UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2015:29

En hastig inblick i den algebraiska geometrin

Adrian Wennström

Examensarbete i matematik, 15 hp
Handledare och examinator: Veronica Crispin Quinonez
Augusti 2015

Department of Mathematics
Uppsala University

Sammanfattning

Genom en hastig genomgång av de algebraiska mängderna, ideal i $k[x_1, \ldots, x_n]$, koordinatringar, Zariskitopologin, och dessas grundläggande egenskaper och genom en genomgång av Bezouts sats, Buchbergers algoritm, och ett par moderna algebraisk-geometriska strukturer ges en hastig inblick i den algebraiska geometrin.

Innehåll

1 Förord

Geometrin hör, precis som talteorin och möjligen den elementära algebran, till matematikens äldsta grenar. Redan de gamla grekerna ägnade sig åt geometri, men de var knappast de första. De tidigaste skriftkulturerna i Mesopotamien ägnade sig åt olika former av geometri. Man kan visserligen säga att de undersökningar som antikens matematiker ägnade sig åt framstår som rätt så blygsamma för en modern betraktare, Archimedes ägnar till exempel en av sina böcker till att undersöka hur stor en cirkel är, men deras metoder framstår i och för sig som ännu blygsammare.

Långt senare uppstod idéer om koordinatsystem, elementär algebra, matematisk analys, topologi och andra numera självklara verktyg. Dessa verktyg har inte bara påverkat hur man löser matematiska problem utan också vilka frågor som ställs. Just koordinatsystemen och den elementära algebran ger upphov till en uppsjö frågeställningar. Dessa skulle kunna sägas vara den algebraiska geometrins ursprung. Det visar sig nämligen att man bland annat kan finna enkla ekvationer vars lösningsmängder är cirklar, parabler, ellipser, sfärer eller andra geometriska figurer. Man kan ställa sig frågor som huruvida nollställena till $x^2 + y^2 - 1$ går att parametrisera, i hur många punkter olika kurvor möts, ifall de går att klassificera på något lämpligt vis, om en viss kurva verkligen är lösningsmängden till någon uppsättning polynomekvationer och så vidare.

Frågor som dessa är de som den algebraiska geometrin ursprungligen avhandlade. I spåren av tidigare århundradens undersökningar har en teoribildning växt fram som dels behandlar helt nya frågeställningar, dels använder helt andra metoder och som ibland knappast framstår som särskilt geometrisk. Den moderna algebraiska geometrin är egentligen alldeles för stor och alldeles för invecklad för att kunna sammanfattas i ett examensarbete på C-nivå, men en hastig inblick i dess värld är trots detta inte helt omöjlig. För att ge sig i kast med någonting sådant krävs en viss avgränsning. Oavsett hur man bär sig åt är det ohjälpligt att bara en liten del av dess resultat och metoder går att redovisa i ett så komprimerat format.

Det är med andra ord inte mycket mer än studieobjektens allra mest grundläggande egenskaper och en liten bit kuriosa som ryms i dessa 30-talet sidor, men det innebär inte för den sakens skull att de är helt innehållslösa. Början utgörs av en snabb introduktion till de affina algebraiska mängderna, idealens plats i teorin, ringar som hör till dessa och en viss topologi. Efter detta redovisas en av teorins klassiska satser i en lika klassisk form. Bezouts sats ger dels en indikation på hur svåra den algebraiska geometrins frågor kan vara, både när det gäller att ställa dem och att besvara dem. Satsen ger oss också ett naturligt sammanhang för att ta upp de projektiva algebraiska mängderna. Därefter ger vi oss i kast med något som kanske inte egentligen brukar höra den algebraiska geometrin till, men som ändå är intressant i sammanhanget. Buchbergers algoritm och Gröbnerbaserna gör idealen och därmed de algebraiska mängderna mer gripbara på ett häpnadsväckande sätt, men utgör på samma gång en besvikelse. Allt är inte guld som glimmar, och bara för att det går att svara på frågor algoritmiskt så betyder inte det att algoritmerna är särskilt effektiva. Slutligen görs en allt för otillräcklig ansats att öppna dörren till den moderna teorin genom en introduktion till algebraiska varieteter, kärvar[1] och scheman[2].

[1] Fr: faisceaux, En: sheaves
[2] Fr: schémas, En: schemes

2 Vissa grundläggande begrepp

Den algebraiska geometrin uppkom ur studiet av algebraiska kurvor, det vill säga kurvor i planet som är nollställen till polynomekvationer. Mängden av alla gemensamma nollställen till en mängd polynom kallas för en *algebraisk mängd*[3]. Inom den algebraiska geometrin är vi egentligen bara intresserade av polynom över kroppar. Vi använder den vanliga beteckningen $k[x_1, \ldots, x_n]$ för att beteckna mängden av alla polynom över kroppen k i variablerna $x_1, x_2, \ldots, x_n$ och definierar begreppet algebraisk mängd som följer.

Definition 1. *Låt k vara en kropp och låt $P \subseteq k[x_1, \ldots, x_n]$ för något n. Då kallar vi mängden*

$$V = \{(x_1, \ldots, x_n) \in k^n : p(x_1, \ldots, x_n) = 0 \text{ för varje } p \in P\}$$

för en affin algebraisk mängd över k. Om P är en mängd av polynom över k så kallar vi $\mathbf{V}(P)$ för P:s nollställemängd eller dess algebraiska mängd.

Vi illustrerar begreppet med ett enkelt exempel, nämligen enhetscirkeln i $\mathbb{R}^2$.

Exempel 1. *Enhetscirkeln är en affin algebraisk mängd eftersom den utgörs av nollställena till $x^2 + y^2 - 1 \in \mathbb{R}[x, y]$.*

Föremålet för den algebraiska geometrins undersökningar är alltså, åtminstone i den klassiska teorin, den affina algebraiska mängden. Det visar sig emellertid att det går precis lika bra, och till och med bättre, att studera ideal istället för algebraiska mängder. Som bekant är ett ideal en delmängd av en ring som är sluten med avseende på addition och som dessutom är sluten med avseende på multiplikation med hela ringen. Ett elementärt resultat är att $k[x_1, \ldots, x_n]$ är en ring. Given en mängd $P \subseteq k[x_1, \ldots, x_n]$ kan vi bilda idealet $\langle P \rangle$, som består av alla linjära kombinationer av element ur P över $k[x_1, \ldots, x_n]$. Vi definierar idealet av en delmängd av k^n.

Definition 2. *Låt $M \subseteq k^n$. Vi bildar idealet*

$$\mathbf{I}(M) = \langle p \in k[x_1, \ldots, x_n] : p(x) = 0 \text{ för varje } x \in M \rangle$$

och kallar det för M:s ideal.

Utöver ideal associerar vi också en särskild ring till varje algebraisk mängd, bland annat för att vi ska kunna finna en naturlig definition av isomorfier mellan algebraiska mängder. Ringen kallar vi för *koordinatringen.*

Definition 3. *Låt V vara en algebraisk mängd i k^n. V:s* koordinatring, *$\Gamma(V)$ är ringen*

$$\Gamma(V) = k[x_1, \ldots, x_n]/\mathbf{I}(V).$$

Vi definierar också en topologi över k^n med hjälp av våra algebraiska mängder.

Definition 4. Zariskitopologin *över k^n definieras så att en delmängd $X \subset k^n$ är sluten om den är en algebraisk mängd.*

[3]Det förekommer också att man kallar dessa för *varieteter* av franskans *variété*. Detta begrepp används numera också om ett snarlikt objekt som vi kommer att återkomma till senare.

Det framgår ännu inte riktigt vad dessa begrepp ska användas till, men vi utökar exemplet med enhetscirkeln.

Exempel 2. *Enhetscirkeln i $\mathbb{R}^2$ är en algebraisk mängd eftersom den är mängden av alla gemensamma nollställen till polynomet $P = (x^2 + y^2 - 1)^2$. Den är därmed också en sluten mängd i Zariskitopologin på $\mathbb{R}^2$. Dess ideal, $\mathbf{I}(P)$, är $\langle x^2 + y^2 - 1 \rangle$. Dess koordinatring, $\Gamma(\mathbf{V}(P))$, är $\mathbb{R}[x, y]/\langle x^2 + y^2 - 1 \rangle$.*

3 Grundläggande egenskaper

Vi har precis definierat några av de grundläggande begreppen i den algebraiska geometrin. Det är egenligen långt ifrån alla som den moderna algebraiska geometrin behandlar. Utöver de föga moderna projektiva rummen saknas de strukturer som enligt Dieudonné (1974, s. 169) inte bara har revolutionerat den algebraiska topologin och differentialtopologin, utan de som:

> ... ont aussi complètement renouvelé les concepts et les méthodes de la Géométrie algébrique, ...

Vi ska naturligtvis återkomma till dessa nyare begrepp lite senare, men de algebraiska mängdernas mest grundläggande egenskaper var kända långt innan Dieudonnés 1900-tal, och kräver egentligen inte särskilt avancerade metoder.

3.1 Hilberts bassats

Så som algebraiska mängder definierades ovan finns det ingenting som säger att en sådan nödvändigtvis måste gå att beskriva med ett ändligt antal polynom. Det visar sig dock att vilken algebraisk mängd som helst är mängden av de gemensamma nollställena till en ändlig polynommängd. Satsen är egentligen en sats om ideal och kallas Hilberts bassats efter sin upptäckare.

För att uttrycka oss lite klarare lånar vi framställningen från Grillet (2007, III.11). Vi börjar med ett par definitioner.

Definition 5. *Låt R vara en kommutativ ring. En uppräkning av ideal i R, $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$, kallas för en stigande kedja om $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$.*

Definition 6. *En kommutativ ring R kallas Noethersk om det i varje stigande kedja av ideal, $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$, finns ett n så att $m \geq n \implies \mathfrak{a}_n = \mathfrak{a}_m$.*

Grillet visar kvickt att en ring är Noethersk om och endast om alla dess ideal är ändligt genererade. Vi lånar det som ett lemma, och hänvisar till beviset av sats III.11.1 ur Grillet (2007).

Lemma 1. *Låt R vara en kommutativ ring. R är Noethersk om och endast om alla ideal i R är ändligt genererade.*

Vad ska vi nu med det till? Jo, Grillet fortsätter med den sats som han kallar Hilberts bassats. Vi lånar in den också, men hänvisar den bevissugna läsaren till sats III.11.2 i Grillet (2007).

Lemma 2. *Låt R vara en kommutativ ring. Om R är Noethersk så är också $R[X]$ Noethersk.*

Vi lånar lemma III.6.3 från Grillet (2007).

Lemma 3. *Låt k vara en ring, då gäller att $k[x_1, \ldots, x_n] \cong k[x_1, \ldots, x_{n-1}][x_n]$.*

Sin vana trogen har Grillet lämnat det som vi kommer att kalla för Hilberts bassats som en övning, lyckligtvis är det ett en enkel följdsats till Lemma 2.

Sats 1 (Hilberts bassats)**.** *Låt k vara en kropp. Då är varje ideal i $k[x_1, \ldots, x_n]$ ändligt genererat.*

Bevis. Vi visar först att k är Noethersk, sedan visar vi genom induktion över antalet variabler att $k[x_1, \ldots, x_n]$ är Noethersk. Att k verkligen är Noethersk inses lätt. Kroppar har bara två ideal, $\{0\}$ och hela kroppen. Det första av dessa ideal är $\langle 0 \rangle$, som ju är ändligt genererat. Det andra idealet, hela kroppen, kan skrivas som $\langle 1 \rangle$ och är därför ändligt genererat. Alltså är alla ideal i k ändligt genererade, och enligt Lemma 1 kan vi dra slutsatsen att k är Noethersk. Vi inleder nu själva induktionsbeviset.

Basfall Låt k vara som ovan. Då är k Noethersk. Enligt Lemma 2 är $k[x_1]$ Noethersk.

Induktionsantagande Antag att $k[x_1, \ldots, x_{n-1}]$ är Noethersk.

Induktionssteg Vi vill visa att $k[x_1, \ldots, x_n]$ är Noethersk. Eftersom $k[x_1, \ldots, x_{n-1}]$ är Noethersk enligt induktionsantagandet så gäller enligt lemma 3 att $k[x_1, \ldots, x_{n-1}][x_n]$ är Noethersk, och därmed är $k[x_1, \ldots, x_n]$ Noethersk eftersom den är isomorf med $k[x_1, \ldots, x_{n-1}][x_n]$.

Vi drar slutsatsen att $k[x_1, \ldots, x_n]$ är Noethersk för alla n. Enligt Lemma 1 är alla ideal i $k[x_1, \ldots, x_n]$ ändligt genererade. □

3.2 Hilberts nollställesats

Hilbert är inte bara upphovsman till bassatsen med samma namn, han är också upptäckare av den så kallade nollställesatsen (även kallad hans nullstellenzats). Satsen klargör vilka ideal som ligger i $\mathbf{I}$:s målmängd. Vi börjar med en definition som kommer att behövas för att formulera satsen.

Definition 7. *Låt $I \subset k[x_1, \ldots, x_n]$ vara ett ideal, då definierar vi*

$$\sqrt{I} = \{f \in k[x_1, \ldots, x_n] : \textit{Det finns ett } n \in \mathbb{N} \textit{ så att } f^n \in I\}$$

och kallar $\sqrt{I}$ för I:s radikal.

Innan vi ger oss in på själva nollställesatsen ska vi bekanta oss med den så kallade svaga nollställesatsen. För bevis hänvisas läsaren till Cox m.fl. (1997, Sats 4.1.1).

Sats 2 (Den svaga nollställesatsen)**.** *Låt k vara en algebraiskt sluten kropp och $I \subset k[x_1, \ldots, x_n]$ vara ett ideal sådant att $\mathbf{V}(I) = \emptyset$, då är $I = k[x_1, \ldots, x_n]$.*

Det visar sig nämligen att när man väl har visat den svaga nollställesatsen kan man relativt enkelt visa själva nollställesatsen. Satsen gäller bara då k är

algebraiskt sluten och bevisas bland annat av Cox m.fl. (1997, Sats 4.1.2), men då i en lite annorlunda formulering[4].

Sats 3 (Hilberts nollställesats)**.** *Om $I \in k[x_1, \ldots, x_n]$ är ett ideal och k är en algebraiskt sluten kropp, då gäller likheten*

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}.$$

Följden är att $\mathbf{I}$ och $\mathbf{V}$ i själva verket visar sig vara bijektioner mellan de algebraiska mängderna och de radikala idealen, se till exempel sats 4.2.7 i Cox m.fl. (1997) för en mer detaljerad utläggning.

3.3 Algebraiska mängders sammansättning

Det visar sig att algebraiska mängder har en struktur som på sätt och vis påminner om heltalens. Man kan nämligen dela upp algebraiska mängder i två typer, irreducibla och sammansatta. Uppdelningen kan liknas vid heltalens uppdelning i primtal och sammansatta tal, vi kommer att se att det finns en motsvarighet till aritmetikens fundamentalsats.

Vad är då motsvarigheten till primtalen, och vad är motsvarigheten till heltalens multiplikation? Vi definierar först ett par användbara termer. Den första definitionen handlar om topologiska rum. Vi har förstås Zariskitopologin i åtanke.

Definition 8. *Låt X vara ett topologiskt rum. Om varje par $U, V \subset X$ av öppna mängder sådana att $U \cap V = \emptyset$ har egenskapen att $U = \emptyset$ eller $V = \emptyset$ så kallar vi X* irreducibel*.*

Det är inte helt enkelt att förstå hur det här hjälper oss. Tanken är att varje algebraisk mängd V kan betraktas som ett delrum till k^n under delmängdstopologin. Ett exempel på en algebraisk mängd som inte är irreducibel utan som är sammansatt är den som följer.

Exempel 3. *Låt $I = \langle (x^2 + y^2 - 1) \cdot (x^2 - y) \rangle$. Den kvicktänkte läsaren inser att det är unionen av enhetscirkeln och parabeln $y = x^2$ som avses. $\mathbf{V}(I)$ är* inte *irreducibel.*

Betraktar vi den inducerade topologin på $\mathbf{V}(I)$ så ser vi genast att den Zariskiöppna mängden $\mathbb{R}^2 - \mathbf{V}(x^2 - y)$ skär $\mathbf{V}(I)$ i de punkter på enhetscirkeln som inte ligger på parabeln. På samma sätt ser vi att den Zariskiöppna mängden $\mathbb{R}^2 - \mathbf{V}(x^2 + y^2 - 1)$ skär $\mathbf{V}(I)$ i de punkter som ligger på parabeln men inte på enhetscirkeln.

Vi har alltså funnit två öppna delmängder av $\mathbf{V}(I)$ som är disjunkta men som båda är icke-tomma. Därför är $\mathbf{V}(I)$ inte ett irreducibelt rum.

Vi definierar sedan, på samma sätt som Perrin (1995, Mémento d'algèbre 1.2.b), vad ett primideal.

Definition 9. *Ett ideal $\mathfrak{a} \subset R$ är ett primideal* prim *om $R/\mathfrak{a}$ är ett integritetsområde.*

[4] Vår formulering är en ekvivalent formulering som visas som en enkel följdsats se Cox m.fl. (1997, Sats 4.2.6) för detaljerna.

Vi lånar sedan en sats av Perrin (1995, Sats I.3.2) för att koppla samman irreducibla algebraiska mängder och primideal.

Sats 4. *Låt V vara en algebraisk mängd. Då gäller att V är irreducibelt $\iff$ $\mathbf{I}(V)$ är primt $\iff$ $\Gamma(V)$ är ett integritetsområde.*

Vi knyter ihop säcken med ännu en sats(Perrin 1995, Sats I.3.6).

Sats 5. *Varje icketom algebraisk mängd V kan skrivas som en ändlig union $V_1 \cup \cdots \cup V_r$ av irreducibla algebraiska mängder på precis ett sätt så att inget V_i är en delmängd av något annat V_j.*

3.4 Dimension

Det visar sig att problemet att bestämma en algebraisk mängds dimension inte är trivialt. Det kan tyckas självklart att en linje ska vara av dimension ett. Men hur bestämmer man dimensionen av, till exempel, unionen av två linjer? Vad betyder det överhuvudtaget att unionen av en linje och ett plan har en viss dimension? I likhet med Perrin (1995) bestämmer vi redan nu att föra diskussionen enbart för algebraiskt slutna kroppar, och fortsätter sedan direkt med en topologisk definition av dimensionsbegreppet.

Utan att hävda någon som helst originalitet ställer vi upp följande exempel för att förklara tankegången.

Exempel 4. *Låt oss undersöka ett plan i $\mathbb{C}^3$, till exempel $I = \langle z_3 \rangle$. Vi kan lätt finna två Zariskislutna delmängder $\mathbf{V}(\langle z_1, z_2, z_3 \rangle)$ och $\mathbf{V}(\langle z_2, z_3 \rangle)$ av $\mathbf{V}(I)$ som bildar en stigande kedja, men det är inte självklart hur en tredje Zariskisluten delmängd skulle se ut om den samtidigt måste vara irreducibel, måste ha linjen $\{(z_1, 0, 0) \in \mathbb{C}^3 : z_1 \in \mathbb{C}\}$ som delmängd och måste vara en äkta delmängd till $\mathbf{V}(I)$.*

Tanken är med andra ord att en algebraisk mängds dimension bestäms av hur långa stigande kedjor av irreducibla topologiska rum som finns som delmängder. Vi preciserar vad vi menar, och glömmer av bara farten att det finns andra topologier än Zariskitopologin.

Definition 10. *En stigande kedja i X är en uppsättning $X_0, X_1, \ldots, X_n$ av distinkta delmängder till X sådana att $X_0 \subset X_1 \subset \cdots \subset X_n$. Vi säger att en sådan kedja är av längd n.*

Definition 11. *Låt X vara ett topologiskt rum, X:s dimension är densamma som den minsta övre begränsningen av längden av stigande kedjor av irreducibla slutna mängder i X.*

Egentligen är det här inte en särskilt praktisk definition. Det är nämligen inte helt lätt att avgöra huruvida det finns en kedja av en viss längd eller inte. Det kan också vara svårt att avgöra om en enskild mängd är reducibel eller irreducibel. Lyckligtvis finns det fler sätt att beräkna dimensionen av en algebraisk mängd. Till exempel kan vi börja med Krulldimensionen.

Definition 12. *Låt R vara en ring, dess* Krulldimension, $\dim_K(R)$ *är längden av den längsta stigande kedjan av primideal i R.*

Det vore förstås märkligt om det visade sig att dessa två dimensionsbegrepp vore olika. Perrin ger oss följande sats (Perrin 1995, IV.1.7).

Sats 6. *Låt V vara en affin algebraisk varietet och låt $\Gamma(V) = \mathcal{O}_V(V)$ då gäller, om $\dim(V)$ är V:s topologiska dimension, att*

$$\dim(V) = \dim_K(\Gamma(V)).$$

Vi kommer att återvända senare till vad en affin algebraisk varietet är för något, för tillfället är det tillräckligt att postulera att satsen innebär att en algebraisk mängd har samma topologiska dimension som dess koordinatrings Krulldimension.

4 Bezouts sats

Antag att vi har två kurvor i planet som båda är algebraiska mängder. I hur många punkter skär de varandra? Utan vidare reflexion skulle vi säga att det varierar, somliga möts inte överhuvudtaget, andra i ett visst antal punkter och vissa har gemensamma irreducibla komponenter i sin sammansättning. Om vi vidgar våra vyer en aning upptäcker vi att saken blir betydligt mer förutsägbar. Frågan besvaras nämligen elegant av *Bezouts sats* med att antalet skärningspunkter (upp till multiplicitet) för två polynoms algebraiska mängder bara beror på polynomens exponenter. För att alls formulera satsen måste vi först utöka vår begreppsapparat.

4.1 Projektiv algebraisk geometri

4.1.1 Det projektiva planet

Det projektiva planet, $\mathbb{P}^2(\mathbb{R})$, består utöver det vanliga planet av extra punkter som representerar parallella linjers mötesplatser i oändligheten. En konkret, men föga intuitiv beskrivning fås genom att betrakta de projektiva rummen genom de särskilda *homogena koordinater* som beskriver punkterna. För en mer utförlig bakgrund, där bland annat kopplingen till renässansens måleri behandlas mer utförligt hänvisas läsaren till Panofsky (1960) och Kline (1960).

De homogena koordinaterna för en given punkt i $\mathbb{P}^n(k)$ är element ur $k^{n+1} - \{0\}$. Tanken är att punkterna på formen

$$(x_1, x_2, \ldots, x_n, 1) \in k^{n+1} - \{0\}$$

ska motsvara punkterna i k^n på det uppenbara sättet och att koordinaterna

$$(x_1, x_2, \ldots, x_n, 0) \in k^{n+1} - \{0\}$$

ska motsvara punkter i oändligheten. Om $p = (x_1, x_2, \ldots, x_n, 0)$ är en punkt i oändligheten så är tanken det ska vara *ändpunkten*[5] till varje linje som är parallell med linjen som passerar genom origo och genom $(x_1, x_2, \ldots, x_n)$.

Det här är egentligen inte ett särskilt bra koordinatsystem, vi får dels flera olika sätt att skriva varje punkt i oändligheten, och dels får vi oändligt många

[5] Vad nu det betyder i sammanhanget. Det handlar förstås inte om ändpunkter i någon egentlig mening eftersom linjer inte har sådana.

koordinater över. För att göra koordinaterna mer praktiska utökar vi koordinatsystemet och inför en ekvivalensrelation $\sim$ som är sann när två koordinater representerar samma punkt i det projektiva planet.

Definition 13. *Vi definierar en relation $\sim$ på $k^{n+1} - \{0\}$ som följer. Vi säger att $(x_1, x_2, \ldots, x_n, z_1) \sim (y_1, y_2, \ldots, y_n, z_2)$ om något av följande två villkor är uppfyllt.*

1. *$z_1 \neq 0$, $z_2 \neq 0$ och $(\frac{x_1}{z_1}, \frac{x_2}{z_1}, \ldots, \frac{x_n}{z_1}, 1) = (\frac{y_1}{z_2}, \frac{y_2}{z_2}, \ldots, \frac{y_n}{z_2}, 1)$*
2. *$z_1 = z_2 = 0$ och det finns ett $c \in k - \{0\}$ sådant att $c(x_1, x_2, \ldots, x_n, 0) = (y_1, y_2, \ldots, y_n, 0)$*

Nu är vi mogna att definiera det projektiva rummet. Det består helt enkelt av ekvivalensklasserna under $\sim$.

Definition 14. *Det projektiva rummet $\mathbb{P}^n(k)$ är mängden $(k^{n+1} - \{0\})/\sim$*

4.1.2 Homogena polynom

Tyvärr räcker det inte med de projektiva rummen. Vi vill kunna definiera någon form av motsvarighet till de affina algebraiska mängderna i $\mathbb{P}^n(k)$. Tyvärr kan vi inte definiera en projektiv algebraisk mängd som nollställena till ett polynom ur $k[x_1, \ldots, x_{n+1}]$ eftersom olika projektiva koordinater för samma punkt kan anta olika värden. Det kan till och med förekomma att ett polynom är noll för vissa av en punkts homogena koordinater men inte för andra. Det visar sig att vi i alla fall kan få väldefinierade nollställen genom att använda så kallade homogena polynom.

Definition 15. *Låt $c \in k$ och $c \cdot x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \in k[x_1, \ldots, x_n]$ vara ett polynom bestående av en term[6]. Dess* totala grad *är $\sum_{k=1}^{n}(i_k)$.*

Definition 16. *Ett polynom $p \in k[x_1, \ldots, x_{n+1}]$ är* homogent *om varje term har samma totala grad.*

En mycket enkel sats från Cox m.fl. (1997, Sats 8.2.4) säger oss att de homogena polynomen är polynomen vi sökte.

Sats 7. *Låt $f \in k[x_1, \ldots, x_{n+1}]$ vara ett homogent polynom. Om x är en representant i homogena koordinater för en punkt $p \in \mathbb{P}^n(k)$ och $f(x) = 0$ så gäller att $f(x') = 0$ för alla representanter x' sådana att $x' \sim x$. Dessutom gäller att $\mathbf{V}(f) = \{p \in \mathbb{P}^n(k) : f(p) = 0\}$ är en väldefinierad delmängd till $\mathbb{P}^n(k)$.*

4.1.3 Projektiva motsvarigheter till affina begrepp

När vi nu har definierat ett par grundläggande objekt kan vi definiera ett par projektiva motsvarigheter till ett par affina begrepp. Vi börjar med att definiera begreppet projektiv algebraisk mängd.

Definition 17. *Låt $f_1, f_2, \ldots, f_s \in k[x_1, \ldots, x_{n+1}]$ vara en uppsättning homogena poloynom. Vi kallar*

$$\mathbf{V}(f_1, f_2, \ldots, f_s) = \{(x_1, x_2, \ldots, x_{n+1}) \in \mathbb{P}^n(k) : f_i(x_1, x_2, \ldots, x_{n+1}) = 0 \text{ för } 1 \leq i \leq s\}$$

för den projektiva algebraiska mängden *som definieras av polynomen f_i.*

[6] Vi kallar det inte för ett monom eftersom vi vill använda det begreppet senare i en något annorlunda betydelse.

Om de algebraiska mängderna har motsvarigheter i det projektiva rummen, vad är då idealens motsvarigheter? Idealen motsvaras av de *homogena idealen*. Vi börjar med att definiera vad en *homogen komponent* är.

Definition 18. *Låt $f \in k[x_1, \ldots, x_{n+1}]$ vara ett polynom. Ett polynom $g \in k[x_1, \ldots, x_{n+1}]$ kallas för en* homogen komponent *av f om det är homogent och är summan av alla termer i f av samma totala grad som g. Vi säger att g är f:s* homogena komponent av grad *d om g är summan av alla termer i f av total grad d.*

Cox m.fl. ger sedan följande definition av ett homogent ideal.

Definition 19. *Ett ideal i $I \subset k[x_1, \ldots, x_{n+1}]$ kallas för* homogent *om varje homogen komponent av varje polynom i I också ingår i I.*

Den projektiva algebraiska geometrin har utöver detta direkta motsvarigheter till avbildningarna $\mathbf{V}$ och $\mathbf{I}$, Hilberts bassats[7], Hilberts nollställesatser, unik uppdelning i irreducibla element och en hel del annat, men eftersom vi främst kommer att använda den för att kunna formulera Bezouts sats lämnas detaljerna åt läsarens fantasi eller vidare läsning[8]. En intressant dualitetsprincip dyker också upp vid vidare läsning.

4.1.4 Multiplicitet

Polynoms nollställen har en egenskap vi kallar för multiplicitet. Ofta, som i fallet $\mathbb{C}[X]$ vet vi att det finns ett visst antal nollställen, men vissa av dem är i någon bemärkelse dubbla eller till och med av ännu högre multiplicitet. Lite beroende på när vi frågar oss vad ett nollställe har för multiplicitet menar vi lite olika saker, men i princip handlar det om att man kan bryta ut en vissa faktor med någon särskild exponent ur någon särskild funktion. I vårt fall finns det naturligtvis inte någon funktion överhuvudtaget, själva idén är att vi vill finna något multiplicitetsbegrepp som kan användas om gemensamma nollställen till *flera* funktioner, och med det önskemålet att om funktionerna råkar vara två homogena polynom av ordning m respektive n så ska summan av multipliciteterna för alla nollställen bli $m \cdot n$[9].

Man kan göra på ett par olika sätt, ett relativt enkelt är det som används av både Cox m.fl. (1997) och Brieskorn m.fl. (1981), nämligen genom en funktion som vi ska kalla *resultanten* av två polynom. Vi lånar återigen framställningen från Grillet (2007).

Definition 20. *Låt $f(X) = a_m(X - \alpha_1)\cdots(X - \alpha_m)$ och $g(X) = b_n(X - \beta_1)\cdots(X - \beta_n)$ vara polynom av grad m respektive n med koefficienter i en kropp K och rötterna $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ i den algebraiska tillslutningen till K.* Resultanten *av f och g är då*

$$\mathrm{Res}(f, g) = a_m^n b_n^m \prod_{i,j} (\alpha_i - \beta_j)$$

[7] Det vi kallar för ett homogent ideal är i själva verket ett ideal i en polynomring över en kropp, så det är till och med samma sats det handlar om.

[8] Se då till exempel kapitel 8 i Cox m.fl. (1997) eller kapitel 2 i Perrin (1995) för en hastigare genomgång

[9] Här har vi formulerat Bezouts sats i smyg, så att vi vet ungefär vart vi är påväg.

Definitionen är en aning oortodox. Det framgår tydligt att resultanten är noll om och endast om f och g delar ett nollställe i den algebraiska tillslutningen till K. Olyckligtvis behöver vi veta vad det är för rötter det är frågan om. Grillet visar att det finns ett lättare sätt att beräkna resultanten. För bevis, se Grillet (2007, Sats IV.7.2).

Sats 8. *Låt* $f = a_m x^m + \cdots + a_0 x^0$ *och* $g = a_n x^n + \cdots + a_0 x^0$. *Resultanten* $\operatorname{Res}(f, g)$ *kan beräknas med determinanten*

$$\operatorname{Res}(f,g) = \begin{vmatrix} a_m & a_{m-1} & \cdots & a_0 & & \\ & \ddots & \ddots & & \ddots & \\ & & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & & \\ & \ddots & \ddots & & \ddots & \\ & & b_n & b_{n-1} & \cdots & b_0 \end{vmatrix},$$

av $(m+n \times m+n)$*-matrisen, vars första* n *rader består av koefficienterna till* f *förskjutna ett steg till höger per rad, vars* m *sista rader består av koefficienterna till* g *förskjutna ett steg till höger för varje rad efter rad* $n+1$*, och som i övrigt är fylld av nollor.*

För tydlighetens skulle kommer här ett exempel.

Exempel 5. *Låt* $f = (x-1)(x-3) = x^2 - 4x + 3$ *och låt* $g = (x+1)(x-1) = x^2 - 1$. *Resultanten av* f *och* g *är*

$$\operatorname{Res}(f,g) = \begin{vmatrix} 1 & -4 & 3 & 0 \\ 0 & 1 & -4 & 3 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{vmatrix} = \begin{vmatrix} 1 & 3 & 0 \\ 0 & -4 & 3 \\ 1 & -1 & 0 \end{vmatrix} - \begin{vmatrix} 1 & -4 & 3 \\ 0 & 1 & -4 \\ 1 & 0 & -1 \end{vmatrix} = 12 - 12 = 0.$$

Som resultanter har definierats ovan kan de inte användas med polynom i flera variabler. För att råda bot på den bristen börjar vi med att visa en sats om resultanter över faktoriella[10] ringars polynomringar.

Sats 9. *Låt* R *vara en faktoriell ring, låt dessutom* $f, g \in R[x]$ *och låt* K *vara* R*:s fraktionskropp. Om vi beräknar resultanten av* f *och* g *som om de vore polynom över* K *och finner att* $\operatorname{Res}(f, g) = 0$*, då har* f *och* g *en gemensam delare i* $R[x]$ *som inte ligger i* R.

Bevis. Om $\operatorname{Res}(f, g) = 0$ så har f och g ett gemensamt nollställe i den algebraiska tillslutningen till K. Eftersom detta nollställe, låt oss kalla det α, är algebraiskt över K så finns ett unikt irreducibelt moniskt polynom $m \in K[x]$ α som nollställe (Svensson 2001, Sats 18.34). Dessutom delar m varje annat polynom i $K[x]$ som har α som nollställe (Svensson 2001, Sats 18.34).

Vi vet alltså att $f = f_m m$ för något $f_m \in K[x]$ och att $g = g_m m \in K[x]$. Det återstår bara att visa att vi kan finna en gemensam delare även i $R[x]$. Antag att f_m, g_m och m inte ligger i $R[x]$, om de gjorde det vore ju saken redan avgjord. Det inses lätt att om inte $m \in R[x]$ så finns ett polynom i $M \in R[x]$ sådant att $M = cm$ för något $c \in R$. Vi kan därför skriva $f = f_m m = \frac{f_m}{c} cm = \frac{f_m}{c} M$

[10] Med faktoriell ring avses engelskans *Unique Factorisation Domain*.

och på samma sätt kan vi skriva $g = \frac{g_m}{c}M$. Vidare vet vi att $M = dM_p$ för ett primitivt polynom[11] $M_p \in R[x]$ och en konstant i R. Vi vet att $M_p \in R[x]$ är irreducibelt i $K[x]$ eftersom det kan skrivas som $\frac{c}{d}m$ och m är irreducibelt. Alltså har vi funnit ett primitivt polynom $M_p \in R[x]$ som är irreducibelt betraktat som polynom i $K[x]$, enligt Svensson (2001, Sats 17.38) är M_p också reducibelt i $R[x]$.

Vi ser att $f = \frac{f_m}{cd}dM = \frac{f_m}{cd}cdm = f_m m$ och fortsätter därför att faktorisera $\frac{f_m}{cd}$. På ett liknande sätt fortsätter vi genom att välja ut en rot β_1 till f_m i den algebraiska tillslutningen till K. Vi hittar åter det unika minsta moniska irreducibla polynom som har β_1 som nollställe och konstaterar att detta polynom, kalla det f_1, delar f_m i $K[x]$ så att $f_m = qf_1$ där $q \in K[x]$. Men vi kan omvandla f_1 till ett primitivt irreducibelt polynom i $R[x]$ precis som vi gjorde med m och får då att $f = c_1 q_1 f_1 M_p$ där $c_1 \in K$, $q_1 \in K[x]$ och f_1, M_p är primitiva irreducibla polynom i $R[x]$. Om vi fortsätter på samma sätt så kommer vi till slut att ha faktoriserat f i $K[x]$ så att $f = cf_1 f_2 \cdots f_i M_p$ där $c \in K$, $f_n \in R[x]$ och $M_p \in R[x]$ och där dessutom f_n och M_p är primitiva irreducibla polynom i $R[x]$. Vi tillämpar ett analogt resonemang på g och får en liknande faktorisering $g = dg_1 g_2 \cdots g_j M_p$.

Problemet är bara att vi inte kan garantera att dessa två faktoriseringar verkligen fungerar i $R[x]$. Om c eller d inte ligger i R så kommer inte operationen att vara väldefinierad. Vi vet dock att $R[x]$ är en faktoriell ring eftersom R är faktoriell (Svensson 2001, Sats 17.39), så det måste finnas någon unik faktorisering av f sådan att $f = C\phi_1\phi_2 \cdots \phi_k$ där $C \in R$ och ϕ_n är irreducibla primitiva polynom (Grillet 2007, Lemma III.10.8). Antag att $c = \frac{a_f}{b_f}$, då ser vi att $b_f f = a_f f_1 f_2 \cdots f_i M_p$, så $b_f f$ har en unik faktorisering i irreducibla element[12]. Men, om det nu vore så att f och $b_f f$ hade olika uppdelningar i irreducibla element, då skulle ju $b_f f$ ha två uppdelningar

$$b_f f = a_f f_1 f_2 \cdots f_i M_p = b_f C\phi_1\phi_2 \cdots \phi_k.$$

Eftersom R och $R[x]$ är faktoriella inser vi att det måste vara samma uppdelning i irreducibla element, och i synnerhet att M_p är en delare till f. Genom att tillämpa ett liknande resonemang inser vi att M_p även delar g. Alltså har f och g en gemensam delare i $R[x]$. □

Det går alltså att beräkna resultanten av två givna polynom på ett meningsfullt sätt oavsett hur många variabler det handlar om så länge vi väljer ut en variabel. Vi förtydligar vilken vi menar genom följande definition.

Definition 21. *Om $f, g \in k[x_1, \ldots, x_n]$ är polynom i n variabler, då är*

$$\mathrm{Res}(f, g) : k[x_1, \ldots, x_{n-1}][x_n] \to k[x_1, \ldots, x_{n-1}]$$

resultanten i polynomringen av $k[x_1, \ldots, x_{n-1}]$.

Vi ska låna in ett par satser ur Brieskorn m.fl. (1981). Vi börjar med att konstatera att resultanten av två homogena poloynom är ett homogent polynom (Brieskorn m.fl. 1981, Sats 4.4.8).

[11] Med *primitivt polynom* avses ett icke-konstant polynom med relativt primitiva koefficienter. Se Svensson (2001, Definition 17.34)

[12] Eftersom $a_f \in R$ så har även den en uppdelning i irreducibla element.

Sats 10. *Låt $f, g \in k[x_1, \ldots, x_n]$ vara två homogena polynom av grad l respektive m, då är* $\mathrm{Res}(f, g)$ *noll eller ett homogent polynom av grad $l \cdot m$.*

Vi lånar också en sats om polynom i två variabler. För bevis, se Brieskorn m.fl. (1981, Sats 4.4.7).

Sats 11. *Låt k vara algebraiskt sluten och låt $f \in k[x, y]$ vara ett nollskilt homogent polynom av grad n. Då finns n stycken par $(a_i, b_i) \in k^2$ och ett $a \in k$ så att*

$$f(x, y) = a \prod_{i=1}^{n} (b_i x - a_i y),$$

där paren (a_i, b_i) är entydigt bestämda sånär som på en faktor ur k.

Det är uppenbart att paren (a_i, b_i) svarar mot f:s nollställen. Vi definierar multiplicitet för tvådimensionella homogena polynom.

Definition 22. *Låt k vara algebraiskt sluten och låt $f \in k[x, y]$ vara ett homogent polynom, låt $(a, b) \in k^2$ vara ett nollställe till f. Vi säger då att f:s multiplicitet i (a, b), är det största n för vilket $(bx - ay)^n$ delar f.*

En följdsats till sats 11 är också på sin plats.

Sats 12. *Låt k vara algebraiskt sluten och låt $f \in k[x, y]$ vara ett homogent polynom av grad n. Om vi betraktar paren (a_i, b_i) som projektiva koordinater i rummet $\mathbb{P}^1(k)$ så är summan av de projektiva nollställenas multipliciteter precis n.*

Bevis. Enligt sats 11 kan vi skriva

$$f = a \prod_{i=1}^{n} (b_i x - a_i y).$$

Eftersom k är en kropp kan vi konstruera nya koefficienter c_i sådana att

$$c_i = \begin{cases} b_i & \text{om } b_i \neq 0 \\ 1 & \text{om } b_i = 0 \end{cases}$$

och därmed skriva om f så att vi istället får

$$f = a \prod_{i=1}^{n} c_i \prod_{i=1}^{n} \left(\frac{b_i}{c_i} x - \frac{a_i}{c_i} y\right).$$

Dessutom kan vi, i de fall $b_i = 0$ bryta ut $-a_i$ så att de faktorerna blir endast blir x.

Vi ser att för varje nollställe med koordinaterna $(x_i, 1)$ på den projektiva linjen över k, finns en faktor $(x - x_i)^{m_i}$ i f där m_i är nollställets multiplicitet. Vi ser också att om punkten i oändligheten, $(1, 0)$, är ett nollställe så finns en faktor x^m i f där m är multipliciteten i oändligheten. Det är också tydligt att dessa faktorer tillsammans blidar en produkt av n homogena polynom av grad 1. Alltså är summan av multipliciteterna $m_1, \ldots, m_i, m$ exakt n. □

Allt som fattas är nu en definition av multiplicitet för nollställena till två homogena polynom. Vi nöjer oss, precis som Brieskorn m.fl. (1981), med ett specialfall.

Definition 23. *Låt $F, G \in k[x, y, z]$ vara två homogena polynom av grad m respektive n. Låt F och G tillsammans uppfylla följande villkor:*

1. $\mathrm{Res}(F, G) \neq 0$
2. *För varje par av distinkta gemensamma nollställen $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ och $\beta = (\beta_1, \beta_2, \beta_3)$ gäller att linjen som sammanbinder dem inte korsar $(0, 0, 1)$.*

Då kan vi definiera multipliciteten *av en punkt i $\mathbf{V}(F) \cap \mathbf{V}(G)$. Vi beräknar resultanten $R = \mathrm{Res}(F, G)$ och definierar multipliciteten i punkten $p = (x, y, z) \in \mathbf{V}(F) \cap \mathbf{V}(G)$, $\nu_p(F, G)$, som multipliciteten av (x, y) som nollställe till R.*

Det vore förstås lämpligt att kunna definiera multipliciteten av nollställena alldeles oavsett hur de ligger i förhållande till origo, annars skulle bara vissa algebraiska mängders snitt ha multipliciteter. Vi gör det genom att transformera F och G så att eventuella nollställen som ligger på en och samma linje från origo inte längre gör det. Det visar sig lite mer specifikt att om vi transformerar $\mathbb{P}^2(\mathbb{C})$ med någon av transformationerna i $GL(3, \mathbb{C})$ så påverkas inte snittpunktsmultipliciteten. Vi lånar satsen från Brieskorn m.fl. (1981, Lemma 6.1.3)

Sats 13. *Snittpunktsmultipliciteten $\nu_p(F, G)$ för en punkt $p \in \mathbb{P}^2(\mathbb{C})$ beror inte på valet av koordinatsystem*[13]*.*

Det viktiga i sammanhanget är att de linjära transformationerna som det är frågan om kommer ur $GL(3, \mathbb{C})$ och inte ur $GL(2, \mathbb{C})$. Det betyder att vi, till skillnad från i det vanliga fallet, kan räkna translation av ändliga punkter som en linjär transformation eftersom de motsvaras av matriser på formen

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}.$$

Det visar sig att det räcker med translation av ändliga punkter för att bli av med nollställen som ligger på samma linje genom origo eller på $(0, 0, 1)$. Detta inses lätt genom att varje par av punkter i snittet mellan $\mathbf{V}(F)$ och $\mathbf{V}(G)$ bildar ett endimensionellt vektorrum av translationer som orsakar just de två punkterna att hamna på samma linje. Eftersom det bara rör sig om ett ändligt antal endimensionella vektorrum kan vi nöja oss med att välja punkter ur $\mathbb{C}^2$ som inte ligger i någon av dessa. Om vi dessutom undviker de ändlig många translationer som flyttar punkter till $(0, 0, 1)$ så har vi funnit en transformation ur $GL(3, \mathbb{C})$ som gör att vi får en väldefinierad nollställemultiplicitet. Vi utvidgar multiplicitetsbegreppet.

Definition 24. *Om $\mathrm{Res}(F, G) \neq 0$ men det finns en punkt p som saknar väldefinierad snittpunktsmultiplicitet enligt definition (23), då finner vi en transformation $T \in GL(3, \mathbb{C})$ sådan att $\nu_{T(p)}(F \circ T, G \circ T)$ är väldefinierad och skriver*

$$\nu_p(F, G) = \nu_{T(p)}(F \circ T, G \circ T)$$

[13] Det är med andra ord detsamma före och efter transformationer i $GL(3, \mathbb{C})$

för alla $p \in \mathbf{V}(F) \cap \mathbf{V}(G)$.

Innan vi slutligen når själva Bezouts sats visar vi en sats till.

Sats 14. *Om* $F, G \in \mathbb{C}[x, y, z]$ *är homogena polynom sådana att* $\text{Res}(F, G) \neq 0$ *så gäller att* $\text{Res}(F, G)(a, b) = 0$ *om och endast om det finns ett gemensamt nollställe* (a, b, c) *till* F *och* G.

Bevis. Bilda polynomen $F_{(a,b)}(z) = F(a, b, z)$ och $G_{(a,b)}(z) = G(a, b, z)$. Det inses att (a, b, c) är ett gemensamt nollställe till F och G om och endast om c är ett gemensamt nollställe till $F_{(a,b)}$ och $G_{(a,b)}$. Dessa har ett gemensamt nollställe c om och endast om $\text{Res}(F_{(a,b)}, G_{(a,b)}) = 0$. Vi inser lätt att $\text{Res}(F_{(a,b)}, G_{(a,b)}) = \text{Res}(F, G)(a, b)$. Alltså finns ett gemensamt nollställe c till $F_{(a,b)}$ och $G_{(a,b)}$ om och endast om (a, b) är ett nollställe till $\text{Res}(F, G)$ och i förlängningen finns ett nollställe (a, b, c) som är gemensamt för F och G om och endast om (a, b) är ett nollställe till $\text{Res}(F, G)$. □

4.2 Bezouts sats

Nu när vi har definierat alla begrepp och dessutom har lärt oss de satser som krävs presenterar vi själva satsen.

Sats 15 (Bezouts sats)**.** *Låt* C *och* C' *vara kurvor utan gemensamma komponenter i* $\mathbb{P}^2(\mathbb{C})$*, och låt* C *vara mängden av alla nollställen till det homogena polynomet* F *av grad* m *och låt* C' *vara mängden av alla nollställen till det homogena polynomet* G *av grad* n*. Då är*

$$\sum_{p \in C \cap C'} \nu_p(F, G) = m \cdot n.$$

Bevis. Börja med att transformera F och G till något lämpligt koordinatsystem såsom vi får göra enligt sats (13). Kalla de nya polynomen F_T och G_T, kalla de nya nollställena för p_T.

Vi vet att det finns en bijektion mellan nollsällena p_T och nollställena till $\text{Res}(F_T, G_T)$. Sats (14) ger nämligen en avbildning $\mathbb{P}^2(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ som är surjektiv och som är bijektiv om det inte finns distinkta nollställen på formerna $(a, b, 1)$ och (a, b, c) eller något nollställe på formen $(0, 0, 1)$. Eftersom det är just detta som transformationen T hindrar så finns en bijektion mellan nollställena p_T och nollställena till $\text{Res}(F_T, G_T)$. I och med att transformationen från F, G till F_T, G_T är en sammansättning av homogena polynom av grad m och 1 respektive n och 1 så har F_T samma grad som F och G_T samma grad som G. Enligt sats (10) är graden av $\text{Res}(F_T, G_T)$ alltså $m \cdot n$. Eftersom nollställena p_T står i ett bijektivt förhållande med nollställena till resultanten och eftersom $\text{Res}(F_T, G_T)$ enligt sats (12) har samma sammanlagda multiplicitet som $\text{Res}(F_T, G_T)$:s totala grad. Så måste summan av multipliciteterna för F_T och G_T:s gemensamma nollställen vara $m \cdot n$. Därmed måste samma sak gälla för F och G och därmed är satsen bevisad. □

5 Gröbnerbaser och Buchbergers algoritm

Medan vi ännu rör oss idealens och de algebraiska mängdernas värld kan det vara lämpligt att nämna att man numera kan beräkna sådant som förut var svårare. Man kan till exempel:

- Lösa[14] godtyckliga system av polynomekvationer i flera variabler,
- Utföra direkta beräkningar i koordinatringar,
- Avgöra om två ideal är samma ideal,
- Avgöra om ett ideal är ett delideal till ett annat.

Det visar sig nämligen att polynomideal kan ha flera olika genererande mängder och framförallt att vissa av dem är bättre än andra. Dessa bättre genererande mängder kallas *Gröbnerbaser*. När man väl har funnit en Gröbnerbas kan man bland annat använda den för att utföra vissa polynomdivisioner med flera nämnare på en gång[15]. För att finna en Gröbnerbas för ett ideal använder man sig av *Buchbergers algoritm*.

Avsnittet följer väsentligen framställningen i Cox m.fl. (1997).

5.1 Monom

Vi förtydligar först vad vi, eller snarare Cox m.fl., menar med ett *monom*, sedan fortsätter vi med att definiera ett par andra användbara begrepp. Syftet är att skapa ett användbart språk om monom.

Definition 25. *Vi säger att ett polynom $f \in R[x_1, \ldots, x_n]$ är ett* monom *om det kan skrivas $f = x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}$.*

Ett monoms exponenter kallar vi för dess *multigrad*.

Definition 26. *Om $f = x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n} \in R[x_1, \ldots, x_n]$ är ett monom så kallar vi $(m_1, m_2, \ldots, m_n)$ för f:s* exponent *eller* multigrad.

Vi har tidigare definierat begreppet *total grad*. Vi upprepar definitionen.

Definition 27. *Låt $f = x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}$ vara ett monom i $R[x_1, \ldots, x_n]$. Vi säger att f:s* totala grad *är $\sum_{i=1}^{n} m_n$ och skriver $|(m_1, \ldots, m_n)| = \sum_{i=1}^{n} m_i$.*

Av naturliga skäl kommer de flesta monom som dyker upp i fortsättningen att vara monom i flera variabler. Det framgår oftast ur sammanhanget vilka variabler det rör sig om, så för att inte behöva skriva $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ inför vi också följande konvention.

Definition 28. *Låt $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ vara en multigrad. Vi skriver $\mathbf{x}^\alpha$, eller x^α om det är otvetydigt, istället för $\prod_{i=1}^{n} x_i^{\alpha_i}$.*

5.2 Monomordningar

I ringar som $\mathbb{Z}[x]$ eller $\mathbb{C}[x]$ har vi en naturlig *monomordning*. Vi brukar till exempel skriva termer som innehåller x^{100} före de som innehåller x^2 eftersom 100 är större än 2. När vi utökar antalet variabler måste vi ordna termerna annorlunda eftersom multigrader inte är jämförbara på samma sätt som heltal. Vi ska se senare att termernas ordning inte bara är en fråga om estetik, utan att det spelar roll för de algortimer vi ska undersöka. Vi kommer dessutom att se att det finns många olika alternativa ordningar i flera variabler.

[14] Det handlar snarare om att reducera till polynomekvationer i en variabel.
[15] Det kommer att framgå senare vad det betyder.

Låt oss definiera monomordningen som sådan.

Definition 29. *Låt $>_m$ vara en partiell ordning på monomens multigrader i en polynomring $R[x_1, \ldots, x_n]$. Vi säger att $>_m$ är en* monomordning *om den uppfyller följande krav:*

1. *$>_m$ är total*
2. *Om α, β och γ är multigrader så gäller att $\alpha >_m \beta \implies \alpha + \gamma >_m \beta + \gamma$*
3. *$>_m$ är en välordning*

Härnäst konstruerar vi, eller snarare lånar från Cox m.fl., ett par monomordningar. Vi börjar med den lexikala ordningen. För ett bevis för att detta verkligen är en monomordning hänvisas läsaren till Cox m.fl. (1997, Sats 2.2.4).

Definition 30. *Låt $\alpha = (\alpha_1, \ldots, \alpha_n)$ och $\beta = (\beta_1, \ldots, \beta_n)$. I den* lexikala *ordningen monomordningen gäller att $\mathbf{x}^\alpha >_{lex} \mathbf{x}^\beta$ om det finns ett $0 < m \leq n$ sådant att om $0 < i < m$ så är $\alpha_i - \beta_i = 0$ och $\alpha_m - \beta_m > 0$.*

En annan liknande monomordning är den så kallade *graderade lexikala ordningen*, den jämför monomens totala grad, men tillämpar den lexikala ordningen för monom med samma totala grad.

Definition 31. *Låt $\alpha = (\alpha_1, \ldots, \alpha_n)$ och $\beta = (\beta_1, \ldots, \beta_n)$. I den* graderade lexikala *monomordningen gäller att $\mathbf{x}^\alpha >_{grlex} \mathbf{x}^\beta$ om $|\alpha| > |\beta|$ eller om $|\alpha| = |\beta|$ och $\alpha >_{lex} \beta$.*

En lite mer exotisk monomordning är den *graderade omvänt lexikala ordningen*. Den fungerar ungefär som den graderade lexikala ordningen.

Definition 32. *Låt $\alpha = (\alpha_1, \ldots, \alpha_n)$ och $\beta = (\beta_1, \ldots, \beta_n)$. I den* graderade omvänt lexikala *ordningen gäller att $\mathbf{x}^\alpha >_{grevlex} \mathbf{x}^\beta$ om $|\alpha| > |\beta|$ eller om $|\alpha| = |\beta|$ och det finns ett $1 \leq m \leq n$ sådant att om $m < i \leq n$ så gäller att $\alpha_i = \beta_i$ och $\alpha_m < \beta_m$.*

Även dessa två är förstås monomordningar.

Sats 16. *Både den graderade lexikala ordningen och den graderade omvänt lexikala ordningen är monomordningar.*

Bevis. Det är direkt uppenbart att båda ordningarna är totala, det vill säga att för alla par α, β gäller att $\alpha > \beta, \alpha < \beta$ eller $\alpha = \beta$.

Det är också uppenbart att α, β, γ sådana att $\alpha > \beta$ har egenskapen att $\alpha + \gamma > \beta + \gamma$. Om $|\alpha| > |\beta|$ ser vi nämligen på en gång att $|\alpha + \gamma| = \sum_{i=1}^{n} (\alpha_i + \gamma_i) = |\alpha| + |\gamma|$, och på samma sätt att $|\beta + \gamma| = |\beta| + |\gamma|$ så ordningen bevaras. Om å andra sidan $|\alpha| = |\beta|$ men $\alpha > \beta$ så får vi två fall. I det första fallet (den graderade lexikala ordningen) använder vi den lexikala ordningen, som är en monomordning och alltså uppfyller villkoret. I fallet med den graderade omvänt lexikala ordningen vet vi att om $\alpha > \beta$ så finns ett $1 \leq m \leq n$ sådant att vi för varje $m < i \leq n$ har $\alpha_i = \beta_i$ och $\alpha_m < \beta_m$ dessa relationer påverkas inte av att γ_i eller γ_m adderas till både höger- och vänsterleden.

För att visa att båda ordningarna dessutom är välordningar behöver vi bara visa att det för en given multigrad α endast kan finnas ändligt många β med

samma eller lägre multigrad, det är ju endast en delmängd av dessa som är mindre än α i någon av ordningarna.

Vi konstaterar att om $|\alpha| = a$ så kommer det i vilket fall som helst att finnas färre β sådana att $|\alpha| \geq |\beta|$ än det finns n-tupler där varje komponent har värden mellan 0 och a. Vi konstaterar alltså att det måste finnas färre än $(a+1)^n$ stycken β med lägre eller lika stor total ordning som α. Alltså kan varje α under en graderad ordning bara vara större än ändligt många andra element.

Därmed är alla tre kraven uppfyllda och både den graderade lexikala ordningen och den graderade omvänt lexikala ordningen är monomordningar. □

Vi definierar ett par begrepp som beror av vilken monomordning vi har valt. Först och främst definierar vi begreppet *ledande term* för polynom i flera varibler.

Definition 33. *Låt $f \in R[x_1, \ldots, x_n]$ och låt $>_o$ vara en monomordning. Vi säger att en term i f, $g = r\mathbf{x}^\alpha$ där $r \in R\backslash\{0\}$, är f:s ledande term om alla termer med multigrader som överstiger α i $>_o$ har 0 som koefficient. Vi skriver $\mathrm{LT}(f)$ för att beteckna f:s ledande term.*

Definition 34. *Låt $f \in R[x_1, \ldots, x_n]$ och låt $>_o$ vara en monomordning. Vi säger att f:s ledande koefficient är koefficienten framför monomet i $\mathrm{LT}(f)$. Vi betecknar den med $\mathrm{LC}(f)$*

Definition 35. *Låt $f \in R[x_1, \ldots, x_n]$ och låt $>_o$ vara en monomordning. Vi säger att f:s ledande monom är monomet i $\mathrm{LT}(f)$. Vi betecknar den med $\mathrm{LM}(f)$.*

5.3 Division i flera variabler

För polynom i en variabel finns en enkel divisionsalgoritm som påminner om den som används för heltal. Om f är täljaren och g är nämnaren går divisionen ut på att skriva ett polynom f på formen $f = hg + r$ där h är kvoten och r är resten. Vi ska försöka konstruera en divisionsalgoritm i flera variabler och för flera samtidiga nämnare. Med andra ord en algoritm som given en mängd, ett polynom $f \in R[x_1, \ldots, x_n]$ och ett antal nämnare $g_1, g_2, \ldots, g_m$ kan skriva f på formen $f = a_1g_1 + a_2g_2 + \cdots g_m + r$ där a_i och r är polynom. Vi formulerar det som en lånesats (Cox m.fl. 1997, Sats 2.3.3).

Sats 17 (Divisionsalgoritmen i $k[x_1, \ldots, x_n]$)**.** *Fixera en monomordning $>$. Låt $F = (f_1, \ldots, f_s)$ vara polynom i $k[x_1, \ldots, x_n]$. Varje $f \in k[x_1, \ldots, x_n]$ kan skrivas*

$$f = a_1f_1 + \cdots a_sf_s + r,$$

där a_i och r är polynom i $k[x_1, \ldots, x_n]$. Dessutom gäller att $r = 0$ eller att r är en linjärkombination med koefficienter i k av monom som inte är delbara med någon av termerna $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$. Vi kallar r för resten av f vid division med F. Om dessutom $a_if_i \neq 0$ så har vi att f:s multigrad är större än eller lika med a_if_i:s multigrad för varje i.

Lyckligtvis ges vi en explicit algoritm i beviset till samma sats, ungefär enligt följande modell.

```
Indata: f_1, ..., f_s, f
Utdata: a_1, ..., a_s, r

a_1 := 0
a_2 := 0
...
a_s := 0
r := 0
p := f

Så länge som p ≠ 0:
    i := 1
    division_uträttad := falskt
    Så länge som i ≤ s och division_uträttad == falskt:
        Om LT(f_i) delar LT(p):
            a_i := a_i + LT(p)/LT(f_i)
            p := p − (LT(p)/LT(f_i))f_i
            division_uträttad := sant
        Annars:
            i := i + 1
    Om division_uträttad == falskt:
        r := r + LT(p)
        p := p − LT(p)
```

Det visar sig tyvärr att algoritmen saknar vissa önskvärda egenskaper. Till exempel blir inte resten alltid likadan utan beror på i vilken ordning vi räknar upp våra nämnare.

5.4 Gröbnerbaser

Skälet till att vi intresserar oss för hur man kan dividera polynom i $k[x_1, \ldots, x_n]$ med varandra är att resten vid division kan användas som representant för ekvivalensklasser i kvotringar. Om $I = \langle f_1, \ldots, f_s \rangle$ är ett ideal i $k[x_1, \ldots, x_n]$ så kan vi ju bilda ringen $k[x_1, \ldots, x_n]/I$ som består av ekvivalensklasser av polynom i $k[x_1, \ldots, x_n]$. Att ett polynom $f \in k[x_1, \ldots, x_n]$ tillhör samma ekivalensklass som någon representant $r \in k[x_1, \ldots, x_n]/I$ innebär per definition att $f - r \in I$, eller med andra ord att det finns ett element $i = a_1 f_1 + a_2 f_2 + \cdots a_s f_s \in I$ sådant att $f = i + r$. Om vi kunde hitta en standardiserad representant r för varje given ekvivalensklass, och dessutom kunde hitta ett sätt att ta reda på vilken av dessa standardiserade representanter ett givet polynom i $f \in k[x_1, \ldots, x_n]$ har, då skulle det (åtminstone i princip) vara lika lätt att hantera godtyckliga ringar på formen $k[x_1, \ldots, x_n]/I$ som det är att hantera restklassringarna $\mathbb{Z}_n$.

Lyckligtvis är problemet redan löst[16]. Själva idén är att om vi kan finna en särskilt gynnsam bas till idealet I, kallad en Gröbnerbas, så ger divisionsalgoritmen samma rest för två polynom om och endast om de tillhör samma ekvivalensklass i $k[x_1, \ldots, x_n]/I$.

[16]Problemet löstes så sent som 1965 i Bruno Buchbergers doktorsavhandling *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.*

Definition 36. *Bestäm en monomordning. Låt $I \subset k[x_1, \ldots, x_n]$ vara ett ideal. Låt $b = \{f_1, \ldots, f_s\} \subset I$. Vi kallar b för en* Gröbnerbas *om den uppfyller följande villkor.*

$$\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle = \langle \mathrm{LT}(i) : i \in I \rangle$$

Vi vill förstås att Gröbnerbaser ska vara genererande mängder, och gärna att varje ideal ska ha en sådan. Cox m.fl. (1997, Korollarium 2.5.6) ger oss ett bevis för följande sats.

Sats 18. *Bestäm en monomordning. Varje ideal $I \subset k[x_1, \ldots, x_n]$ utöver $\{0\}$ har en Gröbnerbas, och varje Gröbnerbas till I genererar I.*

Gröbnerbasernas relevans i sammanhanget klargörs genom följande sats, med bevis i Cox m.fl. (1997, Sats 2.6.1).

Sats 19. *Låt $G = \{g_1, \ldots, g_t\}$ vara en Gröbnerbas för idealet $I \subset k[x_1, \ldots, x_n]$ och låt $f \in k[x_1, \ldots, x_n]$. Då finns ett unikt $r \in k[x_1, \ldots, x_n]$ med följande egenskaper:*

1. *Ingen av de ledande termerna $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$ delar någon av r:s termer*
2. *Det finns ett $g \in I$ sådant att $f = g + r$*

Dessutom är r resten när f delas av G med divisionsalgoritmen oavsett hur vi ordnar elementen i G.

Vi inför lite ny notation för att fira våra divisionstriumfer.

Definition 37. *Låt $f \in k[x_1, \ldots, x_n]$ och låt $F = (g_1, \ldots, g_t)$. Vi skriver $\overline{f}^F$ för att beteckna resten vid division av f med polynomen i F.*

Vi nöjer oss för ögonblicket och frågar oss istället hur vi kan finna en Gröbnerbas.

5.5 Buchbergers algoritm

För att kunskapen om Gröbnerbaser verkligen ska gå att använda måste vi kunna hitta Gröbnerbaser på ett enkelt sätt. Den tidigare nämnda Bruno Buchbergers förtjänst är just att formulera den första algoritmen för ändamålet. Nyckeln är att finna ett enklare kriterium för att avgöra huruvida en mängd är en Gröbnerbas eller inte, och att sedan successivt modifiera mängden tills den blir en Gröbnerbas.

Som ett första steg inför vi begreppen *S-polynom* och *minsta gemensamma multipel*.

Definition 38. *Låt $f, g \in k[x_1, \ldots, x_n]$ vara nollskilda polynom. Låt α vara f:s multigrad och låt β vara g:s multigrad. Låt sedan $\gamma = (\gamma_1, \ldots, \gamma_n)$, och $\gamma_i = \max(\alpha_i, \beta_i)$. Vi säger att $\mathbf{x}^\gamma$ är* minsta gemensamma multipel *av $\mathrm{LM}(f)$ och $\mathrm{LM}(g)$. Vi skriver $\mathbf{x}^\gamma = \mathrm{MGM}(\mathrm{LM}(f), \mathrm{LM}(g))$.*

Definition 39. *Låt $f, g \in k[x_1, \ldots, x_n]$ S-polynomet av f och g är*

$$S(f, g) = \frac{\mathrm{MGM}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(f)} \cdot f - \frac{\mathrm{MGM}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}\, g} \cdot g.$$

Det utlovade kriteriet är att dessa S-polynom ska representeras av 0 i $k[x_1, \ldots, x_n]/I$, det vill säga att resten är noll vid division med Gröbnerbaser. Vi lånar det som en sats från Cox m.fl. (1997, Sats 2.6.6).

Sats 20. *Låt $I \subset k[x_1, \ldots, x_n]$ vara ett ideal. Den genererande mängden $G = \{g_1, \ldots, g_t\}$ är en av I:s Gröbnerbaser om och endast om varje par g_i, g_j sådant att $i \neq j$ har egenskapen att $\overline{S(g_i, g_j)}^G = 0$.*

Vi undersöker helt enkelt vilka $\overline{S(g_i, g_j)}^G$ som är nollskilda och lägger till dem en och en, enligt en sats med bevis i Cox m.fl. (1997, Sats 2.7.2).

Sats 21 (Buchbergers algoritm)**.** *Låt $I = \langle f_1, f_2, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$ vara ett nollskilt ideal. Då kan en Gröbnerbas för I konstrueras i ett ändligt antal steg med följande algoritm.*

`Indata:` $F = (f_1, f_2, \ldots, f_s)$
`Utdata: en Gröbnerbas` $G = (g_1, \ldots, g_t)$ `som genererar` I `sådan att` $F \subset G$

G`:=` F
`Upprepa:`
    G' `:=` G
    `För varje par` $\{p, q\}$, $p \neq q$ `i` G'`:`
        `s :=` $\overline{S(p,q)}^{G'}$
        `Om` $S \neq 0$`:`
            G `:=` $G \cup \{s\}$
`Tills` $G = G'$.

Lägg märke till att det inte finns några garantier för att det blir *samma* Gröbnerbas bara för att vi utgår från *samma* ideal och monomordning. Att monomordningen spelar roll är mer eller mindre oavhjälpligt, men det vore förstås praktiskt om vi för en given monomordning alltid fick samma Gröbnerbas för samma ideal, och det vore ännu bättre om den kunde vara minimal i någon bemärkelse. Vi introducerar begreppet *reducerad Gröbnerbas*.

Definition 40. *En Gröbnerbas G för ett ideal I kallas för* reducerad *om*

1. $\mathrm{LC}(p) = 1$ *för alla* $p \in G$
2. *Om $p \in G$ så ligger inget av p:s monom i $\langle \mathrm{LT}(G - \{p\}) \rangle$*

Och det visar sig mycket riktigt att dessa alltid existerar, och att de är unika (Cox m.fl. 1997, Sats 2.7.6).

Sats 22. *Låt $I \subset k[x_1, \ldots, x_n]$ vara ett nollskilt ideal. Då finns det en unik reducerad Gröbnerbas för I i varje given monomordning.*

Det går till och med att på ett enkelt sätt konstruera en reducerad Gröbnerbas om vi redan har en annan till hands. I Cox m.fl. (1997) antyds det i beviset av sats (22) hur man kan gå till väga för att skapa en reducerad Gröbnerbas. Det visar sig att vi kan betrakta enskilda polynom i en Gröbnerbas som reducerade eller icke-reducerade och sedan byta ut de icke-reducerade polynomen

mot reducerade, när alla element är reducerade har vi funnit den reducerade Gröbnerbasen för I. Vi lyfter ut det väsentliga för tydlighetens skull.

Definition 41. *Ett enskild polynom g i en Gröbnerbas G för idealet I kallas* reducerat *om följande villkor är uppfyllda.*

1. $\mathrm{LC}(g) = 1$
2. *Ingen av monomen i g ligger i $\langle \mathrm{LT}(G - \{g\})\rangle$*

Lemma 4. *Låt G vara en Gröbnerbas för $I \in k[x_1, \ldots, x_n]$ och låt $g \in G$ vara ett reducerat polynom. Det följer direkt av definitionen att g är reducerat för alla Gröbnerbaser G' med samma ledande monom som G och med $g \in G'$.*

Bevis. $\mathrm{LC}(g)$ är fortfarande 1, så krav 1 är uppfyllt oavsett vilken Gröbnerbas vi väljer. Antag att G' är en annan Gröbnerbas för I sådan att $g \in G'$ och $\mathrm{LM}(G) = \mathrm{LM}(G')$, då kommer $\langle \mathrm{LT}(G - \{g\})\rangle \subset \langle \mathrm{LT}(G' - \{g\})\rangle$ eftersom varje $h \in \mathrm{LT}(G - \{g\})$ har en motsvarighet $ch \in \mathrm{LT}(G' - \{g\})$ där $c \in k$. Men på precis samma sätt inser vi att $\langle \mathrm{LT}(G' - \{g\})\rangle \subset \langle \mathrm{LT}(G - \{g\})\rangle$ så $\langle \mathrm{LT}(G - \{g\})\rangle = \langle \mathrm{LT}(G' - \{g\})\rangle$. Därmed är g reducerad i både G och G'. □

Nästa steg är att för ett givet $g \in G$ som ännu inte är reducerat finna ett reducerat g' sådant att $(G - \{g\}) \cup \{g'\}$ är en Gröbnerbas och sådant att $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}((G - \{g\}) \cup g')\rangle$. Vi lånar ett trevligt lemma från Cox m.fl. (1997, Lemma 2.7.3).

Lemma 5. *Låt G vara en Gröbnerbas för $I \subset k[x_1, \ldots, x_n]$. Låt $p \in G$ vara ett polynom sådant att $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\})\rangle$, då är $G - \{p\}$ också en Gröbnerbas för I.*

Ett polynom som, i enlighet med lemma 5, kan avlägsnas från Gröbnerbasen kallas *överflödigt*. Vi kan uppenbarligen avlägsna överflödiga polynom från en Gröbnerbas ett och ett tills inga överflödiga polynom återstår. Om vi dividerar varje polynom i den nya Gröbnerbasen så att den ledande koefficienten blir 1, så kallar vi Gröbnerbasen minimal. En reducerad Gröbnerbas är uppenbarligen minimal, och en reducerad Gröbnerbas kan konstrueras genom följande algoritm. Beviset och algoritmen är i allt väsentligt hämtade från beviset av sats 2.7.6 i Cox m.fl. (1997).

Sats 23. *Låt $G = (g_1, \ldots, g_s)$ vara en minimal Gröbnerbas för $I \subset k[x_1, \ldots, x_n]$. Då kan en reducerad Gröbnerbas för samma ideal konstrueras enligt följande algoritm.*

`Indata: En minimal Gröbnerbas` $G = \{g_1, \ldots, g_s\}$
`Utdata: En reducerad Gröbnerbas` $R_s = \{r_1, \ldots, r_s\}$

i `:=` 1
R_0 `:=` G
`Så länge som` $i \leq s$`:`
    r_i `:=` $\overline{g_i}^{(R_{i-1} - \{g_i\})}$
    R_i `:=` $(R_{i-1} - \{g_i\}) \cup \{r_i\}$
    i `:=` $i + 1$

Bevis. I varje steg modifierar algoritmen den föregående basen R_{i-1} så att elementet r_i ersätter elementet g_i. Om vi kan visa att r_i är reducerad för varje i, att R_i genererar I för varje i och att R_s är en Gröbnerbas så vet vi att R_s är en reducerad Gröbnerbas för I.

För att r_i inte ska vara reducerad krävs det att någon av monomen i r_i finns i $\langle \mathrm{LT}(R_i - \{r_i\})\rangle$. Det kan inte vara r_i:s ledande term eftersom den förutsattes vara ledande endast i g_i. Divisionsalgoritmen från sats 17 verkar på det sättet att den successivt avlägsnar termer med samma monom som den ledande termen för någon av nämnarna. Alltså kan inte r_i ha en term vars monom är det ledande monomet i något polynom i $R_{i-1} - \{g_i\}$, som av en händelse är *samma* mängd som $R_i - \{r_i\}$. Alltså består r_i av en ledande term som är samma som den i g_i och ett antal termer som inte är ledande i något annat polynom i R_i. g_i:s ledande koefficient var 1, så r_i är reducerad i R_i. Enligt lemma 4 är r_i reducerad i alla Gröbnerbaser där samma ledande monom förekommer. Vi har redan konstaterat att r_i och g_i har samma ledande monom, alltså har $G = R_o$ samma ledande monom som R_s, och därför är r_i reducerat i alla R_j där $j \geq i$.

Att $r_i = \overline{g_i}^{(R_{i-1}-\{g_i\})}$ innebär att $r_i = g_i - (\sum_{p\in(G-\{g_i\})} a_p p)$, alltså genererar R_{i-1} och $R_i = (R_{i-1}-\{g_i\})\cup\{r_i\}$ samma ideal för alla i, och i förlängningen genererar alla R_i samma ideal som $R_0 = G$. Så $\langle R_s\rangle = \langle G\rangle$.

Allt som återstår är att verifiera att R_s verkligen är en Gröbnerbas. Eftersom R_s genererar samma ideal som G så behöver vi bara visa att

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle = \langle \mathrm{LT}(r_1), \ldots, \mathrm{LT}(r_s)\rangle.$$

Eftersom $\mathrm{LT}(g_i) = \mathrm{LT}(r_i)$ för alla i är det tämligen uppenbart att så är fallet.

Alltså har vi visat att R_s är en reducerad Gröbnerbas för I. □

5.6 Det utlovade

I avsnittets början lovades lösningar på ett par problem. Vi börjar med att avgöra huruvida två ideal i $k[x_1, \ldots, x_n]$ är samma ideal. Nu när vi har introducerat ett par nya verktyg kan vi enkelt lösa problemen som hos Cox m.fl. (1997).

Det är tämligen uppenbart vad som ska göras. Eftersom vi precis har kommit fram till att varje ideal i $k[x_1, \ldots, x_n]$ har precis en reducerad Gröbnerbas, och eftersom vi precis har konstruerat en algoritm för att finna just denna unika reducerade Gröbnerbas, är det bara att finna Gröbnerbasen i fråga. Vi formulerar lösningen på problemet som en sats.

Sats 24. *Låt $I = \langle f_1, \ldots, f_s\rangle \subset k[x_1, \ldots, x_n]$ och $J = \langle g_1, \ldots, g_t\rangle \in k[x_1, \ldots, x_n]$ vara polynomideal och bestäm en monomordning. $I = J$ om och endast om de har samma reducerade Gröbnerbas.*

Bevis. Låt $I = J$, då har I och J samma reducerade Gröbnerbas med avseende på vår monomordning eftersom varje ideal bara har en monomordning. Låt å andra sidan I och J ha samma reducerade Gröbnerbas. Då genereras de av samma mängd och är uppenbarligen lika. □

Härnäst löser vi problemet att avgöra huruvida ett ideal I är ett delideal till J. Vi inser att $I \subset J$ om och endast om varje element någon av dess genererande mängder ingår i J. Eftersom vi kan enkelt avgöra om så är fallet genom att beräkna en Gröbnerbas av J och sedan undersöka om resten av varje enskilt

polynom i I:s generatormängd vid division med J:s Gröbnerbas blir noll. Vi formulerar så klart lösningen som en sats.

Sats 25. *Låt $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$ och låt $J = \langle g_1, \ldots, g_t \rangle \subset k[x_1, \ldots, x_n]$ låt G vara en Gröbnerbas för I med avseende på någon monomordning. $I \subset J$ om och endast om $\overline{f_i}^G = 0$ för alla $1 \leq i \leq s$.*

Bevis. Antag att $I \subset J$, då ligger varje f_i i J och eftersom G genererar J kan varje f_i skrivas som en linjärkombination av element ur G med element ur $k[x_1, \ldots, x_n]$, men då är ju resten 0 vid division med G.

Låt istället $\overline{f_i}^G = 0$ för alla i. Eftersom varje element ur I kan skrivas som en linjärkombination av element ur $\{f_1, \ldots, f_m\}$, vars element är linjärkombinationer av element i G är även elementen i I linjärkombinationer av element ur G och därför element ur J. □

Det utlovades en metod för att utföra beräkningar i koordinatringar. Det hör till saken att om vi vill beräkna summan eller produkten av två element ur $k[x_1, \ldots, x_n]$, eller snarare av deras respektive ekvivalensklasser i $k[x_1, \ldots, x_n]/I$ för något ideal I, så består inte svårigheten i att utföra själva additionen eller multiplikationen utan i att om vi multiplicerar eller adderar två element ur $k[x_1, \ldots, x_n]$ så hjälper det inte att summan respektive produkten är en representant för summan respektive produkten i $k[x_1, \ldots, x_n]/I$. Det vi egentligen är ute efter är att representera elementen ur $k[x_1, \ldots, x_n]/I$ på ett standardiserat sätt så att vi vet vilken ekvivalensklass det rör sig om. Lösningen är, förstås, att finna en Gröbnerbas för I och att använda divisionsalgoritmen. Det rör sig förstås inte om någon sats den här gången utan om en definition.

Definition 42. *Låt $I \subset k[x_1, \ldots, x_n]$ vara ett ideal, och låt G vara en reducerad Gröbnerbas med avseende på någon monomordning. Låt $f \in k[x_1, \ldots, x_n]/I$. Vi kallar $\overline{f}^G$ för f:s standardrepresentant för monomordningen i fråga.*

Slutligen löser vi det sista av problemen, att reducera lösningen av ett system av polynom i flera variabler till lösningen av en serie ekvationer i en variabel. Antag att vi har ett system av polynomekvationer, $(f_1, f_2, \ldots, f_s) = \mathbf{0}$. Vi är förstås inte så särskilt fästa vid just polynomen $f_1, \ldots, f_s$, och vi vet sedan tidigare att alla polynom i $\langle f_1, \ldots, f_s \rangle$ har samma gemensamma nollställen som $f_1, \ldots, f_s$. Det betyder att om vi kan finna en ny genererande mängd $\{g_1, g_2, \ldots, g_n\}$ sådan att g_1 endast innehåller variabeln x_1, $g_2 \in k[x_1, x_2]$ och så vidare, då kan vi successivt lösa ekvationerna en efter en och ständigt reducera problemet till att lösa ett antal ekvationer i precis en variabel.

Det vore förstås märkligt om det inte smög sig in någon form av Gröbnerbas någonstans, det har ju visat sig vara något av ett universalrecept. I vårt fall handlar det om att finna en Gröbnerbas för $\langle f_1, \ldots, f_s \rangle$ med avseende på den lexikala ordningen. Vi får inte omedelbart ett system av ekvationer i en variabel, men vi får *nästan* ett sådant system. Vi definierar ett användbart begrepp.

Definition 43. *Låt $I \subset k[x_1, \ldots, x_n]$ vara ett ideal. Vi kallar I_l för det l:te eliminationsidealet om*

$$I_l = I \cap k[x_{l+1}, \ldots, x_n].$$

Nu kan vi formulera oss lite klarare. Det l:e eliminationsidealet är helt enkelt mängden av alla polynom i I som inte innehåller någon av de l första variablerna. Då är förstås I_{n-1} den delmängd av I som består av polynom i $k[x_n]$. Det är tämligen uppenbart att om $(x_1, \ldots, x_n)$ ingår i $\mathbf{V}(I)$ så måste $x_n \in \mathbf{V}(I_{n-1})$, så om vi kunde finna en bas för I_{n-1} så skulle vi kunna hitta varje värde för x_n som kan ingå i $\mathbf{V}(I)$. Om vi alltså har funnit alla tänkbara värden för x_n och om vi dessutom kan hitta en genererande mängd för I_{n-2} så skulle vi kunna sätta in de x_n vi fann i $\mathbf{V}(I_{n-1})$ och då få en uppsättning polynomekvationer i variabeln x_{n-1}. Löser vi var och en av dem och fortsätter på samma sätt har vi till slut funnit alla tänkbara n-tupler som ingår i $\mathbf{V}(I)$. Lyckligtvis ger Cox m.fl. (1997, Sats 3.1.2) oss följande sats.

Sats 26. *Låt $I \subset k[x_1, \ldots, x_n]$ och låt G vara en Gröbnerbas för I med avseende på den lexikala ordningen då gäller för varje l, sådant att $0 \leq l \leq n$, att mängden*

$$G_l = G \cap k[x_{l+1}, \ldots, x_n]$$

är en Gröbnerbas för I_l.

Med andra ord kan vi lösa ett system av polynomekvationer i n variabler genom att beräkna en Gröbnerbas med avseende på den lexikala ordningen, och sedan lösa ekvationen med bara en variabel[17] och successivt substitutera in lösningarna i de övriga ekvationerna för att sedan lösa dem.

6 Moderna strukturer

Tidigare nämndes att varken ideal eller ens algebraiska mängder egentligen är de objekt som den moderna algebraiska geometrin helst behandlar. Det betraktelsesättet att algebraisk geometri väsentligen är studiet av vissa ideal och kvotringar av $k[x_1, \ldots, x_n]$ i syfte att härleda kunskaper om algebraiska mängder har visserligen sin hemvist i 1900-talet, men enligt Dieudonné (1974, VII.15) var den algebraiska geometrin i princip studiet av vissa ideal fram tills omkring 1925. Därefter dyker till exempel studiet av lokala ringar upp.

Genom en utveckling kraftigt inspirerad av differentialtopologin inleds studiet av det vi idag kallar algebraiska varieteter i början av 1950-talet (Dieudonné 1974, VIII.19). Detta nya begrepp bygger i allt väsentligt på algebraiska mängders koordinatringar och Zariskitopologier. Härifrån är steget förstås inte särskilt långt till att befria sig helt från koordinatringarna, och istället försöka studera objekt som beter sig som algebraiska varieteter med det undantaget att de är baserade på godtyckliga kommutativa ringar. Mot slutet av 1950-talet var det också just det som hände (Dieudonné 1974, VIII.28). Det hela resulterade i teorin om så kallade *Schémas*[18] som verkar anses utgöra den moderna algebraiska geometrins kärna[19].

Syftet med de kommande avsnitten är att ge en högst konkret introduktion till ett par av själva grundbegreppen i den modernare teorin. Det är inte riktigt möjligt att göra teorin rättvisa med de tillgängliga verktygen, och det skulle i

[17] Det kommer att finnas högst en ekvation med enbart variabeln x_n. $k[x_n]$ är nämligen ett principalidealområde, så I_{n-1} genereras av ett polynom.

[18] Franska för skiss, överblicksbild eller ritning.

[19] Här är förstås författare som Dieudonné en aning partiska, de är i någon mening medbrottslingar.

vilket fall som helst vara svårt att formulera särskilt mycket av den moderna algebraiska geometrin på de återstående sidorna. Lite mer exakt kommer det som här kallas för kärvar[20], scheman[21], varieteter[22] och groddar[23] att förklaras och konstrueras.

6.1 Kärvar

Tanken med en kärve är följande: vi har någon form av topologiskt rum och någon form av matematiska strukturer som hör ihop med varje öppen mängd. Till exempel kan vi ha en inducerad Zariskitopologi på en algebraisk mängd och olika uppsättningar väldefinierade funktioner på de Zariskiöppna delmängderna. Själva kärven är en avbildning mellan det topologiska rummets öppna mängder och den matematiska strukturen. Vi formulerar oss som Perrin (1995, Kapitel III.1.b).

Definition 44. *Låt X vara mängden av de öppna mängderna i ett topologiskt rum. En avbildning från X till någon mängd Y, $\mathcal{F} : X \to Y$, är en* prekärve[24] *på X om det för varje par U, V av öppna mängder i X sådana att $U \subset V$ finns en restriktionsavbildning $r_{U,V} : \mathcal{F}(V) \to \mathcal{F}(U)$ sådan att*

1. *Om $W \subset U \subset V$ är öppna mängder i X gäller $r_{W,V} = r_{W,U} r_{U,V}$*
2. *Om U är en öppen mängd i X så är $r_{U,U}$ identitetsavbildningen på U*

Vi skriver $f|_V$ för att beteckna $r_{V,U}(f)$.

Ett trivialt exempel är denna prekärve på $\mathbb{C}$.

Exempel 6. *Om det topologiska rummet är standardtopologin på $\mathbb{C}$ och $\mathcal{F}(U)$ är mängden $\{f|_U : f$ är analytisk på $\mathbb{C}\}$ och restriktionsavbildningen är den uppenbara då är $\mathcal{F}$ en prekärve. Villkor 1 är uppfyllt eftersom det bara är definitionsmängden som påverkas av restriktionsavbildningen, det spelar ingen roll i sammanhanget om den avgränsas i flera steg eller inte. Det andra villkoret innebär i sammanhanget enbart att definitionsmängden förblir densamma och är därför också uppfyllt.*

Vi definierar de verkliga kärvarna.

Definition 45. *Låt $\mathcal{F}$ vara en prekärve på X. Vi kallar $\mathcal{F}$ för en* kärve *om den dessutom uppfyller följande villkor:*

3 *Om $\{U_i\}$ är en öppen övertäckning av U och om det finns $f_i \in \mathcal{F}(U_i)$ sådana att om $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$ för alla U_i, U_j så finns precis ett $f \in \mathcal{F}(U)$ sådant att $f|_{U_i} = f_i$ för alla i.*

Vårt tidigare exempel är i själva verket också ett exempel på en kärve.

Exempel 7. *Vi återvänder till exempel 6. Vi inser att $\mathcal{F}$ i själva verket är en kärve. Antag nämligen att det fanns en öppen mängd U som vore en union av*

[20] Fr: Faisceaux, En: Sheaves. Ordet *kärve* är egentligen en ålderdomlig jordbruksterm som syftar på ett knippe säd.
[21] Fr: Schémas, En: Schemes.
[22] Fr: Variétés, En: Varieties
[23] Fr: Germes, En: Germs
[24] Fr: Préfaisceau, En: Presheaf

mängderna $\{U_i\}$ och att det fanns funktioner $f_i \in \mathcal{F}(U_i)$ såsom i definitionen av en kärve. Antag sedan att det fanns två funktioner $f_1, f_2 \in \mathcal{F}(U)$ sådana att $f_1|_{U_i} = f_2|_{U_i}$. Eftersom dessa funktioner är lika på en öppen mängd måste de vara begränsningar av en och samma analytiska funktion F på $\mathbb{C}$, men om så är fallet kan ju inte $F|_U$ vara både f_1 och f_2. Slutsatsen är att det bara kan finnas en funktion $f \in \mathcal{F}(U)$ sådan att $f|_{U_i} = f_i$. Därmed är $\mathcal{F}$ en kärve.

För att förenkla en aning hanterar vi fallet när vi kärvar ihop ett topologiskt rum med en uppsättning funktioner separat, med andra ord de fall där $\mathcal{F}(U)$ är en mängd av funktioner. Till skillnad från Perrin (1995) visar vi att det faktiskt är en kärve det rör sig om.

Lemma 6. *Låt X vara ett topologiskt rum. Låt $\mathcal{F}$ vara en funktion som avbildar öppna mängder i X på mängder av funktioner från öppna mängder till en mängd k. Vi kallar $\mathcal{F}$ för en funktionskärve om följande två kriterier är uppfyllda.*

1. *Om $V \subset U$ är öppna mängder i X så gäller att $f \in \mathcal{F}(U)$ medför att $f|_V \in \mathcal{F}(V)$*

2. *Om U är öppen och det finns en övertäckning av öppna mängder $\{U_i\}$ sådan att det finns $f_i \in \mathcal{F}(U_i)$ sådana att $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$ då finns precis en funktion $f \in \mathcal{F}(U)$ sådan att $f|_{U_i} = f_i$*

Då är $\mathcal{F}$ en kärve vars restriktionsavbildning är begränsningsoperationen.

Bevis. Låt $W \subset V \subset U$ vara öppna mängder, då gäller att $r_{V,U}$ avbildar funktioner $f \in \mathcal{F}(U)$ på funktioner med $f' : V \to k$ sådana att $f'(v) = f(v)$ för $v \in V$. Vi ser också att $r_{V,U}(f) = f'(v) = f(v) = f|_V$ på V så eftersom $f|_V \in \mathcal{F}(V)$ enligt antagande 1 om $\mathcal{F}$ måste $f' \in \mathcal{F}(V)$. Därmed kan vi tillämpa samma argument på $r_{W,V}$ och dra slutsatsen att $r_{W,V} r_{V,U}(f) = r_{W,V}(f|_V) = f|_W = r_{W,U}(f)$. Vi inser lätt att $r_{U,U}$ är identitetsavbildningen. Därmed är $\mathcal{F}$ en prekärve.

Kriteriet för att dessutom vara en kärve uppfylls av antagande två om $\mathcal{F}$. □

Vårt intresse för dessa kärvar kommer sig av att vi vill använda dem för att definiera ett par andra begrepp. Vi börjar med att, åtminstone skenbart, lämna funktionskärvarnas värld. Om vi tänker oss att vi på något smidigt sätt kan bunta ihop ett topologiskt rum och en uppsättning ringar till en kärve, så kallar vi konstruktionen för en *ringkärve*. Vi vill med andra ord att vår kärve ska assosciera varje öppen mängd i X med en ring, och att dessa ringars restriktionsavbildningar ska vara någon form av homomorfismer mellan ringar. Om vi associerar ett topologiskt rum X och någon ringkärve $\mathcal{O}_X$ så kallar vi detta för ett *ringbestyckat rum*. Vi lånar in en definition från Perrin (1995, definition III.1.6)

Definition 46. *Ett topologiskt rum X på vilket vi har definierat en ringkärve $\mathcal{O}_X$, dess så kallade strukturkärve, kallas i kombination med strukturkärven för ett* ringbestyckat rum[25]*. Vi skriver $(X, \mathcal{O}_X)$ för att beteckna ett sådant ringbestyckat rum.*

[25] Fr: espace annelé, en: ringed space.

Det vi i själva verket är ute efter att göra är att finna en strukturkärve för en affin algebraisk mängd och dess Zariskitopologi. Vi börjar med en sats som Perrin lämnat som övning.

Sats 27. *Låt X vara ett topologiskt rum och låt $\mathcal{U}$ vara en bas av öppna mängder för X. Låt k vara en mängd. Antag att vi för varje $U \in \mathcal{U}$ har en mängd $\mathcal{F}(U)$ av funktioner från U till k som uppfyller följande två kriterier:*

1. *Om $V, U \in \mathcal{U}$ och $V \subset U$ och $s \in \mathcal{F}(U)$ så har vi $s|_V \in \mathcal{F}(V)$*
2. *Om en öppen mängd $U \in \mathcal{U}$ övertäcks av öppna mängder $U_i \in \mathcal{U}$ där $i \in I$, och om s är en funktion från U till k sådan att $s|_{U_i} \in \mathcal{F}(U_i)$ för alla i då gäller att $s \in \mathcal{F}(U)$*

Då finns en entydigt bestämd funktionskärve $\overline{\mathcal{F}}$ på X sådant att $\overline{\mathcal{F}}(U) = \mathcal{F}(U)$ för varje $U \in \mathcal{U}$.

Bevis. Vi inspireras av argumentet i Perrin (1995, Lemma III.2.1) men formulerar oss på ett mer begripligt sätt. Vi börjar med att konstruera $\overline{\mathcal{F}}(U)$ för varje öppen mängd U. Låt U_i vara öppna mängder ur $\mathcal{U}$ sådana att $\bigcup_{i\in I} U_i = U$. Vi bildar mängden ${}^U k$ av alla funktioner från U till k och bildar mängden

$$\overline{\mathcal{F}}(U) = \{s \in {}^U k : s|_{U_i} \in \mathcal{F}(U_i) \text{ för alla } i \in I\}.$$

Låt $\{V_j\} \subset \mathcal{U}$ vara en annan uppdelning av U i öppna mängder. Vi bildar mängden

$$\underline{\mathcal{F}}(U) = \{s \in^U k : s|_{V_j} \in \mathcal{F}(V_j) \text{ för alla } j \in J\}.$$

Antag sedan att $s \in \overline{\mathcal{F}}(U)$, men att $s \notin \underline{\mathcal{F}}(U)$. Då finns ett V_j sådant att $s|_{V_j} \notin \mathcal{F}(V_j)$. Eftersom $\bigcup U_i = \bigcup V_j = U$ så är $\bigcup U_i$ en övertäckning av V_j, och eftersom $s|_{U_i} \in \mathcal{F}(U_i)$ för alla i så måste $s \in \mathcal{F}(V_j)$ enligt (2), så vi har nått en motsägelse och konstaterar att det inte spelar någon roll hur vi delar upp de öppna mängderna. $\overline{\mathcal{F}}$ är alltså väldefinierad.

Det som återstår att visa är att $\overline{\mathcal{F}}$ är en funktionskärve. Antag att $V \subset U$ är godtyckliga öppna mängder i X. Antag att $s \in \overline{\mathcal{F}}(U)$. Vi vill visa att $s|_V \in \overline{\mathcal{F}}(V)$, enligt vår definition av $\overline{\mathcal{F}}$ innebär detta att om $V = \bigcup_i V_i$ för $V_i \in \mathcal{U}$ så måste $(s|_V)|_{V_i} = s|_{V_i}$ ligga i $\mathcal{F}(V_i)$ för varje i, eftersom V_i är en delmängd av U så ingår den i någon övertäckning av U. Eftersom vi hade antagit att $s \in \overline{\mathcal{F}}(U)$ så måste alltså $s|_{V_i} \in \mathcal{F}(V_i)$. Eftersom $s|_{V_i} \in \mathcal{F}(V_i)$ för alla i och eftersom $s|_{V_i} = s|_V|_{V_i}$ så måste det vara så att $s_V \in \overline{\mathcal{F}}(V)$.

Vi har visat att $\overline{\mathcal{F}}$ är en funktionsprekärve. Nu vill vi visa att den inte bara är en prekärve utan att den är en riktig funktionskärve. Om så är fallet gäller för varje övertäckning $\{U_i\}$ av varje öppen mängd U att om det finns $f_i \in \overline{\mathcal{F}}(U_i)$ för varje i sådana att $f_i|_{U_i\cap U_j} = f_j|_{U_i\cap U_j}$ för varje par i, j, så finns en och endast en funktion $f \in \overline{\mathcal{F}}(U)$ sådan att $f|_{U_i} = f_i$ för alla i. Det är tämligen uppenbart att det finns åtminstone ett $f \in {}^U k$ sådant att $f|_{U_i} = f_i$ för alla i, nämligen det f som för varje x beräknas genom värdet av f_i om $x \in U_i$, en sådan definition är konsekvent eftersom vi antog att $f_i|_{U_i\cap U_j} = f_j|_{U_i\cap U_j}$. Av samma skäl kan det bara finnas precis ett sådant f eftersom hela dess definitionsmängd är innesluten i $\bigcup U_i$. Frågan är om ett sådant f är garanterat att ingå i $\overline{\mathcal{F}}(U)$. För att ta reda på det betraktar vi de öppna mängderna U_i lite närmare och inser att varje U_i är en union av element $\mathcal{U}_{i,j} \in \mathcal{U}$. Det innebär att varje $f_i = f|_{U_i}$ i $\overline{\mathcal{F}}(U_i)$ måste

ha egenskapen att $f_i|_{\mathcal{U}_{i,j}} \in \mathcal{F}(\mathcal{U}_{i,j})$ och alltså att $f_i|_{\mathcal{U}_{i,j}} = f_{U_i}|_{\mathcal{U}_{i,j}} \in \mathcal{F}(\mathcal{U}_{i,j})$ eftersom $\mathcal{U}_{i,j} \subset U_i$ måste det alltså gälla att $f|_{\mathcal{U}_{i,j}} \in \mathcal{F}(\mathcal{U}_{i,j})$. Eftersom $\bigcup \mathcal{U}_{i,j} = \bigcup U_i$ måste även $\{\mathcal{U}_{i,j}\}$ vara en övertäckning av U, och därmed kan vi konstatera att i och med att $f|_{\mathcal{U}_{i,j}} \in \mathcal{F}(\mathcal{U}_{i,j})$ för alla $\mathcal{U}_{i,j}$ så gäller att $f \in \overline{\mathcal{F}}(U)$.

Vi har alltså visat att $\overline{\mathcal{F}}$ är en funktionskärve. Allt som återstår är att visa att det inte kan finnas någon annan funktionskärve $\mathcal{F}'$ sådan att $\mathcal{F}'(U) = \mathcal{F}(U)$ om $U \in \mathcal{U}$. Om $U \in \mathcal{U}$ är det tämligen uppenbart att $s \in \mathcal{F}'(U)$ om och endast om $s \in \overline{\mathcal{F}}(U)$. Antag istället att vi har en öppen mängd $U \notin \mathcal{U}$. Antag sedan att det finns ett $s \in \overline{\mathcal{F}}(U)$ men $s \notin \mathcal{F}'(U)$. Vi vet att U är en union av $U_i \in \mathcal{U}$ och att $\overline{\mathcal{F}}$ är en funktionskärve, så vi kan direkt dra slutsatsen att om $s \in \overline{\mathcal{F}}(U)$ så gäller att $s|_{U_i} \in \overline{\mathcal{F}}(U_i)$ för alla U_i, och vi skriver $s_i = s|_{U_i}$. Härnäst inser vi att $s|_{U_i \cap U_j} = s|_{U_i}|_{U_i \cap U_j} = s_i|_{U_i \cap U_j}$ för alla par i, j, men att det dessutom måste gälla att $s|_{U_i \cap U_j} = s|_{U_j}|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$. Alltså gäller att $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$. Men, $\overline{\mathcal{F}}(U_i) = \mathcal{F}(U_i) = \mathcal{F}'(U_i)$, så detsamma gäller även i $\mathcal{F}'$, vilket gör att vi kan garantera att det unika s för vilket $s|_{U_i} = s_i$ även måste ingå i $\mathcal{F}'(U)$. Därav inser vi att $\overline{\mathcal{F}}(U) \subset \mathcal{F}'(U)$. Genom ett liknande resonemang ser vi att om $s \in \mathcal{F}'(U)$ så måste s också ingå i $\overline{\mathcal{F}}(U)$ så $\mathcal{F}'(U) \subset \overline{\mathcal{F}}(U)$ och $\overline{\mathcal{F}}(U) = \mathcal{F}'(U)$ för alla öppna mängder U. I så fall drar vi slutsatsen att $\overline{\mathcal{F}} = \mathcal{F}'$ och att $\overline{\mathcal{F}}$ är unik. □

Härnäst tänker vi oss följande situation. Vi har en algebraisk mängd V vars inducerade Zariskitopologi är X. Hur kan vi skapa en strukturkärve åt V? För det första är en sak värd att notera.

Lemma 7. *Låt V vara en algebraisk mängd i k^n och låt $I = \mathbf{I}(V)$. Ekvivalensklasserna i $\Gamma(V)$ består av de polynom som antar samma värden på V som klassernas representanter.*

Bevis. Antag att $G = (G_1, \ldots, G_s)$ är en reducerad Gröbnerbas för $\mathbf{I}(V)$, låt $f, g \in k[x_1, \ldots, x_n]$. Antag att f och g har samma representant i $k[x_1, \ldots, x_n]/I$. Det innebär att $\overline{f}^G = r$ och $\overline{g}^G = r$ och framförallt att $f = f_1G_1 + \cdots + f_sG_s + r$ och $g = g_1G_1 + \cdots + g_sG_s + r$. Eftersom V är de gemensamma nollställena för alla polynom i $\langle G_1, \ldots, G_s \rangle$ är $f|_V = r = g|_V$. Alltså är $f = g$ på V. □

Det är förvisso ingen djup insikt i sig, utan det viktiga i sammanhanget är att gränsen mellan ringkärvar och funktionskärvar kanske inte är så skarp. Om vi kunde definiera en funktionskärve på X, gärna baserad på $\Gamma(V)$, då kanske det går att förvandla funktionskärven till en ringkärve och därmed till en lämplig strukturkärve. Då skulle vi kunna förvandla varje algebraisk mängd till ett ringbestyckat rum, och just det kommer vi att ha nytta av senare. Vi kommer dock att behöva bekanta oss med multiplikativa mängder en aning. Vi lånar lite formuleringar från Perrin (1995, Mémento d'algèbre 1.6b).

Definition 47. *Låt R vara en kommutativ ring med identitet. En mängd $S \subset R$ kallas* multiplikativ *om $1 \in S$ och varje par $a, b \in S$ har egenskapen att $ab \in S$.*

Det viktiga i sammanhanget är att dessa multiplikativa mängder kan användas för att skapa en *lokalisering* av en ring. vi låter Grillet (2007) stå för inspirationen, men visar att lokaliseringar verkligen är ringar.

Definition 48. *Låt R vara en kommutativ ring med identitet och S en multiplikativ delmängd av R. Låt $\sim$ vara en relation på $R \times S$ sådan att*

$$(r_1, s_1) \sim (r_2, s_2) \iff \exists t \in S : t(r_1 \cdot s_2 - r_2 \cdot s_1) = 0.$$

Vi skriver r/s eller $\frac{r}{s}$ för att beteckna $(r, s) \in (R \times S)$.

Det visar sig förstås att $\sim$ är en ekvivalensrelation, framförallt visar det sig att $(R \times S)/\sim$ är en ring.

Sats 28. *Låt R vara en kommutativ ring med identitet och låt S vara en multiplikativ delmängd sådan att $0 \notin S$. Då är $\sim$ en ekvivalensrelation och $(R\times S)/\sim$ är en ring under följande operationer:*

$$r_1/s_1 + r_2/s_2 = (r_1s_2 + r_2s_1)/(s_1s_2)$$

och

$$(r_1/s_1) \cdot (r_2/s_2) = (r_1r_2)/(s_1s_2)$$

Bevis. Vi börjar med att visa att $\sim$ är reflexiv, symmetrisk och transitiv. När vi har konstaterat att $\sim$ är en ekvivalensrelation visar vi att $(R \times S)/\sim$ är en ring.

Det är uppenbart att $(r, s) \sim (r, s)$ för alla $r \in R$, $s \in S$, eftersom

$$1(r \cdot s - r \cdot s) = 1 \cdot 0 = 0,$$

så $\sim$ är reflexiv. Vi vill visa att $\sim$ är symmetrisk, låt $r_1, r_2 \in R$ $s_1, s_2 \in S$. Då ser vi att $(r_1, s_1) \sim (r_2, s_2)$ om och endast om det finns ett $t \in S$, sådant att

$$t(r_1s_2 - r_2s_1) = 0$$

vilket så klart medför att $tr_1s_2 = tr_2s_1$, vilket i sin tur innebär att $0 = t(r_2s_1 - r_1, s_2)$ och att $(r_2, s_2) \sim (r_1, s_1)$. Alltså måste $\sim$ vara symmetrisk. Vi undersöker huruvida $\sim$ är transitiv genom att postulera att om $(r_1, s_1) \sim (r_2, s_2)$ och $(r_2, s_2) \sim (r_3, s_3)$, då måste det vara så att det finns $t_1, t_2 \in S$ sådana att $t_1(r_1s_2 - r_2s_1) = 0$ och $t_2(r_2s_3 - r_3s_2) = 0$ men vill visa att det dessutom finns ett $t_3 \in S$ sådant att $t_3(r_1s_3 - r_3s_1) = 0$. Så är förstås fallet om och endast om $t_3r_1s_3 = t_3r_3s_1$. Vi inser förstås att

$$t_1(r_1s_2 - r_2s_1) = 0 \iff t_1s_2r_1 = t_1s_1r_2,$$

och vi förstår utan vidare att

$$t_2(r_2s_3 - r_3s_2) = 0 \implies \forall s \in S : st_2(r_2s_3 - r_3s_2) = s \cdot 0 = 0$$

och fortsätter genom att sätta $s = t_1s_1$ så att vi får

$$t_1s_1t_2(r_2s_3 - r_3s_2) = 0 \implies t_2t_1s_1r_2s_3 = t_2t_1s_1r_3s_2.$$

Men då är vår lycka gjord eftersom vi vet att $t_1s_1r_2 = t_1s_2r_1$, så genom lämpliga förändringar i vänsterledet får vi

$$(t_2t_1s_2)r_1s_3 = (t_2t_1s_2)r_3s_1 \implies (t_1t_2s_2)(r_1s_3 - r_3s_1) = 0.$$

Eftersom $t_1, t_2, s_2 \in S$ och S är multiplikativt sluten så ligger $t_1t_2s_2 \in S$ och därmed måste det gälla att $(r_1, s_1) \sim (r_3, s_3)$. Alltså är $\sim$ en ekvivalensrelation.

Allt som återstår är att visa att $(R \times S)/\sim$ är en ring. För att förenkla saker och ting antar vi redan från början att $(R \times S)/\sim$ är kommutativ, det framgår redan av definitionen att både multiplikationen och additionen måste

vara kommutativa. Vi börjar sedan med att visa att operationerna på $(R\times S)/\sim$ är väldefinierade. Låt $r_1/s_1 \sim r_1'/s_1'$ och låt $r_2/s_2 \sim r_2'/s_2'$. Vi ser att

$$r_1/s_1 + r_2/s_2 = \frac{r_1s_2 + r_2s_1}{s_1s_2} \qquad \text{och} \qquad \frac{r_1}{s_1}\cdot\frac{r_2}{s_2} = \frac{r_1r_2}{s_1s_2}$$

och

$$r_1'/s_1' + r_2'/s_2' = \frac{r_1's_2' + r_2's_1'}{s_1's_2'} \qquad \text{och} \qquad \frac{r_1'}{s_1'}\cdot\frac{r_2'}{s_2'} = \frac{r_1'r_2'}{s_1's_2'}$$

vi vet att det finns $t_1, t_2 \in S$ sådana att $t_1r_1s_1' = t_1r_1's_1$ och $t_2r_2s_2' = t_2r_2's_2$ och vill visa att det finns $t_3, t_4 \in S$ sådana att

$$t_3((r_1's_2' + r_2's_1')(s_1s_2)) = t_3((r_1s_2 + r_2s_1)(s_1's_2')) \tag{1}$$

eftersom det skulle innebära att additionen vore väldefinierad, och

$$t_4(r_1'r_2's_1s_2) = t_4(r_1r_2s_1's_2') \tag{2}$$

eftersom det skulle betyda att multiplikationen vore väldefinierad. Vi börjar med att undersöka additionen. Vi låter vår intuition säga oss att $t_3 = t_1t_2$. Då ser vi med en gång att vänsterledet av (1) kan skrivas om enligt

$$\begin{aligned} t_3r_1's_2's_1s_2 + t_3r_2's_1's_1s_2 &= (t_1r_1's_1)(t_2s_2's_2) + (t_2r_2's_2)(t_1s_1's_1) \\ &= (t_1r_1s_1')(t_2s_2's_2) + (t_2r_2s_2')(t_1s_1's_1) \\ &= t_1t_2r_1s_1's_2's_2 + t_1t_2r_2s_1's_1s_2' \\ &= t_3(r_1s_1's_2's_2 + r_2s_1's_1s_2') \\ &= t_3((r_1s_2 + r_2s_1)(s_1's_2')), \end{aligned}$$

som ju är högerledet i (1). Därmed är det visat att additionen är väldefinierad. När det gäller multiplikationen provar vi samma finurliga knep, att sätta in $t_4 = t_1t_2$ i (2). Vi undersöker vänsterledet i (2) och ser att

$$t_4(r_1'r_2's_1s_2) = (t_1r_1's_1)(t_2r_2's_2) = (t_1r_1s_1')(t_2r_2s_2') = t_4(r_1r_2s_1's_2'),$$

som är (2):s högerled. Alltså är både additionen och multiplikationen väldefinierade i $(R \times S)/\sim$.

Vi fortsätter med att avgöra huruvida $(R\times S)\sim$ är en ring. Det är tydligt att $(R\times S)$ är sluten båda med avseende på addition och multiplikation. Vi fortsätter med att visa att additionen är associativ. Låt $r_1/s_1, r_2/s_2, r_3/s_3 \in (R \times S)/\sim$ vi vill visa att $(r_1/s_1 + r_2/s_2) + r_3/s_3 = r_1/s_1 + (r_2/s_2 + r_3/s_3)$. Det gör vi genom att konstatera att

$$\left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right) + \frac{r_3}{s_3} = \frac{r_1s_2 + r_2s_1}{s_1s_2} + \frac{r_3}{s_3} = \frac{r_1s_2s_3 + r_2s_1s_3 + r_3s_1s_2}{s_1s_2s_3}$$

och genom att jämföra med

$$\frac{r_1}{s_1} + \left(\frac{r_2}{s_2} + \frac{r_3}{s_3}\right) = \frac{r_1}{s_1} + \frac{r_2s_3 + r_3s_2}{s_2s_3} = \frac{r_1s_2s_3 + r_2s_1s_3 + r_3s_1s_2}{s_1s_2s_3},$$

vilket naturligtvis betyder att additionen är associativ. Härnäst visar vi att det finns en additiv identitet, nämligen $0/1$. Låt $r/s \in (R \times S)$, då gäller att

$0/1 + r/s = \frac{0s+r}{s} = \frac{r+0s}{s} = r/s + 0/1$, så det finns en additiv identitet. Vi visar att det finns additiva inverser till varje $r/s \in (R \times S)$ genom att konstatera att

$$r/s + (-r)/s = \frac{rs - rs}{s^2} = \frac{0}{s^2} \sim \frac{0}{1},$$

eftersom $t(0 \cdot s^2 - 0 \cdot 1) = 0$ för alla t. Det är tämligen uppenbart att additionen är kommutativ, låt $r_2/s_1, r_2/s_2 \in (R \times S)/\sim$, då ser vi att

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} = \frac{r_2 s_1 + r_1 s_2}{s_2 s_1} = \frac{r_2}{s_2} + \frac{r_1}{s_1}.$$

Vi har alltså konstaterat att $(R \times S)/\sim$ är en abelsk grupp med avseende på additionen. Det som återstår är att visa att den är en monoid med avseende på multiplikationen och att distributivitetslagarna är uppfyllda.

Att multiplikationen är sluten råder det inte minsta tvivel om, men för att den ska vara en monoid måste vi för det första visa att multiplikationen är associativ, för det andra måste vi visa att det finns en identitet. Låt därför $r_1/s_1, r_2/s_2, r_3/s_3 \in (R \times S)/\sim$. Vi ser direkt att

$$\left(\frac{r_1}{s_1}\frac{r_2}{s_2}\right)\frac{r_3}{s_3} = \frac{r_1 r_2}{s_1 s_2}\frac{r_3}{s_3} = \frac{r_1 r_2 r_3}{s_1 s_2 s_3} = \frac{r_1}{s_1}\frac{r_2 r_3}{s_2 s_3} = \frac{r_1}{s_1}\left(\frac{r_2}{s_2}\frac{r_3}{s_3}\right),$$

så multiplikationen är associativ. Vi undersöker sedan som hastigast om inte $1/1$ skulle råka vara identiteten, låt $r/s \in (R \times S)/\sim$, då ser vi att

$$\frac{r}{s}\frac{1}{1} = \frac{r \cdot 1}{s \cdot 1} = \frac{r}{s} = \frac{1}{1}\frac{r}{s}.$$

Slutligen visar vi att distributivitetslagarna är uppfyllda. Antag att

$$r_1/s_1, r_2/s_2, r_3/s_3 \in (R \times S)/\sim .$$

Vi ser att

$$\left(\frac{r_1}{s_1} + \frac{r_2}{s_1}\right)\frac{r_3}{s_r} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}\frac{r_3}{s_3} = \frac{r_1 s_2 r_3 + r_2 s_1 r_3}{s_1 s_2 s_3}.$$

Vi ser också att

$$\frac{r_1 r_3 s_3 s_2 + r_2 r_3 s_3 s_1}{s_1 s_2 s_3^2} = \frac{r_1 r_3 (s_3 s_2) + r_2 r_3 (s_3 s_1)}{(s_1 s_3)(s_2 s_3)} = \frac{r_1 r_3}{s_1 s_3} + \frac{r_2 r_3}{s_2 s_3} = \frac{r_1}{s_1}\frac{r_3}{s_3} + \frac{r_2}{s_2}\frac{r_3}{s_3}.$$

Vi vill alltså verifiera att

$$\frac{r_1 r_3 s_2 + r_2 r_3 s_1}{s_1 s_2 s_3} \sim \frac{r_1 r_3 s_2 s_3 + r_2 r_3 s_1 s_3}{s_1 s_2 s_3^2}.$$

Ett beprövat knep för att visa att två storheter är samma storhet är att multiplicera med 1. I $(R \times S)/\sim$ är $1/1$ den multiplikativa identiteten, och lyckligtvis ger vilket $s \in S$ som helst $1/1 \sim s/s$ eftersom $1(1 \cdot s - s \cdot 1) = 0$. Vi ser därför att

$$\frac{r_1 r_3 s_2 + r_1 r_3 s_1}{s_1 s_2 s_3} \sim \frac{r_1 r_3 s_2 + r_1 r_3 s_1}{s_1 s_2 s_3}\frac{s_3}{s_3} \sim \frac{r_1 r_3 s_2 s_3 + r_2 r_3 s_1 s_3}{s_1 s_2 s_3^2},$$

vilket var precis vad vi önskade. Slutsatsen är att $(R \times S)/\sim$ är distributiv och att det är frågan om en ring. □

För enkelhetens skull ger vi vår nya ring ett namn, och inför ett mer praktiskt beteckningssätt.

Definition 49. *Låt R vara en kommutativ ring med identitet och låt S vara en multiplikativ delmängd av R sådan att $0 \notin S$. Vi skriver $S^{-1}R = R_S = (R \times S)/\sim$ och kallar R_S för R:s* lokalisering *till S.*

Det vi egentligen har för avsikt att göra är att modifiera $\Gamma(V)$ genom att lokalisera den på något lämpligt vis. Om vi har ett nollskilt polynom i $f \in \Gamma(V)$ kan vi bilda mängden $S = \{g \in \Gamma(V) : \exists n \in \mathbb{N} : g = f^n\}$ som är uppenbart multiplikativ. Vi inför ett beteckningssätt.

Definition 50. *Låt $f \in \Gamma(V)$ och låt f vara nollskild. Vi bildar den multiplikativa mängden $S_f = \{g \in \Gamma(V) : \exists n \in \mathbb{N} : g = f^n\}$ och skriver $\Gamma(V)_f = S_f^{-1}\Gamma(V) = \Gamma(V)_{S_f}$ för att beteckna $\Gamma(V)$:s lokalisering till S_f.*

Vi återvänder till frågan om strukturkärven för en algebraisk mängd V. Tanken är att vi gör om V till ett topologiskt rum X med V:s inducerade Zariskitopologi, kärven ska associera V med desss koordinatring, och ska associera mängderna i X:s bas med olika lokaliseringar av $\Gamma(V)$. Eftersom varje baselement består av snittet mellan X och komplementet till mängden av något polynoms nollställen kan vi relativt kvickt konstruera ett kärve för varje irreducibel algebraisk mängd V, för bevis se Perrin (1995, Vérification III.2.4).

Sats 29. *Låt $f \in \Gamma(V)$ var nollskild, då låter vi $D(f)$ beteckna mängden $V - \mathbf{V}(f)$. Om V är en irreducibel affin algebraisk mängd finns det ett kärve $\mathcal{O}_V$ på V:s Zariskitopologi X som associerar X med $\Gamma(V)$, sådant att om $D(f)$ ligger i X:s bas så är $\mathcal{O}_V(D(f)) = \Gamma(V)_f$ och sådant att restriktionen av varje $g \in \Gamma(V)$ till $D(f)$ är avbildningen $i : g \mapsto g/1$. Vi kallar kärven för V:s kärve av reguljära funktioner.*

Det går också att göra på samma sätt när V inte är irreducibel, men då är inte de inblandade ringarna lika trevliga.

6.2 Varieteter

Tanken med kärvarna var att vi skulle formulera om själva idén om den algebraiska mängden i modernare ordalag, i termer av ringbestyckade rum. Perrin (1995, kapitel III.3) hjälper oss på vägen.

Vi inför ett morfismbegrepp för ringbestyckade rum, tanken är att om $(X, \mathcal{O}_X)$ och $(Y, \mathcal{O}_Y)$ är ringbestyckade rum och om vi kan hitta en kontinuerlig funktion $\phi : X \to Y$ som liksom översätter X till Y och om det visar sig att det är samma kärve, då är ϕ en morfism.

Definition 51. *Låt $(X, \mathcal{O}_X)$ och $(Y, \mathcal{O}_Y)$ vara ringbestyckade rum. Vi kallar $\phi : X \to Y$ för en morfism mellan ringbestyckade rum om den är kontinuerlig och om vi för varje öppen mängd $U \in Y$ och varje $f \in \mathcal{O}_Y(U)$ kan konstatera att $\phi(f) \in \mathcal{O}_X(\phi^{-1}(U))$. Två ringbestyckade rum kallas isomorfa om ϕ är en homeomorfism mellan X och Y.*

Vi har redan funnit strukturkärvar som passar till algebraiska mängder och deras Zariskitopologier. Vi vill gärna att de ringbestyckade rummen som dessa sturkturkärvar bildar med sina algebraiska mängder ska utgöra grunden för de

nya begreppen, men vi behöver förstås inte begränsa oss onödigt mycket. Vi låter ringbestyckade rum som är tillräckligt likna de algebraiska mängderna räknas som fullvärdiga.

Definition 52. *En affin algebraisk varietet är ett ringbestyckat topologiskt rum* $(X, \mathcal{O}_X)$ *som är isomorft med ett ringbestyckat rum* $(V, \mathcal{O}_V)$ *där* V *är en algebraisk mängd i* k^n *och* $\mathcal{O}_V$ *är dess kärve av reguljära funktioner.*

Om å andra sidan vi kan finna ett ringbestyckat rum som liknar en algebraisk mängd, men som kanske inte är isomorf med $(V, \mathcal{O}_V)$, så kallar vi det helt enkelt för en algebraisk varietet.

Definition 53. *Ett ringbestyckat rum* $(X, \mathcal{O}_X)$ *kallas för en* algebraisk varietet *om* X *är kvasikompakt*[26] *och om varje* $x \in X$ *ingår i någon öppen mängd* $U \subset X$ *sådan att* $(U, \mathcal{O}_X|_U)$ *är isomorf med en affin algebraisk varietet.*

Beskrivningen ovan är en aning abstrakt. Om matematikens uppgift vore att göra det begripliga obegripligt och om 1900-talet karaktäriserades av den här sortens formuleringar så skulle vetenskapen ha gjort stora framsteg de senaste 100 åren. Vetenskapen har visserligen inte stagnerat, men den har förhoppningsvis inte heller blivit obegriplig.

Om vi istället för att utgå från kärven utgår från det topologiska rummet när vi försöker bilda oss en uppfattning av vad en affin algebraisk varietet är för något, då blir saker en aning klarare. Att varieteten är isomorf med en algebraisk mängd och dess förknippade reguljära funktioner betyder då att varje affin algebraisk varietet väsentligen består av en algebraisk mängd, och att det vi är intresserade av är de öppna delmängderna. De öppna mängderna är, som bekant, komplementen till alla ändliga punktmängder och snitten av dessa med komplementen till mängdens irreducibla komponenter. Eftersom det finns en bijektion mellan öppna och slutna mängder kan vi betrakta det som att varje punkt och varje irreducibel komponent finns representerad i topologin, och dessutom att alla ändliga unioner av dessa också är representerade. I någon bemärkelse är alltså Zariskitopologin en direkt motsvarighet till själva den algebraiska mängden men med extra punkter för alla algebraiska delmängder.

Dessa öppna mängder är associerade med olika ringar vars element är funktioner på sina respektive öppna mängder. Själva kärvestrukturen kommer vi att använda för att skapa lokala ringar och groddar.

Vi ska uptäcka att dessa algebraiska varieteter i princip består av en uppsättning affina algebraiska varieteter. Av definitionen framgår det att vissa öppna mängder i en algebraisk varietet svarar mot affina algebraiska mängder. Vi ger dem ett särskilt namn, den här gången från Perrin (1995, kapitel III.4).

Definition 54. *Låt* $(X, \mathcal{O}_X)$ *vara en algebraisk varietet. En öppen delmängd* $U \subset X$ *kallas för en affin öppen mängd om* $(U, \mathcal{O}_X|_U)$ *är en affin algebraisk varietet.*

Det framgår tydligt av definitionen av en algebraisk varietet att det måste finnas en övertäckning av affina öppna mängder, men det visar sig att det blir bättre, enligt sats III.4.3 i Perrin (1995) gäller nämligen följande.

Sats 30. *Låt* $(X, \mathcal{O}_X)$ *vara en algebraisk varietet. Då finns en ändlig mängd affina öppna mängder* $U_1, \ldots, U_n$ *sådana att* $\{U_i\}$ *är en bas för* X*.*

[26] Varje övertäckning har en ändlig delmängd som också är en övertäckning.

6.3 Groddar

För vissa typer av frågeställningar behöver vi diskutera en algebraisk varietets lokala egenskaper. I varieteternas strukturkärvar finns redan lokaliseringar till öppna mängder definierade, men man kan fråga sig hur lokal en lokalisering till allt utom ett ändligt antal punkter egentligen kan vara. Vi ska konstruera *lokala ringar* på algebraiska varieteter, och börjar med att definiera så kallade groddar enligt Perrins exempel (Perrin 1995, kapitel III.5).

Definition 55. *Låt $(X, \mathcal{O}_X)$ vara en algebraisk varietet och låt $x \in X$. Om U är en öppen mängd med $x \in U$ så kan vi bilda en mängd $M_U = \{(U, f) : f \in \mathcal{O}_X(U)\}$. Låt $\mathcal{U}$ vara mängden av alla öppna mängder i X där x ingår, då kan vi bilda mängden $M = \bigcup_{U \in \mathcal{U}} M_U$. Låt $(U, f) \sim_M (U, g)$ om det finns ett $(W, h) \in M$ sådant att $W \subset U \cap W$ och $f|_W = g|_W = h$. Då kan vi definiera mängden $\mathcal{O}_{X,x} = M/\sim_M$. Vi kallar elementen i $\mathcal{O}_{X,x}$ för* groddar *och om f har den öppna mängden U som definitionsmängd använder beteckningen f_x för att betrakta grodden $(U, f) \in \mathcal{O}_{X,x}$.*

Vi kan ge $\mathcal{O}_{X,x}$ en ringstruktur enligt följande sats ur Perrin (1995, Sats III.5.2)

Sats 31. *Mängden $\mathcal{O}_{X,x}$ är behäftad med en naturlig ringstruktur. Ringen i fråga är en lokal k-algebra med de maximala idealet $m_{X,x} = \{f \in \mathcal{O}_{X,x} : f(x) = 0\}$. Dessutom gäller att $\mathcal{O}_{X,x}/m_{X,x} \cong k$.*

Summan eller produkten av $(U, f), (V, g) \in \mathcal{O}_{X,x}$ fås förstås genom att välja ut en lämplig delmängd $W \subset U \cap V$ och genom att sedan addera eller multiplicera $f|_W$ och $g|_W$.

Definition 56. *Låt $(X, \mathcal{O}_X)$ vara en algebraisk varietet och låt $x \in X$. Vi kallar $\mathcal{O}_{X,x}$ för $(X, \mathcal{O}_X)$:s lokala ring i punkten x.*

6.4 Scheman

Schema är hämtat från franskans *schéma* och engelskans *scheme*. Ordagrant betyder det skiss, ritning eller översikt. Ordet har den enda nackdelen att vi i Sverige gärna använder det för att beteckna olika former av tidsplaneringar. Själva ordet *schéma* är i sig varken ett franskt eller engelskt ord från början. Det har uppstått ur den klassiska grekiskans σχῆμα, som enligt Passow (1841, σχῆμα, ατος, τό) visserligen kan översättas till ”teckning, grundritning, utkast”, men som framförallt syftar på någon eller någots gestalt, utseende, form eller framställning. Utan att bli för filologiska kan vi tillägga att det grekiska ordet syftar just till ett föremåls geometriska form när det används i ett matematiskt sammanhang (Liddell m.fl. 1996, σχῆμα, ατος, τό, 8a). Man kan visserligen fråga sig hur djupa grekiskkunskaper 1900-talets matematiker hade och om det inte snarare har kommit via latinet, men med tanke på det tidiga 1900-talets utbildningssystem så är det inte osannolikt att de hade grundläggande grekiskkunskaper. Oavsett hur det förhåller sig med den saken så är ordets gammelgrekiska betydelse inte helt ointressant i sammanhanget. Det visar sig nämligen att ett schema på sätt och vis är en gestaltning av något, närmare bestämt är det lite som en geometrisk tolkning av en godtycklig kommutativ ring.

Som bekant har varje affin algebraisk varietet $(V, \mathcal{O}_V)$ en så kallad *koordinatring*. Eftersom koordinatringen i sig innehåller all relevant information om

varieteten och dess Zariskitopologi så kan vi lika gärna betrakta det som att en varietet är en geometrisk tolkning av koordinatring. Om vi ska kunna göra det så måste vi kunna hitta ett sätt att extrahera den geometriska informationen ur koordinatringen, i synnerhet måste vi kunna få fram Zariskitopologin. Vi tar hjälp av Eisenbud m.fl. (2000).

Definition 57. *Låt R vara en kommutativ ring med identitet. Vi bildar mängden*

$$\mathrm{Spec}(R) = \{I \subset R : I \text{ är ett primideal}\}$$

och kallar den för R:s spektrum.

Tanken med dessa spektrum är förstås att om $\Gamma(V)$ är en algebraisk mängds koordinatring, vars primideal dels är V:s punkter och dels är dess övriga irreducibla algebraiska delmängder, så kan vi i princip återskapa både V och Zariskitopologin på V med hjälp av $\mathrm{Spec}(\Gamma(V))$. Hur ska vi egentligen kunna finna *funktioner* sådana att V:s öppna mängder är noll på dessa funktioner om allt vi har att utgå från är en ring och ett par ideal? Vi definierar fram nya ”funktioner” som trots att de verkar högst märkliga visar sig vara ungefär som vanliga funktioner i vanliga fall.

Definition 58. *Låt R vara en kommutativ ring med identitet. Vi associerar varje punkt $f \in R$ med en funktion $\phi_f : \mathrm{Spec}(R) \to R$ sådan att om $\iota_{\mathfrak{a}} : R \to R/\mathfrak{a}$ är den naturliga homomorfismen mellan R och $R/\mathfrak{a}$ så är*

$$\phi_f(\mathfrak{a}) = \iota_{\mathfrak{a}}(f).$$

Vi skriver $f(\mathfrak{a})$ för att beteckna $\phi_f(\mathfrak{a})$.

Lite närmare bestämt kan vi visa att dessa lite udda ”funktioner” på sätt och vis svarar mot våra vanliga funktioner om den kommutativa ringen R råkar vara en koordinatring.

Sats 32. *Låt V vara en algebraisk mängd och låt $\Gamma(V)$ vara dess koordinatring. Om $f \in \Gamma(V)$ och $\xi \in \mathrm{Spec}(\Gamma(V))$ är det maximala ideal i $\Gamma(V)$ som svarar mot punkten x, då gäller att*

$$f(\xi) = f(x).$$

Bevis. Att ξ svarar mot $x = (\xi_1, \xi_2, \ldots, \xi_n)$ innebär att ξ är det maximala idealet $\langle x_1 - \xi_1, x_2 - \xi_2, \ldots, x_n - \xi_n \rangle \subset k[x_1, \ldots, x_n]$. Vi visar genom induktion över antalet variabler att satsen gäller i alla $k[x_1, \ldots, x_n]$.

Vi antar först att $V \subset k$. I $k[x_1]$ och $k[x_1]/\mathbf{I}(V)$ gäller att det maximala ideal som svarar mot punkten ξ_1 genereras av $\langle x_1 - \xi_1 \rangle$. Framförallt vet vi att varje polynom f av grad m måste gå att faktorisera enligt

$$f = c \cdot \prod_{i=1}^{m} (x_1 - \alpha_i) = c \cdot \prod_{i=1}^{m} ((x_1 - \xi_1) + (\xi_1 - \alpha_i))$$

då kan vi hitta ett polynom h sådant att

$$f = c(x_1 - \xi_1) \cdot h + c \cdot \prod_{i=1}^{m} (\xi_1 - \alpha_i) = c(x_1 - \xi_1) \cdot h + f(\xi_1).$$

Vi avbildar f in i $\Gamma(V)/\langle x_1 - \xi_1\rangle$ på det uppenbara sättet och får $f(\xi) = f(\xi_1)$. Alltså gäller satsen i basfallet.

Vi använder följande induktionantagnde: Om $V \subset k^{n-1}$ är en algebraisk mängd och $\xi = \langle x_1 - \xi_1, \ldots, x_{n-1} - \xi_{n-1}\rangle$ är det maximala ideal i $\Gamma(V)$ som svarar mot punkten $x = (\xi_1, \ldots, \xi_{n-1}) \in V$ då gäller för varje polynom $f \in \Gamma(V)$ att $f(\xi) = f(x)$.

Vi övergår sedan till vårt induktionssteg. Låt $V \subset k^n$ vara en algebraisk mängd och låt $\xi = \langle x_1 - \xi_1, \ldots, x_n - \xi_n\rangle$ vara det maximala ideal i $\Gamma(V)$ som svarar mot punkten $x = (\xi_1, \ldots, \xi_n) \in V$. Låt sedan $f \in \Gamma(V)$ vara ett polynom av grad m. Vi inser att det finns $h_i \in k[x_1, \ldots, x_{n-1}]$ sådana att

$$f = \sum_{i=0}^{m} h_i \cdot x_n^i.$$

Om vi betraktar h_i som polynom i $\Gamma(k^{n-1}) = k[x_1, \ldots, x_{n-1}]$ så vet vi, enligt induktionsantagandet, att det kan skrivas på formen $h_i = h_i(\xi_1, \ldots, \xi_{n-1}) + I_i$ där $I_i \in \langle x_1 - \xi_1, \ldots, x_{n-1} - \xi_{n-1}\rangle$. Om vi sätter in den nyvunna kunskapen i f ser vi att

$$f = \sum_{i=0}^{m} (h_i(x) + I_i)x_n^i = \sum_{i=0}^{m} h_i(x)x_n^i + \sum_{i=0}^{m} I_i x_n^i.$$

Varje x_n^i är förstås i sig ett polynom i en variabel, vi skriver om f en gång till med hjälp av polynomen g_i.

$$\begin{aligned} f &= \sum_{i=0}^{m} h_i(x)(x_n - \xi_n + \xi_n)^i + \sum_{i=0}^{m} I_i x_n^i \\ &= \sum_{i=0}^{m} \left(h_i(x)(x_n - \xi_n) \cdot g_i + h_i(x)\xi_n^i\right) + \sum_{i=0}^{m} I_i x_n^i \\ &= \sum_{i=0}^{m} h_i(x)\xi_n^i + \sum_{i=0}^{m} \left(h_i(x)g_i \cdot (x_n - \xi_n) + I_i x_n^i\right) \\ &= f(x) + \sum_{i=0}^{m} \left(h_i(x)g_i \cdot (x_n - \xi_n) + I_i x_n^i\right). \end{aligned}$$

Den uppmärksamme läsaren ser att

$$\sum_{i=0}^{m} \left(h_i(x) \cdot g_i \cdot (x_n - \xi_n) + I_i x_n^i\right) \in \xi,$$

i själva verket gäller alltså att $f = f(x) + I$ där $I \in \xi$, och därmed måste det också vara så att $f(\xi) = f(x)$.

Vi kan alltså dra slutsatsen att lemmat håller oavsett antalet variabler och att det därmed är bevisat. □

När vi alltså har dragit slutsatsen att de nya funktionerna fungerar som de gamla i de fall båda går att använda så kan vi enkelt definiera något som vi ska kalla *Zariskitopologin* på $\mathrm{Spec}(R)$.

Definition 59. *Låt R vara en kommutativ ring med identitet. Vi bildar en topologi,* Zariskitopologin*, på* $\mathrm{Spec}(R)$ *på följande vis.*

Låt $S \subset R$ vara en mängd funktioner[27] *i R. Vi associerar en sluten mängd $V(S) \subset \mathrm{Spec}(R)$ med varje S så att*

$$V(S) = \{x \in \mathrm{Spec}(R) : \forall f \in S : f(x) = 0\}.$$

Då kan vi bilda ett topologiskt rum X på $\mathrm{Spec}(R)$ som består av de öppna mängderna

$$X = \{\mathrm{Spec}\, R - V(S) : S \subset R\}.$$

Vi kallar X för $\mathrm{Spec}(R)$:s Zariskitopologi.

Vi ser förstås att om $R = \Gamma(V)$ för någon algebraisk mängd V, så är det den vanliga Zariskitopologin det rör sig om.

Efter att ha funnit motsvarigheter till Zariskitopologin och den algebraiska mängden har det blivit dags att finna en motsvarighet till kärvar av reguljära funktioner på $\Gamma(V)$. Tanken har än så länge varit att vi skulle låtsas som om vi befann oss i en koordinatring. Om vi gjorde det kunde vi definiera $\mathcal{O}_{\mathrm{Spec}(R)}$ genom att sätta $\mathcal{O}_{\mathrm{Spec}(R)}(D(f)) = R_f$, det vill säga då kunde vi definiera kärven genom att lokalisera koordinatringen till någon lämplig multiplikativ mängd. Om R skulle råka vara till exempel $\mathbb{Z}$ eller en koordinatring så fungerar den här konstruktionen utan vidare. Problemet är om vi väljer en ring, till exempel $\mathbb{Z}_4$, som innehåller nilpotenta element. När vi beskrev lokaliseringar och multiplikativa mängder hoppade vi över fallet där en ring lokaliseras till en multiplikativ delmängd som innehåller 0. Ett litet lemma är på sin plats.

Lemma 8. *Låt R vara en kommutativ ring med identitet och låt S vara en multiplikativ delmängd sådan att $0 \in S$. Då innehåller R_S precis ett element.*

Bevis. Låt a/b och c/d vara två element i R_S. Vi ser på en gång att $a/b \sim c/d$ eftersom $t(ac - db) = 0$ om vi väljer $t = 0 \in S$. Alltså finns bara en ekvivalensklass av element ur $R \times S$ under $\sim$ och därmed finns bara ett element i R_S. □

De öppna mängderna $D(f)$ kallas för de distingerade öppna mängderna av Eisenbud m.fl. (2000). De utgör en bas för Zariskitopologin på $\mathrm{Spec}(R)$, och i likhet med när vi konstruerade kärvar på de algebraiska mängderna kan vi förstås konstruera kärvar på $\mathrm{Spec}\, R$ på basen. Vi lånar sats I-18 ur Eisenbud m.fl. (2000).

Sats 33. *Låt R vara en kommutativ ring med identitet och låt $X = \mathrm{Spec}(R)$. Antag att $D(f)$ täcks av de öppna mängderna $D(f_a) \subset D(f)$. Då gäller följande.*

1. *Om $g, h \in R_f$ är lika i alla R_{f_a} så är de lika i R_f.*
2. *Om det för varje a finns ett $g_a \in R_{f_a}$ sådant att sådan att $g_a = g_b$ i $R_{f_a f_b}$ för varje par a, b, då finns ett $g \in R_f$ sådant att $g = g_a$ i R_{f_a} för varje a.*

Med andra ord uppfyller lokaliseringsoperationen på basen de krav som ställs för att det ska finnas en unik kärve $\mathcal{O}_{\mathrm{Spec}\, R}$ sådant att $\mathcal{O}_{\mathrm{Spec}\, R}(D(f)) = R_f$. Vi kallar denna kärve för R:s kärve av reguljära funktioner.

[27] Det är alltså våra nydefinierade ”funktioner” det handlar om, inte vanliga funktioner.

Den här kärven är det sista vi behöver för att kunna definiera våra scheman. I princip är ett schema en utvidgning av den algebraiska varieteten, precis som i fallet med varieteter definierar vi först en enklare variant med epitetet affint.

Definition 60. *Vi kallar ett ringbsetyckat rum* $(X, \mathcal{O}_X)$ *för ett* affint schema *om det är isomorft med ett ringbestyckat rum* $(\mathrm{Spec}(R), \mathcal{O}_{\mathrm{Spec}(R)})$ *där* R *är en kommutativ ring med identitet och* $\mathcal{O}_{\mathrm{Spec}(R)}$ *är dess förknippade reguljära funktioner.*

På precis samma sätt fortsätter vi sedan att definiera ett schema som ett ringbestyckat rum som åtminstone lokalt är ett affint schema.

Definition 61. *Låt* $(X, \mathcal{O}_X)$ *vara ett ringbestyckat rum. Om det finns en öppen övertäckning* U_i *av* X *sådan att* $(U_i, \mathcal{O}_X|_{U_i})$ *är ett affint schema för varje* U_i*, då kallar vi* $(X, \mathcal{O}_X)$ *för ett* schema.

Därmed är vi färdiga med vår korta introduktion till några moderna algebraiskgeometriska strukturer. Genom den algebraiska geometrins ursprung och kärna, den algebraiska mängden, har vi introducerat den algebraiska geometrins undersökningsområde. Med hjälp av dels abstraktalgebraiska verktyg, dels topologiska verktyg och ett och annat från här och var har vi svarat på en del enklare frågeställningar. Slutligen har vi generaliserat den algebraiska geometrins begrepp och därmed skapat en grund för vidare efterforskningar. Syftet: att ge läsaren en hastig inblick i den algebraiska geometrins värld.

Referenser

Brieskorn, Egbert & Knörrer, Horst (1981). *Ebene algebraische Kurven*. Boston: Birkhauser

Cox, David, Little, John & O'Shea, Donal (1997).*Ideals, varieties and algorithms: an introduction to computational algebraic geometry and commutative algebra*. 2:a upplagan. New York: Springer.

Dieudonné, Jean Alexandre (1974). *Cours de géométrie algébrique. 1, Aperçu historique sur le développement de la géométrie algébrique*. Paris: Presses Universitaires de France

Eisenbud, David & Harris, Joe (2000). *The Geometry of Schemes*. New York: Springer Verlag.

Grillet, Pierre Antoine (2007). *Abstract Algebra*. 2:a Upplagan. New York: Springer Business + Media, LLC.

Kline, Morris (1960). Projektiv geometri. I Newman, James Roy (red.), *Sigma: en matematikens kulturhistoria. Bd. 4.* Stockholm: Forum. S. 1507-1527.

Liddell, Henry George & Scott, Robert (1996). *A Greek-English lexicon.* Nionde upplagan. Oxford: Oxford Univ. Press

Panofsky, Erwin (1960). Dürer som matematiker. I Newman, James Roy (red.), *Sigma: en matematikens kulturhistoria. Bd. 4.* Stockholm: Forum. S. 1486-1506.

Passow, Franz (1841-1841). *Grekiskt och svenskt lexicon.* Örebro:[28]

Perrin, Daniel (1995). *Géométrie algébrique, Une introduction*. Paris: InterEditions.

Svensson Per-Anders (2010). *Abstrakt Algebra*. Andra tryckningen. Studentlitteratur: Lund.

[28]Det rör sig om en svensk översättning av ett grekiskt-tyskt lexikon från 1800-talet. Översättningen, vars fullständiga namn är *Grekiskt och svenskt lexicon af Franz Passow. / Öfversättning af G. W. Gumœlius.* gavs ut i två volymer, A-K och Λ-Ω, båda tryckta 1841. Det är alltså en fullständig källhänvisning det rör sig om trots det lite udda formatet.