionspunkt om och endast om

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

¹⁴Speciellt antar vi alltså att P inte är singulär.

Med notationen $F(x, y, 1) = f(x, y)$ har vi alltså att $(0, 0)$ är en inflexionspunkt om och endast om

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

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

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

(åter är alla derivator underförstått uträknade i $(0, 0)$). $T_P F$ ges av $y = -\frac{f_x}{f_y}x$, som är en graf, så skärningstalet ges av multipliciteten

$$I_P(T_P F, F) = I_{(0,0)}(f, T_{(0,0)}f) = \text{mult}_0 f(x, -\frac{f_x}{f_y}x).$$

En rättfram räkning ger nu

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

Vi ser att skärningstalet är större än 3 om och endast om P är en inflexionspunkt. Detta avslutar beviset.

14.2 Klassificering av glatta projektiva tredjegradskurvor

Vi inför härmed beteckningen *glatt* kurva som en stavelsebesparande synonym till en kurva utan singulära punkter. Vi har redan sett att glatta andragsgradskurvor alla är projektivt ekvivalenta.¹⁵ 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. Vi kan flytta den till $(0, 1, 0)$ efter en lämplig projektiv transformation¹⁶. Vi kan också se till att tangentlinjen till C är linjen $z = 0$. Då ges C av $F(x, y, z) = 0$, där $F(0, 1, 0) = 0 = F_x(0, 1, 0) = F_y(0, 1, 0) = H(0, 1, 0)$. Om vi i lemmat i förra kapitlet byter roll på y och z och sätter $d = 3$ får vi följande uttryck för Hessianen.

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

¹⁵I fallet med andragsgradskurvor är alla irreducibla kurvor glatta, vilket inte är fallet för kurvor av högre grad.

¹⁶Projektiva transformationer avbildar inflexionspunkter till inflexionspunkter: En övning till en senare lektion.

I inflexionspunkten $(x, y, z) = (0, 1, 0)$ är detta

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

Men $F_z(0, 1, 0) \neq 0$, eftersom $(0, 1, 0)$ annars vore en singular punkt, så vi måste ha

$$F_{xx}(0, 1, 0) = 0.$$

Observera att polynomet $F_{xx}(x, y, z)$ är av grad 1, eftersom F är av grad 3. $F_{xx}(0, 1, 0) = 0$ betyder då att F_{xx} är oberoende av y :

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

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 (vi döper om koefficienterna):

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

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

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

där $h(x, z)$ är ett samlingsnamn för alla y -oberoende termer. 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 avbildningen

$$\mathbf{F}(x, y, z) = (x, y - \frac{ax + cz}{2b}, z)$$

transformerar nu vårt polynom till formen

$$F(x, y, z) = bzy^2 + H(x, z),$$

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. Vi kan således efter en omskalning av variablerna x, y, z skriva ekvationen $F = 0$ som

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

där a, b, c är olika eftersom kurvan annars är singulär¹⁷. Nu ger transformationen

$$\mathbf{F}(x, y, z) = (x + az, y, z)$$

ekvationen

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

Låt η vara någon rot till $\eta^2 = b - a$ och sätt $\lambda = \frac{c - a}{b - a}$. Då får vi till slut, efter den diagonala transformationen

$$\mathbf{F}(x, y, z) = \left(x, \eta y, \frac{z}{b - a} \right),$$

att

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

Detta avslutar beviset.

Anmärkning. Denna sats visar att man alltid kan reducera en icke-singulär tredjegradskurva till denna standardform för något värde på parametern λ . För en fullständig projektiv klassificering måste man också beskriva exakt vilka av dessa λ som beskriver ekvivalenta kurvor. 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{CP}^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

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

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.

Övningar.

1. Visa att kurvan

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

är glatt om och endast om alla a, b, c är olika.

¹⁷Detta lämnas som övning åt läsaren att kontrollera.

2. Visa att om

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

så är $\nabla F(0, 1, 0) = (0, 0, 1)$ och $\nabla H_F(0, 1, 0) = (24, 0, 8(\lambda - 1))$.

3. Visa att projektiva transformationer tar inflexionspunkter till inflexionspunkter.

14.3 Klassificering av singulära tredjegradskurvor.

Vi såg i förra kapitlet att det finns en familj av glatta tredjegradskurvor parametrerad av en komplex parameter λ . När det gäller singulära 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

$$\begin{aligned} p(x, y) &= x^3 + bx^2y + cxy^2 + dy^3 = x^3 + bx^2y + (3\beta^2xy^2 + \beta^3y^3) - (3\beta^2xy^2 + \beta^3y^3) + cxy^2 + dx^2y = \\ &= (x + \beta y)^3 + y^2((c - 3\beta^2)x + (d - \beta^3)y) = (x + \beta y)^3 + y^2(Ax + By). \end{aligned}$$

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

$$\begin{aligned} p(x, y) &= x^3 + bx^2y + cxy^2 + dy^3 = x^3 + (3\beta x^2y + 3\beta^2xy^2) + dy^3 - (3\beta x^2y + 3\beta^2xy^2) + bx^2y + cxy^2 \\ &= (x + \beta y)^3 + xy((b - 3\beta)x + (c - 3\beta^2)y) = (x + \beta y)^3 + xy(Ax + By). \end{aligned}$$

Sats. Låt C vara en singulär irreducibel tredjegradskurva i \mathbb{CP}^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 z^2 -termer. Detta kan vi inse t.ex. genom att Maclaurinutveckla i xy -kartan. Avsaknad av z^3 -term motsvarar då avsaknad av konstantterm i Maclaurinutvecklingen och avsaknad av z^2 -term motsvarar avsaknad av linjära termer. 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 $\mathbf{F}(x, y, z) = (x, y - ax, z)$ och ekvationen får då 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 $\mathbf{F}(x, y, z) = (x, y, z + Ax + By)$, så att ekvationen får utseendet $y^2z = (x + \beta y)^3$. Sätter vi nu bara $\mathbf{F}(x, y, z) = (x - \beta y, y, z)$ så får vi ekvationen

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

Fall B. I det andra fallet gör vi först variabelbytet

$$\mathbf{F}(x, y, z) = (y - bx, y - ax, z)$$

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 $\mathbf{F}(x, y, z) = (x, y, Ax + By + z)$ som ger ekvationen formen

$$xyz = (x + \beta y)^3.$$

Här kan vi göra variabelbytet $\mathbf{F}(x, y, z) = (x, y/\beta, \beta z)$ (observera att $\beta \neq 0$ av irreducibilitetsskäl), och få

$$xyz = (x + y)^3.$$

Nu gör vi till sist variabelbytet $\mathbf{F}(x, y, z) = (x + y, x - y, -8z)$, vilket ger

$$(y + x)(y - x)8z = 8x^3 \iff y^2z = x^2(x + z).$$

Detta avslutar beviset.

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 sammanfalla menar vi med detta att linjen är tangentlinjen i P . Enligt Bezouts sats skär linjen kurvan C i en tredje punkt. Kalla denna punkt för $P * Q$. Det kan åter hända att denna sammanfaller med P eller Q (eller båda), i vilket fall linjen är tangentlinjen i denna punkt. Upprepa nu allt detta med punkterna O och $P * Q$ för att bilda $O * (P * Q)$, 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: $P + Q = Q + P$.
- (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 $P \mapsto P + (O' - O)$ är en gruppisomorfism från (C, O) till (C, O') .

Anmärkning. Notera att $*$ -operationen inte har samma goda egenskaper, t.ex. är den inte associativ. Den är bara en hjälp för att definiera $+$.

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 rummet V_3 som består av homogena polynom av grad $d - 2$ uppfyller

$$\dim_{\mathbb{C}} V_3 = \binom{d}{2}.$$

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. Kom också ihåg att när vi tänker på polynom istället för kurvor får vi en dimension extra (λp och p har samma nollställen), så det rum som satsen handlar om är av dimension 1, om vi tänker på de kurvor som polynomen motsvarar.

Lemma 1. Låt åtta punkter P_1, \dots, P_8 vara givna. Definiera vektorrummet

$$V_3(P_1, \dots, P_8) = \{F \in \mathbb{C}_h[x, y, z] \mid F(P_i) = 0, i = 1, \dots, 8\}.$$

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 andragsgradskurva.

Då är rummet $V_3(P_1, \dots, P_8)$ tvådimensionellt.

Bevis. Eftersom varje punkt svarar mot ett homogent linjärt villkor på de tio koefficienterna till ett tredjegradspolynom, vet vi från början att

$$\dim_{\mathbb{C}} V_3(P_1, \dots, P_8) \geq 2.$$

Vi delar upp i tre fall.

Fall 1. I detta fall gör vi det starkare antagandet att inte ens tre punkter är kolinjära och att inte ens sex av dem ligger på samma irreducibla andragsgradskurva. Låt oss anta, för att sedermera nå en motsägelse, att

$$\dim_{\mathbb{C}} V_3(P_1, \dots, P_8) \geq 3.$$

Låt $L = 0$ vara en linje genom två av punkterna, säg P_7 och P_8 . Specificera ytterligare två (från de övriga punkterna distinkta) punkter P_9 och P_{10} på L . Dessa tillför två homogena villkor till så vi har att

$$\dim_{\mathbb{C}} V_3(P_1, \dots, P_{10}) \geq 1.$$

Tag $0 \neq F \in V_3(P_1, \dots, P_{10})$. Om L och F inte har gemensamma faktorer är $I(F, L) \geq 4$, eftersom $F(P_i) = L(P_i) = 0$, $i = 7, \dots, 10$. Enligt Bezouts sats är dock $I(F, L) = 3$. Alltså har L och F gemensamma faktorer. Eftersom L är irreducibel betyder detta att $F = LG$ för något andragradspolynom G . L kan inte gå igenom någon av punkterna P_1, \dots, P_6 eftersom det motsäger kolinjäritetsantagandet (L går redan igenom P_7 och P_8 , som du minns). Alltså går $G = 0$ igenom dessa punkter. Notera att eftersom G går igenom P_1, \dots, P_5 och inte ens tre av dessa ligger på en rät linje, är G irreducibelt om det existerar (enligt en tidigare sats om andragradskurvor genom fem punkter i kapitel 13.1). Men existensen av ett sådant G motsäger antagandet om att inte ens sex av punkterna ska ligga på samma irreducibla andragradskurva. Det bevisar satsen i detta fall.

Fall 2. I detta fall antar vi att tre av punkterna, säg P_6, \dots, P_8 , är kolinjära. Låt L vara en linje genom dessa punkter och specificera ytterligare en punkt på denna, säg P_9 . Låt

$$F \in V_3(P_1, \dots, P_9).$$

Vi ska visa att det bara finns ett sådant F , upp till en övergripande konstant. Om L och F inte har gemensamma faktorer är $I(F, L) \geq 4$, eftersom $F(P_i) = L(P_i) = 0$, $i = 6, \dots, 9$. Enligt Bezouts sats är dock $I(F, L) = 3$. Alltså är $F = LG$. Eftersom inte fyra av punkterna P_1, \dots, P_8 ligger på en linje är kurvan $G = 0$ entydigt bestämd av villkoren $G(P_1) = \dots = G(P_5)$, enligt tidigare sats om andragradskurvor. Det följer att $F = 0$ är entydigt bestämd. Alltså är $\dim_{\mathbb{C}} V_3(P_1, \dots, P_9) = 1$, så $\dim_{\mathbb{C}} V_3(P_1, \dots, P_8) \leq 2$.

Fall 3. Antag att sex av punkterna, säg P_3, \dots, P_8 ligger på samma irreducibla andragradskurva $G = 0$. Då är $G(P_1) \neq 0 \neq G(P_2)$. Välj en till punkt P_9 så att $G(P_9) = 0$. Låt $0 \neq F \in V_3(P_1, \dots, P_9)$. Vi ska återigen visa att det bara finns ett sådant F . Om G inte delar F är $I(F, G) \geq 7$ vilket motsäger Bezouts sats. Alltså är G en faktor i F , så att $F = GL$, för någon linje L . Men eftersom $F(P_1) = F(P_2) = 0$ måste L då vara den entydiga linjen genom P_1 och P_2 . Alltså är F entydigt bestämd av de givna nio villkoren, så vi har åter $\dim_{\mathbb{C}} V_3(P_1, \dots, P_9) = 1$ varav följer $\dim_{\mathbb{C}} V_3(P_1, \dots, P_8) \leq 2$.

Detta avslutar beviset.

Lemma 2. Låt F, F_1 och F_2 vara tredjegradspolynom som definierar kurvorna C, C_1 och C_2 i \mathbb{CP}^2 . Antag att $F_1 = 0$ och $F_2 = 0$ skär varandra i nio distinkta punkter P_1, \dots, P_9 , $P_i \neq P_j$. Antag att $F(P_i) = 0$, $i = 1, \dots, 8$. Då är också $F(P_9) = 0$.

Bevis. Vi visar först att villkoren i Lemma 1 är uppfyllda för punkterna P_1, \dots, P_8 . Om fyra av dem, säg P_1, \dots, P_4 , ligger på samma linje $L = 0$, så måste enligt Bezout, antingen $3 = I(F_i, L) \geq 4$ för $i = 1, 2$ eller så innehåller både F_1 och F_2 den irreducibla faktorn L och

deras snitt innehåller oändligt många punkter. I båda fallen har vi en motsägelse. Om sju av punkterna ligger på samma irreducibla andragsgradskurva $G = 0$ är antingen $6 = I(F_i, G) \geq 7$ för $i = 1, 2$ eller så innehåller kurvornas snitt oändligt många punkter. Motsägelse igen. Det följer från Lemma 1 att vektorrummet $V_3(P_1, \dots, P_8)$ har dimension 2. Uppenbarligen är F , F_1 och F_2 tre nollskilda vektorer i detta rum och därför linjärt beroende. Det finns alltså komplexa tal a, b, c , ej alla noll, så att

$$aF_1 + bF_2 + cF = 0$$

Talet $c \neq 0$, ty annars är $C_1 = C_2$. Evaluerar vi båda sidor av denna likhet i P_9 får vi, eftersom $F_1(P_9) = F_2(P_9) = 0$

$$F(P_9) = 0,$$

vilket skulle bevisas. 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: $P_1 = O$, $P_2 = P$, $P_3 = Q$, $P_4 = R$, $P_5 = P * Q$, $P_6 = Q * R$, $P_7 = P + Q$, $P_8 = Q + R$ 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 observerar att

$$C_1 \cap C = \{P_1, \dots, P_8, P_9 = (P + Q) * R\}$$

Om alla P_1, \dots, P_9 är olika måste enligt Lemma 2 även C_2 gå igenom $(P + Q) * R$. Men eftersom

$$C_2 \cap C = \{P_1, \dots, P_8, P * (Q + R)\}.$$

betyder det att $(P + Q) * R = P * (Q + R)$. Detta avslutar beviset i det fall att alla punkterna i konstruktionen är olika. Det allmänna fallet skissar vi i nästa avsnitt.

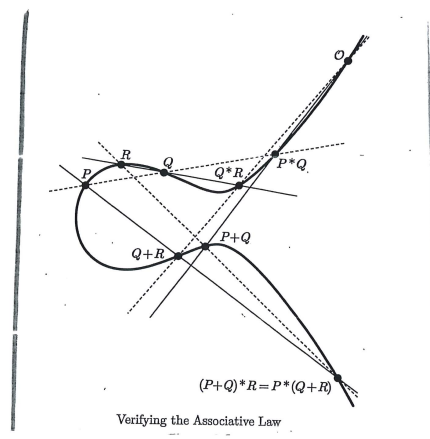
15.3 Topologisk slutkläm på beviset av associativiteten. (Överkurs.)

För att avsluta argumentet i fallet då vissa av punkterna P_1, \dots, P_9 sammanfaller använder vi följande lemma. Beviset är rättframt för någon som kan lite topologi. (Man kan också göra ett mer algebraiskt argument. Ett sådant bevis skulle inte behöva anta att vi arbetar över \mathbb{C}).

Lemma 3.

- (a) Avbildningarna $C \times C \rightarrow C$ givna av $(P, Q) \mapsto P * Q$ respektive $(P, Q) \mapsto P + Q$ är kontinuerliga.
- (b) De två avbildningarna $C \times C \times C \rightarrow C$ givna av $(P, Q, R) \mapsto (P + Q) + R$, respektive $(P, Q, R) \mapsto P + (Q + R)$ är kontinuerliga.
- (c) Mängden av tripler $(P, Q, R) \in C \times C \times C$ sådana att punkterna P_1, \dots, P_9 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 punkterna sammanfaller, kan approximeras godtyckligt väl med punkttripplar som ger 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 $C \subset \mathbb{CP}^2$ är på formen

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

skär C linjen $z = 0$ i en entydig punkt, som är en inflexionspunkt. Om O väljs som denna punkt, så har grupplagen följande egenskaper.

- (a) Inversoperationen $P \rightarrow -P$ 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: $-P = P * O = P * (O * O)$. Det följer att $P + Q = -(P * Q)$. Så $P + Q + R = 0 \iff P + Q = -R \iff R = P * Q$ och vi är klara.

15.5 Något om elliptiska kurvor över andra kroppar än \mathbb{C} . **Ej skrivet än.**

16 Mer algebra.

Låt R vara en ring, med vilket vi i denna kurs ju menar en kommutativ ring med 1.

16.1 Radikalideal och reducerade ringar.

Definition. Radikalen \sqrt{I} till ett ideal $I \subseteq R$ är

$$\sqrt{I} = \{f \in R \mid \exists n : f^n \in I\}.$$

Definition. Ett *radikalideal* $I \neq R$ är ett ideal som sammanfaller med sin radikal: $\sqrt{I} = I$.

Anmärkning. Radikalen är ett ideal. Beviset är en övning, se nedan.

Anmärkning: Ordet radikal kommer från latinets *radix* som betyder rot. Som framgår av definitionen är ett radikalideal ett ideal som innehåller alla n :te rötter till alla element, för alla $n \in \mathbb{N}$.

Sats. Varje primideal är ett radikalideal.

Bevis. Detta är omedelbart från begreppens definitioner.

Exempel.

- (i) Radikalen av ett ideal $m\mathbb{Z} \subset \mathbb{Z}$ är $\sqrt{m\mathbb{Z}} = r\mathbb{Z}$, där r är den största kvadratfria faktorn i m . Med andra ord, om m har primtalsfaktoriseringen $m = p_1^{s_1} \cdot \dots \cdot p_n^{s_n}$ så är $r = p_1 \cdot \dots \cdot p_n$. För att se den ena inklusionen betrakta implikationerna

$$s \in \sqrt{m\mathbb{Z}} \iff s^N \in m\mathbb{Z} \iff m|s^N \implies r|s^N \implies r|s \iff s \in r\mathbb{Z}.$$

Den näst sista implikationen här gäller eftersom r är kvadratfri. För den andra inklusionen låt m och r ha primtalsfaktoriseringar som ovan. Låt $N = \max s_i$. Då är uppenbarligen $r^N = m \cdot p_1^{N-s_1} \cdot \dots \cdot p_n^{N-s_n} \in m\mathbb{Z}$.

T.ex. är $6\mathbb{Z} \subset \mathbb{Z}$ ett radikalideal men $4\mathbb{Z} \subset \mathbb{Z}$ är det inte - det innehåller ju t.ex. inte kvadratroten 2 till 4. ($\sqrt{4\mathbb{Z}} = 2\mathbb{Z}$).

- (ii) På samma sätt som ovan visar man att radikalen av ett ideal $(f) \subset \mathbb{C}[x]$ är på samma sätt (r) där $r = r(x)$ är produkten av de distinkta irreducibla faktorerna i $f(x)$. T.ex. är $\sqrt{(x(x+1)^2)} = (x(x+1))$
- (iii) På samma sätt som ovan visar man att radikalen $\sqrt{(f)}$ av ett huvudideal $(f) \subset \mathbb{C}[x, y]$ genereras 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. Notera att (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. Det kan få bli en övning. 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, se nedan. 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.

Övningar.

1. Visa att radikalen till ett ideal är ett ideal.
2. Visa att I är ett radikalideal $\iff R/I$ saknar nilpotenta nollskilda element.
3. Visa att

$$\sqrt{I} \subseteq \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p}.$$

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 geometri utan bevis (dessa läses endast kursivt).

Definition. Låt $F \subseteq \mathbb{C}[x_1, \dots, x_n]$. Vi skriver

$$V(F) = \{\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{C}^n \mid \forall f \in F : f(\mathbf{x}) = 0\}.$$

Mängder $V(F)$ av detta slag kallas *affina 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 Hilbert¹⁸ säger dessutom att varje ideal I i en polynomring över en kropp är *ändligt genererat*¹⁹ så faktiskt är varje algebraisk mängd av formen $V(f_1, \dots, f_n)$, 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 :

$$I(V) = \{f \in \mathbb{C}[x_1, \dots, x_n] \mid \forall \mathbf{x} \in V : f(\mathbf{x}) = 0\}.$$

Det är lätt att se att $I(V)$ är ett ideal. Dessutom är $V = \bigcap_{f \in I(V)} V(f) = V(I(V))$.²⁰

¹⁸Hilberts sats, David Hilbert (1862-1943).

¹⁹Ringar i vilka alla ideal är ändligt genererade kallas Noetherska ringar, efter Emmy Noether (1882-1935).

²⁰Beviset av de flesta (inte alla) av påståendena som är utströdda i detta kapitel kan betraktas som övningar (dock överkurs).

Vi har alltså en korrespondens

$$\{\text{Ideal i } \mathbb{C}[x_1, \dots, x_n]\} \leftrightarrow \{\text{Algebraiska mängder i } \mathbb{C}^n\},$$

som tillordnar ett ideal $I(V)$ till varje algebraisk mängd V och en algebraisk mängd $V(I)$ till varje ideal I . Denna korrespondens uppfyller $V(I(V)) = V$ enligt ovan, men i allmänhet är $I(V(I)) \neq I$ som nedanstående exempel i dimension $n = 1$ 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. Den nämnda korrespondensen ovan ger en *bijektion* mellan de algebraiska mängderna i \mathbb{C}^n och *radikalidealerna* i $\mathbb{C}[x_1, \dots, x_n]$.

Fakta. 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 primidealerna i $\mathbb{C}[x, y]$.

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

$$f|_V : V \subset \mathbb{C}^2 \rightarrow \mathbb{C}.$$

Två polynom f och g definierar samma funktion på V 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. Kvotalgebran

$$\mathbb{C}[V] := \mathbb{C}[x, y]/(p)$$

kallas *koordinatringen för V* och kan alltså tänkas som rummet av polynomfunktioner definierade på V . Elementen i koordinatringen kallas *reguljära funktioner*.

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 $I \subset \mathbb{C}[x_1, \dots, x_n]$ som motsvarar $V = V(I)$ är *koordinatringen för V* definierad som

$$\mathbb{C}[V] = \mathbb{C}[x_1, \dots, x_n]/I.$$

Om f är reducibelt är inte koordinatringen ett integritetsområde. Se exemplet (iv) nedan.

Exempel. Vi använder Noethers isomorfitsats för att beräkna några koordinatringar nedan. Observera att $\mathbb{C}[x, y]$ som \mathbb{C} -algebra genereras av de tre elementen $1, x, y$ så det räcker att ange värdet på dessa element för att specificera en algebramorfism. (Vi har förstås alltid $\phi(1) = 1$, dessutom.)

- (i) Koordinatringen på x -axeln $y = 0$ är

$$\mathbb{C}[x, y]/(y) \cong \mathbb{C}[x].$$

Definiera nämligen en surjektiv algebramorfism $\phi : \mathbb{C}[x, y] \rightarrow \mathbb{C}[x]$ genom $\phi(x) = x$, $\phi(y) = 0$. Kärnan $\ker \phi = (y)$, så ϕ inducerar den angivna isomorfismen. Detta verkar rimligt, eftersom ringen av polynomfunktioner på \mathbb{C} bör vara $\mathbb{C}[x]$.

- (ii) Koordinatringen för linjen $y = x$ är

$$\mathbb{C}[x, y]/(y - x) \cong \mathbb{C}[x],$$

isomorfismen här är här inducerad av $\phi : \mathbb{C}[x, y] \rightarrow \mathbb{C}[x]$, given av $\phi(x) = x$, $\phi(y) = x$. 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

$$\mathbb{C}[x, y]/(y - p(x)) \cong \mathbb{C}[x],$$

isomorfismen här ges av $\phi(x) = x$, $\phi(y) = p(x)$. Att $f(x, y)$ ligger i $\ker(\phi)$ här är detsamma som att $f(x, p(x)) = 0$ dvs. $y - p(x)$ delar $f(x, y)$.

- (iv) Koordinatringen för en disjunkt union V av n punkter $(a_1, b_1), \dots, (a_n, b_n)$ är isomorf med \mathbb{C}^n (produkt och addition i varje lucka separat). Betrakta algebramorfismen

$$\phi : \mathbb{C}[x, y] \rightarrow \mathbb{C}^n,$$

som ges av $\phi(f) = (f(a_1, b_1), \dots, f(a_n, b_n))$. Den är surjektiv och har $\ker \phi = (x - a_1, y - b_1) \cap \dots \cap (x - a_n, y - b_n) = I(V)$. 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 $(1, 0, 0 \dots 0)(0, 1, 0 \dots 0) = (0, 0, \dots, 0)$ 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. Korrespondensen ovan ger en ekvivalens av kategorier mellan kategorin av algebraiska mängder och reguljära avbildningar (se nedan) och kategorin av ändligt genererade reducerade \mathbb{C} -algebror och algebramorfismer. Det vore att gå för långt att beskriva vad detta är, men det betyder ungefär att all intressant information om en algebraisk mängd, står att finna i dess koordinatring. 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.

Exempel. Om V är irreducibel är $I(V)$ ett primideal så $\mathbb{C}[V]$ saknar nolldelare. Om V har flera komponenter så har $\mathbb{C}[V]$ nolldelare. Betrakta t.ex. V givet av $I = (xy)$. På V kan vi betrakta de två reguljära funktionerna $x + I$ och $y + I$. Ingen av dessa är noll i $\mathbb{C}[V]$ men produkten av dem är. Ett annat exempel har vi i (iv) ovan, när $n \geq 2$

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. $R = \mathbb{C}[x]/(x^2)$. Här 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 och vi ska betrakta den som ett slags generaliserat funktionsrum i alla fall. Den korrekta teorin för att hantera ringar som denna geometriskt är teorin för *scheman*.²¹

17.3 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 sådana polynomfunktioner.

Definition. Låt $V \subseteq \mathbb{C}^n$ vara en algebraisk mängd. En *reguljär avbildning* $\mathbf{f} : V \rightarrow \mathbb{C}^m$ är en avbildning sådan att den kan beskrivas med komponenter $\mathbf{f} = (f_1, \dots, f_m)$ där $f_1, \dots, f_m \in \mathbb{C}[V]$.

Definition. Två algebraiska mängder $V \subseteq \mathbb{C}^n$ och $W \subseteq \mathbb{C}^m$ sägs vara *isomorfa* om det finns reguljära avbildningar $\mathbf{f} : V \rightarrow \mathbb{C}^m$ och $\mathbf{g} : W \rightarrow \mathbb{C}^n$, så att $\mathbf{f} \circ \mathbf{g} = \text{id}_W$ och $\mathbf{g} \circ \mathbf{f} = \text{id}_V$.

Exempel:

- (i) Låt $p(t)$ vara ett polynom. Avbildningen $\mathbf{f} : \mathbb{C} \rightarrow \mathbb{C}^2$, 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 $g : \Gamma \rightarrow \mathbb{C}$, $g(x, y) = x$, så Γ är *isomorf* med \mathbb{C} .
- (ii) Avbildningen $f : \mathbb{C} \rightarrow \mathbb{C}^2$, 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 isomorfism* (det finns ingen sådan isomorfism).
- (iii) Affina avbildningar ges av polynom (av grad 1) och är därför reguljära.

Anmärkning. Observera att (iii) innebär att affint ekvivalenta kurvor är isomorfa, men att (i) kan användas för att ge exempel på isomorfa kurvor som inte är affint ekvivalenta. Nämligen, linjen $\mathbb{C} \subset \mathbb{C}^2$ är isomorf med varje polynomgraf, men polynomgrafer av olika grad kan inte vara affint ekvivalenta.

²¹Se t.ex. Eisenbud/Harris, *The Geometry of Schemes* för en introduktion.

Fakta. En reguljär avbildning $\mathbf{F} : V \rightarrow W$ mellan algebraiska mängder inducerar en \mathbb{C} -algebrahomomorfism $\mathbf{F}^* : \mathbb{C}[W] \rightarrow \mathbb{C}[V]$ genom $\mathbf{F}^*(f) = f \circ \mathbf{F}$. Om \mathbf{F} är en isomorfism av algebraiska mängder så är \mathbf{F}^* en algebraisomorfism.

Övning (frivillig). Visa faktumen ovan.

17.4 Rationella funktioner

Definition. Låt $R = \mathbb{C}[x_1, \dots, x_n]$. Som vi redan diskuterat i kapitlet med algebrarepetition, kallas ett element av fraktionskroppen $Q(R)$ en *rationell funktion*. Vi använder beteckningen $\mathbb{C}(x_1, \dots, x_n)$ 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 och koordinatringen $\mathbb{C}[V] = \mathbb{C}[x, y]/(p)$ 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*.

Anmärkning. Man bör notera att elementen i $\mathbb{C}(V)$ vanligen endast är partiellt definierade. Nämnaren kan vara noll och 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 $\frac{f}{g}$ där $g(P) \neq 0$.

Sats. Om en rationell funktion är reguljär i alla punkter på V är den en reguljär funktion (dvs. restriktionen av en polynomfunktion).

Bevis. Utelämnas. Se senare kurser i algebraisk geometri.

Sats. Om en rationell funktion är reguljär i P har den ett väldefinierat värde $\frac{f(P)}{g(P)} \in \mathbb{C}$ där.

Bevis. Övning. Se nedan.

Övning.

1. Visa satsen ovan.

17.5 Rationella avbildningar

Definition. En *rationell avbildning* $\mathbf{f} : V \rightarrow \mathbb{C}^n$ är en (partiellt definierad) avbildning som kan beskrivas med komponenter $\mathbf{f} = (f_1, \dots, f_n)$ där $f_1, \dots, f_n \in \mathbb{C}(V)$. Vi kallar f *reguljär* i \mathbf{x} om alla f_i är reguljära i \mathbf{x} .

Precis som i förra avsnittet har \mathbf{f} ett väldefinierat värde i de punkter där den är reguljär.

Definition. Bilden $\mathbf{f}(V)$ av V under \mathbf{f} är bilden av mängden av alla punkter där \mathbf{f} är reguljär.

Exempel.

- (i) Låt $V = \{(x, y) \in \mathbb{C}^2 \mid x^2 + y^2 = 1\}$. Avbildningen $\mathbf{f} : \mathbb{C} \rightarrow \mathbb{C}^2$ given av

$$\mathbf{f}(t) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right)$$

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 $(0, t)$, där $t = \tan \frac{\theta}{2}$ och V i

$$\mathbf{f}(t) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) = (\cos \theta, \sin \theta).$$

- (ii) Avbildningen $g : \mathbb{C}^2 \rightarrow \mathbb{C}$ given av $g(x, y) = y/x$ är en rationell avbildning. Låt V beteckna kurvan $V = \{y^2 = x^3\}$. Då är g reguljär i alla punkter på $V \setminus \{(0, 0)\}$ och ger där en invers till $\mathbf{f} : \mathbb{C} \setminus \{0\} \rightarrow V \setminus \{(0, 0)\}$, given av $t \mapsto (t^2, t^3)$. Vi säger att \mathbb{C} och V är *birationellt ekvivalenta*²².
- (iii) De två ovanstående exemplen är mer generella än de ser ut. Alla kägelsnitt (irreducibel andragsgradskurva) och singulära tredjegradskurvor kan parametreras med rationella funktioner på detta sätt. De är alltså birationellt ekvivalenta med \mathbb{C} . Sådana kurvor kallas *rationella kurvor*.
- (iv) Avbildningen

$$F : \mathbb{C}^2 \rightarrow \mathbb{C}^2,$$

given av

$$F(x, y) = \left(\frac{ax + by + c}{gx + hy + k}, \frac{dx + ey + f}{gx + hy + k} \right),$$

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.

²²En rationell avbildning $f : X \rightarrow Y$ är en *birationell ekvivalens* om $f(X)$ är tät i Y och det finns en rationell avbildning $g : Y \rightarrow X$ 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 $X \rightarrow Y$ är i ett-ett-korrespondens med isomorfier mellan kropparna $k(Y) \rightarrow k(X)$.

18 Lokalisering och skärningstalets definition.

18.1 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 helt och hållet parallell med konstruktionen av fraktionskroppar (som ni är bekanta med).

Sats. Låt R vara ett integritetsområde och $S \subseteq R \setminus \{0\}$ 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 $R \rightarrow S^{-1}R$ given av $r \mapsto r/1$ är en injektiv ringhomomorfism.

Bevis. Eftersom $R \times S \subseteq R \times (R \setminus \{0\})$ och ekvivalensrelationerna som bildar $S^{-1}R$ resp. $Q(R)$ är desamma, kan $S^{-1}R$ identifieras med delringen

$$S^{-1}R \cong \{f \in Q(R) \mid f = p/q \text{ där } q \in S\} \subseteq Q(R).$$

Notation. Det viktigaste exemplet är när $\mathfrak{p} \subset R$ är ett primideal och $S = R \setminus \mathfrak{p}$ ²³. 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 $S = \{1, f, f^2, \dots\}$. Då skriver vi

$$R_f = S^{-1}R.$$

Detta kallas ibland lokalisering *utanför f* (eng. *localization away from f*).

Exempel.

²³Notera att definitionen av ett primideal säger precis att dess komplement är en multiplikativ mängd.

(i) Om $R = \mathbb{Z}$ och $\mathfrak{p} = (3)$ så är lokaliseringen

$$\mathbb{Z}_{\mathfrak{p}} \cong \left\{ \frac{p}{q} \in \mathbb{Q} \mid 3 \nmid q \right\} \subset \mathbb{Q}$$

(ii) Om $R = \mathbb{Z}$ och $S = \{1, 3, 3^2, 3^3, \dots\}$ så är lokaliseringen

$$\mathbb{Z}_3 \cong \left\{ \frac{p}{q} \in \mathbb{Q} \mid \exists m \in \mathbb{N} : q = 3^m \right\} \subset \mathbb{Q}.$$

(ii) Om $R = \mathbb{C}[x]$ och primidealet det maximala idealet $\mathfrak{m} = (x)$ är

$$\mathbb{C}[x]_{(x)} \cong \left\{ \frac{p}{q} \in \mathbb{C}(x) \mid x \nmid q \right\} = \{p/q \in \mathbb{C}(x) \mid q(0) \neq 0\} \subset \mathbb{C}(x).$$

(iii) Om $R = \mathbb{C}[x, y]$ och primidealet det maximala idealet $\mathfrak{m} = (x - a, y - b)$ är

$$\mathbb{C}[x, y]_{\mathfrak{m}} \cong \left\{ \frac{p}{q} \in \mathbb{C}(x, y) \mid q(a, b) \neq 0 \right\} \subset \mathbb{C}(x, y).$$

(iv) Om $R = \mathbb{C}[x, y]$ och primidealet huvudidealet $\mathfrak{p} = (f)$ för ett irreducibelt polynom f är

$$\mathbb{C}[x, y]_{\mathfrak{p}} = \mathbb{C}[x, y]_{(f)} = \left\{ \frac{p}{q} \in \mathbb{C}(x, y) \mid f \nmid q \right\} \subset \mathbb{C}(x, y).$$

Exemplet (iii) ovan är extra viktigt för oss i denna kurs så det får ett eget namn i följande definition.

Definition. Den lokala ringen i en punkt $P = (a, b)$ är lokaliseringen av $\mathbb{C}[x, y]$ till det maximala ideal $\mathfrak{m} = (x - a, y - b)$ som motsvarar P . Den betecknas

$$\mathcal{O}_P = \mathbb{C}[x, y]_{\mathfrak{m}}$$

\mathcal{O}_P innehåller alltså inverser till alla element som inte är 0 i P och vi kan tänka på $\mathcal{O}_P = \mathbb{C}[x, y]_{\mathfrak{m}} \subset \mathbb{C}(x, y)$ som delringen bestående av de *rationella funktioner som är reguljära i P* .

Exempel. Let $P = (0, 0) \in \mathbb{C}^2$. $\mathcal{O}_P \subset \mathbb{C}(x, y)$ består av de rationella funktioner som kan skrivas $\frac{f}{g}$ där g har icke-försvinnande konstantterm.

Den lokala ringen \mathcal{O}_P har gett upphov till följande allmänna begrepp.

Definition. En ring R kallas *lokal*, om den har ett enda maximalt ideal.

Följande sats visar att den lokala ringen är en lokal ring.

Sats. Lokaliseringen $R_{\mathfrak{p}}$ av R i ett primideal \mathfrak{p} är en lokal ring. Det maximala idealet ges av $\mathfrak{p}R_{\mathfrak{p}} \subset R_{\mathfrak{p}}$, dvs. det består av bråk p/q där $p \in \mathfrak{p}$.

Bevis. Varje element $x \in R \setminus \mathfrak{p}$ är inverterbart i $R_{\mathfrak{p}}$, så varje äkta ideal i $R_{\mathfrak{p}}$ måste vara innehållit i $\mathfrak{p}R_{\mathfrak{p}}$.

Anmärkning. Termen “lokalisering” kan förklaras på följande sätt. I en polynomring R är bara de nollskilda konstanterna inverterbara. Ringen av alla rationella funktioner innehåller inverser till alla polynom, men betraktade som funktioner har de diverse singulariteter. Lokaliseringen kommer till nytta om vi bara är intresserade av geometri nära P och således är beredda att ignorera singulariteter som inte ligger i P .²⁴

Anmärkning Om $I \subset R$ är ett ideal och $R_{\mathfrak{p}}$ lokaliseringen av R i ett primideal, kommer motsvarande ideal i $R_{\mathfrak{p}}$ att betecknas med $I_{\mathfrak{p}}$. Det leder till den något udda notationen $\mathfrak{p}_{\mathfrak{p}}$ för det maximala idealet i $R_{\mathfrak{p}}$.

18.2 Lokalisering i allmänna fallet. (Mestadels överkurs.)

Definitionen av lokalisering som vi gav den i förra avsnittet fungerar så länge S inte innehåller nolldelare. Annars måste vi definiera lokaliseringen på följande sätt istället. Det 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.

Definition. Låt R vara en ring och $S \subset R$ en multiplikativ mängd. Lokaliseringen av R med avseende på S är

$$S^{-1}R = (R \times S) / \sim,$$

där

$$(x, s) \sim (y, t) \iff \text{Det finns } u \in S : u(xt - ys) = 0.$$

Vi betecknar (x, s) med $\frac{x}{s}$.

Följande sats visar att definitionen ovan inte är nonsens.

Sats.

- (a) \sim är en ekvivalensrelation.
- (b) Om addition och multiplikation definieras med samma formler som i förra avsnittet blir $S^{-1}R$ en ring.
- (c) Den naturliga avbildningen $R \rightarrow S^{-1}R$ given av $r \mapsto \frac{r}{1}$ är en (inte nödvändigtvis injektiv) ringhomomorfism.

²⁴Mer 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 identiskt noll på V lokaliseringen $R_{\mathfrak{p}}$. I den här kursen kommer vi dock bara att behöva lokalisera i punkter, dvs. i maximala ideal.

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 $v(yr - tz) = 0$, dvs. $yrv = vtz$. Vi behöver visa att $(x, s) \sim (z, r)$. Multiplicera $u(xt - ys) = 0$ med rv . Vi får $urvt(xt - ys) = 0 \iff urvxt - us(yrv) = 0 \iff urvxt - us(vtz) = 0 \iff uvt(xr - sz) = 0$. 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 gör fallet med addition och lämnar multiplikationen till läsaren. Om $\frac{x'}{s'} \sim \frac{x}{s}$, så att det finns $u \in S$ sådant att $u(xs' - x's) = 0$, har vi

$$\frac{x}{s} + \frac{y}{t} = \frac{xt + ys}{st} = \frac{us'xt + us'ys}{us'st} = \frac{usx't + us'y's}{us'st} = \frac{x't - ys'}{s't} = \frac{x'}{s'} + \frac{y}{t},$$

samt

$$\frac{x}{s} \cdot \frac{y}{t} = \frac{xy}{st} = \frac{uxys'}{usts'} = \frac{ux'y's}{usts'} = \frac{x'y}{s't} = \frac{x'}{s'} \cdot \frac{y}{t}.$$

(c) Vi har

$$f(rs) = \frac{rs}{1} = \frac{r}{1} \frac{s}{1} = f(r)f(s).$$

$$f(r+s) = \frac{r+s}{1} = \frac{r}{1} + \frac{s}{1} = f(r) + f(s)$$

Sats. Låt R, R' vara ringar och $S \subset R$ en multiplikativ mängd. Låt vidare $f : R \rightarrow R'$ vara en ringhomomorfism sådan att $f(S)$ består av inverterbara element i R' . Då finns en entydig ringhomomorfism $\tilde{f} : S^{-1}(R) \rightarrow R'$ som uppfyller $\tilde{f} \circ \iota = f$. Den ges av $\tilde{f}\left(\frac{r}{s}\right) = \frac{f(r)}{f(s)}$.

Bevis. Entydighet: Om \tilde{f} är som angivet, gäller

$$\tilde{f}\left(\frac{r}{s}\right) = \tilde{f}\left(\frac{r}{1}\right) \tilde{f}\left(\frac{1}{s}\right) = \tilde{f}\left(\frac{r}{1}\right) \left(\tilde{f}\left(\frac{s}{1}\right)\right)^{-1} = \frac{f(r)}{f(s)},$$

så det finns bara ett sätt att definiera \tilde{f} . För att se att detta är en väldefinierad avbildning, antag att det finns $u \in S$ så att $urs' = ur's$. Då är

$$\frac{f(r')}{f(s')} = \frac{f(ur's)}{f(us's)} = \frac{f(urs')}{f(uss')} = \frac{f(u)f(r)f(s')}{f(u)f(s)f(s')} = \frac{f(r)}{f(s)}.$$

Till sist behöver vi visa att \tilde{f} är multiplikativ, additiv och bevarar 1. De två sistnämnda verifikationer är triviala och lämnas till läsaren. Additiviteten är också rättfram:

$$\tilde{f}\left(\frac{r}{s} + \frac{r'}{s'}\right) = \tilde{f}\left(\frac{rs' + r's}{sr}\right) = \frac{f(rs' + r's)}{f(sr)} = \frac{f(r)f(s') + f(r')f(s)}{f(s)f(r)} = \tilde{f}\left(\frac{r}{s}\right) + \tilde{f}\left(\frac{r'}{s'}\right).$$

Om $I \subset R$ är ett ideal och $S \subset R$ är en multiplikativ mängd är

$$S^{-1}I = \{i/s \in S^{-1}R \mid i \in I, s \in S\}$$

ett ideal i $S^{-1}R$. Låt \bar{S} vara bilden av S under den kanoniska homomorfismen $R \rightarrow R/I$.

Sats. Avbildningen $\kappa : S^{-1}R/S^{-1}I \rightarrow \bar{S}^{-1}(R/I)$, given av

$$\kappa\left(\frac{r}{s} + S^{-1}I\right) = \frac{r + I}{s + I}$$

är en ringisomorfism.

Bevis. Utgå från sammansättningen av de kanoniska avbildningarna

$$k : R \rightarrow R/I \rightarrow \bar{S}^{-1}(R/I).$$

Bilden av S är \bar{S} så den innehåller bara inverterbara element. Därför ger den förra satsen en utvidgning till

$$\tilde{k} : S^{-1}R \rightarrow \bar{S}^{-1}(R/I),$$

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 isomorfitsats.

18.3 Exempel på lokalisering i algebraisk geometri.

Lokalisering används i algebraisk geometri för att undersöka geometri *lokalt*, t.ex. nära en viss punkt.

Exempel. Betrakta koordinatringen för den disjunkta unionen av två punkter $V = \{\pm 1\}$ i \mathbb{C} . Avbildningen

$$(\text{ev}_1, \text{ev}_{-1}) : \mathbb{C}[x] \rightarrow \mathbb{C}^2$$

som ges av

$$f \mapsto (f(1), f(-1))$$

inducerar en algebrasomorfism

$$\mathbb{C}[V] = \mathbb{C}[x]/(x^2 - 1) \cong \mathbb{C}^2,$$

via Noethers isomorfin. Notera att den första faktorn i \mathbb{C}^2 motsvarar punkten $x = 1$ och den andra $x = -1$.

Om vi gör samma sak efter att ha lokaliserat $\mathbb{C}[x]$ i punkten $x = -1$, dvs inverterat komplementet till det maximala idealet $\mathfrak{m} = (x + 1)$, händer följande. $\mathbb{C}[x]_{\mathfrak{m}}$ är enligt ovan isomorf med ringen av rationella funktioner vars nämnare är nollskild i $x = -1$. Vi kan alltså skriva varje element i $\mathbb{C}[x]_{\mathfrak{m}}$ som en rationell funktion

$$\frac{p(x)}{q(x)} = \frac{a_0 + a_1(x + 1) + \dots + a_n(x + 1)^n}{b_0 + b_1(x + 1) + \dots + b_m(x + 1)^m},$$

där $b_0 \neq 0$.

Notera att i $\mathbb{C}[x]_{\mathfrak{m}}$ genererar polynomen $x^2 - 1$ och $x + 1$ samma ideal, eftersom $x - 1$ är inverterbart:

$$(x + 1)f(x) = (x^2 - 1)\frac{f(x)}{x - 1}.$$

I kvotringen $\mathbb{C}[x]_{\mathfrak{m}}/(x^2 - 1)_{\mathfrak{m}} = \mathbb{C}[x]_{\mathfrak{m}}/(x + 1)_{\mathfrak{m}}$ är

$$\frac{p(x)}{q(x)} = \frac{a_0}{b_0} \in \mathbb{C}$$

eftersom

$$b_0 p(x) - a_0 q(x) = b_0(a_0 + \dots + a_n(x + 1)^n) - a_0(b_0 + \dots + b_m(x + 1)^m) = (x + 1)Q(x),$$

som representerar 0 i kvotringen. Det följer att

$$\mathbb{C}[x]_{\mathfrak{m}}/(x^2 - 1)_{\mathfrak{m}} \cong \mathbb{C}.$$

Observera att isomorfismen ges av evaluering i punkten $x = -1$.

Med hjälp av satsen i förra avsnittet om att kvotbildning och lokalisering kommuterar, har vi också

$$(\mathbb{C}[x]/(x^2 - 1))_{\bar{\mathfrak{m}}} = \mathbb{C}[x]_{\mathfrak{m}}/(x^2 - 1)_{\mathfrak{m}} \cong \mathbb{C}.$$

Här betecknar $\bar{\mathfrak{m}}$ det ideal som $x + 1$ genererar i kvotringen. Notera att i vänsterledet är ringen som lokaliseras inte ett integritetsområde.

Exempel. $\mathbb{C}[x]/(x^2)$ är inte reducerad, eftersom (x^2) inte är ett radikalideal. Som \mathbb{C} -vektorrum är den isomorf med \mathbb{C}^2 , eftersom varje polynom är ekvivalent med sin linjarisering $a_0 + a_1x$,

modulo x^2 . Lokalisering i $\mathfrak{m} = (x)$ ändrar inte på detta. I $\mathbb{C}[x]_{\mathfrak{m}}$ är varje element en rationell funktion

$$f(x) = \frac{p(x)}{q(x)} = \frac{a_0 + a_1x + \dots + a_nx^n}{b_0 + b_1x + \dots + b_mx^m},$$

där $b_0 \neq 0$. I kvotringen $\mathbb{C}[x]_{\mathfrak{m}}/(x^2)_{\mathfrak{m}}$ är detta ekvivalent med ett linjärt polynom $c_0 + c_1x$ där $c_0 = \frac{a_0}{b_0}$ och $c_1 = \frac{a_1b_0 - b_1a_0}{b_0^2}$. Detta är precis linjariseringen av $f(x)$ i 0. Dessa påståenden lämnar vi som övning till läsaren.

Övning.

- (a) Visa att $c_0 = f(0)$ och $c_1 = f'(0)$.
- (b) Visa att $f(x)$ är ekvivalent med $c_0 + c_1x$ i kvotringen.
- (c) Generalisera till fallet $\mathbb{C}[x]/(x^n)$, $n \geq 2$.

18.4 Skärningstalets definition och exempel.

Om $P = (a, b) \in \mathbb{C}^2$ och motsvarande maximala ideal är $\mathfrak{m} = (x - a, y - b)$, definierade vi *den lokala ringen i P* som följande lokalisering

$$\mathcal{O}_P = \mathbb{C}[x, y]_{\mathfrak{m}}.$$

Låt $f, g \in \mathbb{C}[x, y]$. Vi definierar skärningstalet mellan f och g i P på följande sätt:

Definition.

$$I_P(f, g) = \dim_{\mathbb{C}} \mathcal{O}_P/(f, g)_{\mathfrak{m}}.$$

Anmärkning. Ibland vill vi skriva tu vad vi menar med \mathcal{O} och använder då den mer belastade men tydligare notationen

$$I_P(f, g) = \mathbb{C}[x, y]_{\mathfrak{m}}/(f, g)_{\mathfrak{m}}.$$

Exempel. De två polynomen $f(x, y) = y - x^2 + 1$ och $g(x, y) = y$ har de gemensamma nollställena $(0, 1)$ och $(0, -1)$. För att beräkna skärningstalet i $(0, -1)$ lokaliserar vi i idealet $\mathfrak{m} = (x + 1, y)$ och får

$$\mathbb{C}[x, y]_{\mathfrak{m}}/(y - x^2 + 1, y)_{\mathfrak{m}} \cong \mathbb{C}[x]_{(x+1)}/(x^2 - 1)_{(x+1)} \cong \mathbb{C}.$$

Beräkningen i det sista steget kommer från exemplen i förra kapitlet. Alltså är skärningstalet

$$I_{(0, -1)}(f, g) = 1.$$

På samma sätt ser vi att

$$I_{(0, 1)}(f, g) = 1.$$

Detta stämmer med vår intuition, de två kurvorna skär varandra transversellt i dessa punkter.

Exempel. Betrakta nu $f(x, y) = y - x^2$ och $g(x, y) = y$. De tangerar varandra i $(0, 0)$ och vi förväntar oss att skärningstalet ska vara 2, eftersom multipliciteten hos nollstället 0 till x^2 är 2. Mycket riktigt, om vi lokaliserar i $\mathfrak{m} = (x, y)$ och åter använder exempelräkningarna i förra kapitlet får vi

$$\mathbb{C}[x, y]_{\mathfrak{m}} / (y - x^2, y)_{\mathfrak{m}} \cong \mathbb{C}[x]_{(x)} / (x^2)_{(x)} \cong \mathbb{C}^2.$$

så $I_P(y - x^2, y) = 2$.

Anmärkning. På samma sätt ser man förstås att $I_P(y - x^n, y) = n$.

Exempel. Betrakta kurvorna $f = y - x^3(x - 1)$ och $g = y$. Det är lätt att se att om $\mathfrak{m} = (x, y)$ har vi

$$\mathbb{C}[x, y]_{\mathfrak{m}} / (y - x^3(x - 1), y)_{\mathfrak{m}} = \mathbb{C}[x]_{(x)} / (x^3(x - 1))_{(x)} = \mathbb{C}[x]_{(x)} / (x^3)_{(x)},$$

där den sista likheten är för att lokalisering i $(x, y) = (0, 0)$ gör $x - 1$ inverterbart. Skärningstalet i $(0, 0)$ är alltså

$$I_{(0,0)}(f, g) = \dim_{\mathbb{C}} (\mathbb{C}[x]_{(x)} / (x^3)_{(x)}) = \dim_{\mathbb{C}} \mathbb{C}^3 = 3.$$

Samma sorts räkningar fast med $\mathfrak{m} = (x - 1, y)$ ger

$$\mathbb{C}[x, y]_{\mathfrak{m}} / (y - x^3(x - 1), y)_{\mathfrak{m}} = \mathbb{C}[x]_{(x-1)} / (x - 1)_{(x-1)} = \mathbb{C}.$$

så

$$I_{(1,0)}(f, g) = 1.$$

18.5 Relationen till koordinatringen.

Ringens som förekommer i definitionen av skärningstalet, nämligen

$$\mathbb{C}[x, y]_{\mathfrak{m}} / (f, g)_{\mathfrak{m}} = (\mathbb{C}[x, y] / (f, g))_{\bar{\mathfrak{m}}}$$

ser väldigt mycket ut som en koordinatring. Närmare bestämt, $\mathbb{C}[x, y] / (f, g)$ vore koordinatringen för den algebraiska mängden $V = V(f) \cap V(g)$ om idealet (f, g) vore ett radikalideal. Detta är dock inte fallet i allmänhet, och detta är en förutsättning för att vi ska kunna använda den för att definiera skärningstalet.

Koordinatringen $\mathbb{C}[V] = \mathbb{C}[x, y] / \sqrt{(f, g)}$ innehåller bara information om V , som här består av ett ändligt antal punkter. Den kan inte säga något om hur f och g skär varandra eftersom det inte syns i V . Vilka andra ekvationer som helst som har samma lösningar V kan ju användas för att definiera $\mathbb{C}[V]$.

Det finns ett geometriskt objekt som har koordinatring $\mathbb{C}[x, y] / (f, g)$, men det är inte en algebraisk mängd, utan det enklaste exemplet på vad som i högre algebraisk geometri kallas ett *schema*. Den allmänna definitionen är ganska komplicerad, men i detta fall kan ni tänka på schemat som bestående av "punkter med multiplicitet".

Vi betraktar det sista exemplet i förra avsnittet i relation till denna generaliserade koordinatring.

Exempel. Som \mathbb{C} -vektorrum har vi

$$\mathbb{C}[x, y]/(y - x^3(x - 1), y) \cong \mathbb{C}[x]/(x^4 - x^3) \cong \mathbb{C}^4,$$

eftersom varje element kan representeras med ett polynom av grad 3 (högre potenser kan reduceras eftersom $x^4 = x^3$). Vi har också från förra avsnittet att de två lokaliseringarna har dimension 1 respektive 3. Vi känner också till från tidigare kurser att $1 + 3 = 4$.

Man kan mer allmänt visa följande sats.

Sats. Låt $I \subset \mathbb{C}[x, y]$ vara ett ideal (ej nödvändigtvis radikalt) sådant att $V(I)$ består av ändligt många punkter P_1, \dots, P_n . Låt \mathfrak{m}_i vara det maximala ideal som motsvarar P_i . Då gäller:

$$\mathbb{C}[x, y]/I = \bigoplus_{i=1}^n \mathbb{C}[x, y]_{\mathfrak{m}_i}/I_{\mathfrak{m}_i}.$$

19 Skärningstalet uppfyller axiomen.

19.1 Formulering av satsen.

Låt $P = (a, b) \in \mathbb{C}^2$ och låt $\mathfrak{m} = (x - a, y - b)$ vara motsvarande maximala ideal. Om det är nödvändigt att specificera punkten P , skriver vi $\mathfrak{m} = \mathfrak{m}_P$. Den lokala ringen i P är som du minns lokaliseringen

$$\mathcal{O}_P = \mathbb{C}[x, y]_{\mathfrak{m}},$$

som vi betraktar som en delring av $\mathbb{C}(x, y)$. Två polynom genererar ett ideal $(f, g)_{\mathfrak{m}} \subseteq \mathcal{O}_P$. Notera att de ingående ringarna och idealen också alla är vektorrum över \mathbb{C} och att det är denna struktur som är central i definitionen av skärningstalet, ringstrukturen spelar ingen roll då man beräknar en dimension.

Definirepetition. Om $f, g \in \mathbb{C}[x, y]$ och $P \in \mathbb{C}^2$ definierar vi

$$I_P(f, g) = \dim_{\mathbb{C}} \mathcal{O}_P/(f, g)_{\mathfrak{m}}.$$

Nu kan vi till sist bevisa följande efterlängtade sats:

Sats. Skärningstalet $I_P(f, g) \in \mathbb{N} \cup \{\infty\}$, har följande egenskaper.

(o) Skärningstalet är invariant under projektiva transformationer.

(i) $I_P(f, g) = I_P(g, f)$.

(ii) $I_P(f, g) = 0 \iff f(P) \neq 0$ eller $g(P) \neq 0$.

(iii) Låt $O = (0, 0) \in \mathbb{C}^2$. Då är $I_O(x, y) = 1$.

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

(v) $I_P(f, g) = I_P(f, g + fh)$.

19.2 Bevis av att $I_P(f, g)$ uppfyller axiomen.

Bevis.

(o) En projektiv transformation ges i affina koordinater av en birationell isomorfism²⁵

$$\mathbf{F} : \mathbb{C}^2 \rightarrow \mathbb{C}^2,$$

som inducerar en \mathbb{C} -algebraisomorfism

$$\mathbf{F}^* : \mathbb{C}(x, y) \rightarrow \mathbb{C}(x, y),$$

genom

$$\mathbf{F}^* \left(\frac{p}{q} \right) = \frac{\mathbf{F}^*(p)}{\mathbf{F}^*(q)} = \frac{p \circ \mathbf{F}}{q \circ \mathbf{F}}.$$

Denna uppfyller uppenbarligen

$$\mathbf{F}^*(\mathcal{O}_P) = \mathcal{O}_{\mathbf{F}^{-1}(P)} \text{ och } \mathbf{F}^*((f, g)_{\mathfrak{m}_P}) = (\mathbf{F}^*(f), \mathbf{F}^*(g))_{\mathfrak{m}_{\mathbf{F}^{-1}(P)}}.$$

\mathbf{F}^* inducerar därför en isomorfism $\mathcal{O}_P/(f, g)_{\mathfrak{m}_P} \cong \mathcal{O}_{\mathbf{F}^{-1}(P)}/(\mathbf{F}^*(f), \mathbf{F}^*(g))_{\mathfrak{m}_{\mathbf{F}^{-1}(P)}}$.

(i) är uppenbart eftersom $(f, g)_{\mathfrak{m}} = (g, f)_{\mathfrak{m}}$.

(ii) $I_P(f, g) = 0 \iff \mathcal{O}_P = (f, g)_{\mathfrak{m}} \iff 1 \in (f, g)_{\mathfrak{m}} \iff \exists a, b \in \mathcal{O}_P : 1 = af + bg$. 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 $1 \in (f, g)$.

(iii) Låt $\mathfrak{m} = (x, y)$.

$$I_O(f, g) = \dim_{\mathbb{C}} \mathbb{C}[x, y]_{\mathfrak{m}} / (x, y)_{\mathfrak{m}} = \dim_{\mathbb{C}} \mathbb{C} = 1.$$

(v) $I_P(f, g) = I_P(f, g + fh)$ eftersom de berörda idealen är lika: $(f, g)_{\mathfrak{m}} = (f, g + fh)_{\mathfrak{m}}$

(iv) 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.

$$0 \rightarrow \mathcal{O}_P/(f, h)_{\mathfrak{m}} \xrightarrow{\Phi} \mathcal{O}_P/(f, gh)_{\mathfrak{m}} \xrightarrow{\Psi} \mathcal{O}_P/(f, g)_{\mathfrak{m}} \rightarrow 0,$$

²⁵Den har t.o.m. formen

$$\left(\frac{ax + by + c}{gx + hy + k}, \frac{dx + ey + f}{gx + hy + k} \right)$$

som vi sett tidigare.

där

$$\Phi(z + (f, h)_{\mathfrak{m}}) = gz + (f, gh)_{\mathfrak{m}}$$

och

$$\Psi(x + (f, gh)_{\mathfrak{m}}) = x + (f, g)_{\mathfrak{m}}.$$

Vi vill visa att denna följd är en kort exakt följd, dvs. att Φ är injektiv, Ψ är surjektiv och att $\ker \Psi = \Phi(\mathcal{O}_P/(f, h)_{\mathfrak{m}})$. Då följer det nämligen från "dimensionssatsen" i avsnitt 3.5 att

$$\mathcal{O}_P/(f, gh)_{\mathfrak{m}} \cong \mathcal{O}_P/(f, h)_{\mathfrak{m}} \oplus \mathcal{O}_P/(f, g)_{\mathfrak{m}},$$

så att

$$I_P(f, gh) = \dim_{\mathbb{C}}(\mathcal{O}_P/(f, gh)_{\mathfrak{m}}) = \dim_{\mathbb{C}}(\mathcal{O}_P/(f, g)_{\mathfrak{m}}) + \dim_{\mathbb{C}}(\mathcal{O}_P/(f, h)_{\mathfrak{m}}) = I_P(f, g) + I_P(f, h).$$

(i) Ψ är surjektiv. Detta är uppenbart.

(ii) För att visa $\ker \Psi = \Phi(\mathcal{O}_P/(f, h)_{\mathfrak{m}})$, låt $x + (f, gh)_{\mathfrak{m}}$ vara ett element i $\mathcal{O}_P/(f, gh)_{\mathfrak{m}}$. Vi har att (för några a och b i \mathcal{O}_P):

$$\begin{aligned} \Psi(x + (f, gh)_{\mathfrak{m}}) = 0 &\iff x + (f, g)_{\mathfrak{m}} = 0 \iff x = af + bg \iff \\ &\iff x + (f, gh)_{\mathfrak{m}} = bg + (f, gh)_{\mathfrak{m}} \iff x \in \Phi(\mathcal{O}_P/(f, h)_{\mathfrak{m}}), \end{aligned}$$

så $\ker \Psi = \Phi(\mathcal{O}_P/(f, h)_{\mathfrak{m}})$.

(iii) Φ är injektiv. Beviset för detta är lite mer involverat. Antag att $z + (f, h)_{\mathfrak{m}} \in \ker \Phi$, så att $gz \in (f, gh)_{\mathfrak{m}}$. Då har vi

$$gz = af + bgh,$$

där $f, g, h \in \mathbb{C}[x, y]$ är polynom, men där a, b och $z \in \mathcal{O}_P$. De senare har därför nämnare (som är nollskilda i P). 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 $z + (f, h)_{\mathfrak{m}} = 0 \in \mathcal{O}_P/(f, h)_{\mathfrak{m}}$, vilket skulle visas.

Fall 2. Antag att f och g har en gemensam irreducibel faktor q sådan att $q(P) = 0$. Då är $(f, g)_\mathfrak{m} \subseteq (p)_\mathfrak{m}$, så avbildningen $x + (f, g)_\mathfrak{m} \mapsto x + (q)_\mathfrak{m}$ är en surjektiv linjär avbildning

$$\mathcal{O}_P/(f, g)_\mathfrak{m} \rightarrow \mathcal{O}_P/(q)_\mathfrak{m} = \mathbb{C}[x, y]_\mathfrak{m}/(q)_\mathfrak{m}.$$

Det följer att vi måste ha:

$$\dim_{\mathbb{C}} \mathcal{O}_P/(q)_\mathfrak{m} \leq \dim_{\mathbb{C}} \mathcal{O}_P/(f, g)_\mathfrak{m}.$$

Vi ska nu visa att vänsterledet är ∞ .

Betrakta algebramorfismen

$$i : \mathbb{C}[x, y]/(q) \rightarrow \mathbb{C}[x, y]_\mathfrak{m}/(q)_\mathfrak{m},$$

som ges av

$$i(f + (q)) = f + (q)_\mathfrak{m}.$$

Vi visar nu att den är injektiv²⁶.

Vi har

$$i(f + (q)) = 0 \iff f + (q)_\mathfrak{m} = 0 \iff f = \frac{u}{v}q,$$

där $v(P) \neq 0$. Vi har alltså $fv = uq$. Eftersom q är irreducibel, så gäller $q|f$ eller $q|v$. Det senare är omöjligt eftersom $v(P) \neq 0$ medan $q(P) = 0$. Alltså har f en faktor q så $f + (q) = 0$ och i är därför injektiv. Vi har då

$$\dim_{\mathbb{C}} \mathbb{C}[x, y]/(q) \leq \dim_{\mathbb{C}} \mathbb{C}[x, y]_\mathfrak{m}/(q)_\mathfrak{m} \leq \dim_{\mathbb{C}} \mathcal{O}_P/(f, g)_\mathfrak{m}.$$

Vi är nu klara om vi kan 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, \dots, P_n sådana att $q(P_i) = 0, \forall 0 \leq i \leq n$. Då kan vi konstruera $f_1, \dots, f_n \in \mathbb{C}[x, y]$ s.a. $f_i(P_j) = 0$ om $i \neq j$ och $f_i(P_i) = 1$ för alla i ²⁷. 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, \dots, 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

$$\dim_{\mathbb{C}} \mathbb{C}[x, y]/(q) = \infty.$$

²⁶Detta följer också direkt från satsen om att lokalisering och kvotbildning kommuterar i avsnitt 18.2, eftersom

$$\mathbb{C}[x, y]_\mathfrak{m}/(q)_\mathfrak{m} = (\mathbb{C}[x, y]/(q))_\mathfrak{m}$$

och $\mathbb{C}[x, y]/(q)$ är ett integritetsområde.

²⁷Övning!

Därför har vi till sist

$$\dim_{\mathbb{C}} \mathcal{O}_P/(f, g)_{\mathfrak{m}} \geq \dim_{\mathbb{C}} \mathbb{C}[x, y]_{\mathfrak{m}}/(q)_{\mathfrak{m}} \geq \dim_{\mathbb{C}} \mathbb{C}[x, y]/(q) = \infty.$$

Eftersom f och gh har en gemensam faktor om f och g har det, gäller också

$$\dim_{\mathbb{C}} \mathcal{O}_P/(f, gh)_m = \infty.$$

Båda sidorna i (vi) är alltså oändliga i detta fall.

Detta avslutar beviset.

20 En alternativ definition av skärningstalet. (Överkurs.)

Kom ihåg att vi tidigare visade en sats som sa att om $f(x, y) = y - p(x)$ är en graf så kan skärningstalet i origo beräknas som

$$I_0(f, g) = \text{mult}_0 g(x, p(x)).$$

Idén var att man då kunde parametrisera $f = 0$ med parametern x och därigenom reducera problemet till att studera g 's restriktion till kurvan $f = 0$. Med lite ansträngning kan man använda denna idé för att beräkna skärningstalet oavsett om f är en graf eller inte. Det är ämnet för detta avsnitt. Vi begränsar oss till fallet då skärningspunkten ligger i origo, vilket förstås inte är en allvarlig begränsning.

20.1 Formella potensserier och parametrisering av kurvor.

Låt $\mathbb{C}[[x]]$ beteckna mängden av formella potensserier i en variabel x . Ordet formell betyder här att vi betraktar potensserier utan att bry oss om till exempel konvergens. Elementen i ringen är bara uttryck

$$f(x) = a_0 + a_1x + a_2x^2 + \dots = \sum_{k=0}^{\infty} a_k x^k.$$

Dessa kan adderas och multipliceras, och multipliceras med komplexa tal och de naturliga räknereglerorna gör $\mathbb{C}[[x]]$ till en \mathbb{C} -algebra. Givetvis kan vi betrakta polynom som en ovanligt kort potensserie, så $\mathbb{C}[x] \subset \mathbb{C}[[x]]$. Notera att formella potensserier inte är funktioner så de har inte värden i olika punkter x . Undantaget är $x = 0$ där vi sätter $f(0) = a_0$ om $f(x)$ är som ovan. $\mathbb{C}[[x]]$ har följande egenskaper.

- $\mathbb{C}[[x]]$ är en faktoriell ring. Från detta och en sats i kursen i algebraiska strukturer (framtiden) följer att polynomringen $\mathbb{C}[[x]][y]$ med koefficienter i $\mathbb{C}[[x]]$ också är faktoriell.
- $\mathbb{C}[[x]]$ är en *lokal* ring, dvs. den har ett enda maximalt ideal $\mathfrak{m} = (x)$.

Sats. Låt $f(x, y) \in \mathbb{C}[x, y]$ vara ett nollskilt polynom. Då finns $d, k, r \in \mathbb{N} \setminus \{0\}$ så att

$$f(t^d, y) = t^k (y - p_1(t)) \cdots (y - p_r(t)) u(t, y),$$

där $p_i(t) \in \mathbb{C}[[t]]$ alla uppfyller $p_i(0) = 0$ och $u(t, y) \in \mathbb{C}[[t]][y]$ uppfyller $u(0, 0) \neq 0$. Givet d är denna form unik upp till permutation av $\{p_i\}$.

Vi bevisar satsen nedan, men låt oss först titta på några exempel.

Exempel. Om $f(x, y)$ är grafen till ett envariabelpolynom $p(x)$ är detta förstås trivialt. Vi har då nämligen $d = r = 1$, $k = 0$ och $u(y, t) = 1$.

$$f(t, y) = y - p(t).$$

Exempel. Om $f(x, y)$ uppfyller $f(0, 0) = 0$ och $f_y(0, 0) \neq 0$ är $y = y(x)$ lokalt kring origo och y kan Taylorutvecklas i en formell potensserie, $y = p(x) \in \mathbb{C}[[x]]$. Då gäller $f(t, p(t)) = 0$ i $\mathbb{C}[[t]]$, så $y - p(t)$ delar f i $\mathbb{C}[[t]][y]$, så $f(t, y) = (y - p(t))h(t, y)$. Här är $h(0, 0) = f_y(0, 0) \neq 0$. Här har vi $d = 1 = r$ och $k = 0$.

Exempel. Här är en konkret variant av det förra exemplet. Låt

$$f(x, y) = x^2 + (y - 1)^2 - 1 = (y - 1 - \sqrt{1 - x^2})(y - 1 + \sqrt{1 - x^2}).$$

Med binomialutvecklingen får vi

$$\sqrt{1 - t^2} = \left(1 - \frac{t^2}{2} + \frac{t^4}{8} + \dots\right),$$

så vi kan skriva, med $d = r = 1$, $k = 0$:

$$f(t, y) = \left(y - \frac{t^2}{2} + \frac{t^4}{8} + \dots\right) \left(y - 2 - \frac{t^2}{2} + \frac{t^4}{8} + \dots\right) = \left(y - \frac{t^2}{2} + \frac{t^4}{8} + \dots\right) h(t, y).$$

Exempel. Låt $f(x, y) = y^2 - x^3$, så att f är singulär i origo. Då ser vi genast att

$$f(t^2, y) = y^2 - t^6 = (y - t^3)(y + t^3),$$

som är på den önskade formen med $d = 2 = r$, $k = 0$.

Exempel. Låt $f(x, y) = x^3 - y^2x$. Vi har

$$f(t, y) = t(y - t)(y + t),$$

med $d = 1 = k$, $r = 2$.

Nu får det vara nog med exempel. Nu bevisar vi satsen. Vi behöver några Lemman. ²⁸

Lemma 1. Låt $f \in \mathbb{C}[[x]][y]$ vara given av

$$f(x, y) = \sum p_i(x)y^i.$$

²⁸Att skriva snygga bevis för dessa kan vara en del av ett examensarbete på kandidatnivå om skärningstal och relaterade saker. Any takers?

Låt $m_i = \text{mult}_0 p_i$. Antag att det finns ett $R \in \mathbb{N}$ så att $p_i(0) = 0$ för $i < R$, men $p_R(0) \neq 0$. Sätt

$$\nu = \min\left\{\frac{m_i}{R-i} \mid 0 \leq i < R\right\}.$$

- (a) Om $\nu < \infty$, skriv $\nu = \frac{k}{l}$, där $\gcd(k, l) = 1$ och k, l positiva heltal. Då finns det ett tal $\omega \in \mathbb{C}$ så att

$$f(t^l, t^k(\omega + z)) = t^{kR}g(t, z),$$

där

$$g(t, z) = \sum q_i(t)y^i,$$

och det finns ett $S \in \mathbb{N}$ så att $S \leq R$ och $q_i(0) = 0$ för $i < S$, men $p_S(0) \neq 0$.

- (b) Om $l \neq 1$, dvs. om ν inte är ett heltal, så är $S < R$.

- (c) Om $l = \infty$ så är $f(x, 0) = 0 \in \mathbb{C}[[x]]$.

Lemma 2. Låt $f \in \mathbb{C}[[x]][y]$,

$$f(x, y) = \sum p_i(x)y^i.$$

Antag att det finns ett $R \in \mathbb{N}$ så att $p_i(0) = 0$ för $i < R$, men $p_R(0) \neq 0$. Då finns en potensserie $p(t)$ utan konstantterm och ett positivt heltal d , så att $f(t^d, p(t)) = 0$.

Bevis av Satsen. Applicera Lemma 2 upprepade gånger.

20.2 Alternativ definition av skärningstalet.

Låt $f, g \in \mathbb{C}[x, y]$. Skriv, som i satsen ovan,

$$f(t^d, y) = t^k(y - p_1(t)) \cdots (y - p_r(t))u(t, y).$$

Vi definierar skärningstalet i origo som

$$I_O(f, g) = \frac{1}{d} \left(k \cdot \text{mult}_{y=0} g(0, y) + \sum_{i=1}^r \text{mult}_{t=0} g(t^d, p_i(t)) \right).$$

Anmärkning. Talet $k \neq 0$ bara om f har faktorn x , dvs. om motsvarande kurva innehåller y -axeln som komponent. Annars får formeln det behagligare utseendet

$$I_O(f, g) = \frac{1}{d} \sum_{i=1}^r \text{mult}_{t=0} g(t^d, p_i(t)).$$

Exempel. Låt $g(x, y) = y - ax$ och $f(x, y) = y^2 - x^3$, som i exemplet ovan. Vi får

$$I_0(f, g) = \frac{1}{2}(\text{mult}_0 g(t^2, t^3) + \text{mult}_0 g(t^2, -t^3)) = \frac{1}{2}(\text{mult}_0(t^3 - at^2) + \text{mult}_0(t^3 + at^2)).$$

Detta är 2 om $a \neq 0$, och 3 om $a = 0$, vilket överensstämmer med räkningar i tidigare kapitel.

20.3 Bevis för axiomen för denna definition.

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.