Algebraische Kurven - Vorlesung 4

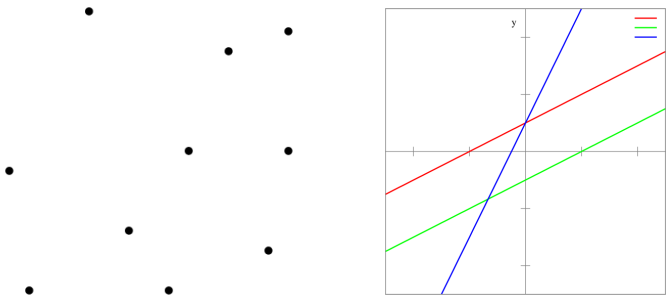
Irreduzible affin-algebraische Mengen

Definition 1. Eine affin-algebraische Menge $V \subseteq \mathbb{A}^n_K$ heißt *irreduzibel*, wenn $V \neq \emptyset$ ist und es keine Zerlegung $V = Y \cup Z$ mit affin-algebraischen Mengen $Y, Z \subset V$ gibt.

Die Zariski-abgeschlossene Menge V ist also irreduzibel genau dann, wenn $V \neq \emptyset$ ist und eine Zerlegung $V = Y \cup Z$ nur möglich ist mit $V = Y$ oder mit $V = Z$. Dasselbe folgt dann sofort für endliche Darstellungen.

Die Irreduzibilität ist eine rein topologische Eigenschaft, wobei man obige Definition mit abgeschlossenen Mengen formulieren muss anstatt mit affin-algebraischen Mengen (den abgeschlossenen Mengen in der Zariski-Topologie).

Die folgenden Bilder zeigen einige nicht irreduzible affin-algebraische Teilmengen. Was sind dabei die irreduziblen Komponenten (siehe unten)?



Beispiel 2. Wir betrachten den affinen Raum $\mathbb{A}^n_K$. Wenn K endlich ist, so besteht der Raum nur aus endlich vielen Punkten und nur die einpunktigen Teilmengen sind irreduzibel. Insbeondere ist der affine Raum außer bei $n = 1$ nicht irreduzibel.

Bei unendlichem K ist der affine Raum $\mathbb{A}^n_K$ hingegen irreduzibel. Sei nämlich $\mathbb{A}^n_K = Y \cup Z$ mit echten affin-algebraischen Teilmengen. D.h. für die offenen Komplemente $U = A^n_K - Y$ und $W = A^n_K - Z$ ist einerseits $U, W \neq \emptyset$, aber $U \cap W = \emptyset$. Das widerspricht aber Aufgabe 3.8.

Lemma 3. *Sei $V \subseteq \mathbb{A}^n_K$ eine affin-algebraische Menge mit Verschwindungsideal $\mathrm{Id}\,(V)$. Dann ist V irreduzibel genau dann, wenn $\mathrm{Id}\,(V)$ ein Primideal ist.*

Beweis. Sei $\mathrm{Id}\,(V)$ kein Primideal. Dann gibt es Polynome $F, G \in K[X_1, \ldots, X_n]$ mit $FG \in \mathrm{Id}\,(V)$, aber $F, G \notin \mathrm{Id}\,(V)$. Dies bedeutet, dass es Punkte $P, Q \in V$ gibt mit $F(P) \neq 0$ und $G(Q) \neq 0$. Wir betrachten die

beiden Ideale $\mathfrak{a}_1 = \mathrm{Id}\,(V) + (F)$ und $\mathfrak{a}_2 = \mathrm{Id}\,(V) + (G)$. Wegen $P \in V(\mathfrak{a}_1)$ und $Q \in V(\mathfrak{a}_2)$ ist $V(\mathfrak{a}_1), V(\mathfrak{a}_2) \subset V$. Andererseits ist

$$V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) = V(\mathfrak{a}_1 \cdot \mathfrak{a}_2) = V(\mathrm{Id}\,(V)) = V\,,$$

so dass eine nicht-triviale Zerlegung von V vorliegt und somit V nicht irreduzibel ist.

Sei nun V nicht irreduzibel, mit der nicht-trivialen Zerlegung $V = Y \cup Z$. Sei $Y = V(\mathfrak{a}_1)$ und $Z = V(\mathfrak{a}_2)$. Wegen $Y \subset V$ gibt es $F \in \mathfrak{a}_1$, $F \notin \mathrm{Id}\,(V)$. Ebenso gibt es $G \in \mathfrak{a}_2$, $G \notin \mathrm{Id}\,(V)$. Für $P \in V = Y \cup Z$ ist $(FG)(P) = 0$, da F auf Y und G auf Z verschwindet. Also ist $FG \in \mathrm{Id}\,(V)$ und daher ist $\mathrm{Id}\,(V)$ kein Primideal. □

Definition 4. Sei V eine affin-algebraische Menge. Eine affin-algebraische Teilmenge $W \subseteq V$ heißt eine *irreduzible Komponente* von V, wenn sie irreduzibel ist und wenn es keine irreduzible Teilmenge $W \subset W' \subseteq V$ gibt.

Ist V irreduzibel, so ist V selbst die einzige irreduzible Komponente von V. Wir werden später sehen, dass jede affin-algebraische Menge sich schreiben lässt als eine endliche Vereinigung von irreduziblen Komponenten.

Beispiel 5. Wir betrachten die Gleichung

$$F = Y^2 + X^2(X+1)^2 = 0\,.$$

In den reellen Zahlen hat diese Gleichung zwei Lösungen: da ein reelles Quadrat nie negativ ist, kann F nur dann 0 sein, wenn beide Summanden null sind, und das impliziert einerseits $Y = 0$ und andererseits $X = 0$ oder $X = -1$. Insbesondere ist die reelle Lösungsmenge nicht zusammenhängend und nicht irreduzibel (und das Verschwindungsideal zur reellen Situation ist sehr groß).

Betrachtet man F dagegen über den komplexen Zahlen, so gibt es eine Faktorisierung

$$F = (Y + iX(X+1))(Y - iX(X+1))$$

in irreduzible Polynome. Dies zeigt zugleich, dass F als Polynom in $\mathbb{R}[X,Y]$ irreduzibel ist (obwohl das reelle Nullstellengebilde nicht irreduzibel ist). Die Nullstellenmenge über den komplexen Zahlen besteht aus den beiden Graphen $Y = \pm iX(X+1)$, die sich in $(0,0)$ und $(-1,0)$ schneiden.

Bei der Gleichung $Y^2 + Z^2 + X^2(X+1)^2$ gibt es wieder nur zwei reelle Lösungspunkte, das Polynom ist aber sowohl reell als auch komplex betrachtet irreduzibel.

Beispiel 6. Wir betrachten im affinen Raum $\mathbb{A}^3_K$ ($K = \mathbb{R}$) die beiden *Zylinder*

$$S_1 = \{(x,y,z) :\, x^2 + y^2 = 1\} \text{ und } S_2 = \{(x,y,z) :\, y^2 + z^2 = 1\}\,.$$

Das sind beides irreduzible Mengen, wie wir später sehen werden (für K unendlich). Wie sieht ihr Durchschnitt aus? Der Durchschnitt wird beschrieben durch das Ideal $\mathfrak{a}$, das durch X^2+Y^2-1 und Y^2+Z^2-1 erzeugt wird. Zieht man die eine Gleichung von der anderen ab, so erhält man

$$X^2-Z^2=(X-Z)(X+Z)\in\mathfrak{a}\,.$$

Die beiden einzelnen Faktoren gehören aber nicht zu $\mathfrak{a}$, da bspw. $(1,0,-1)$ ein Punkt des Schnittes ist, an dem $X-Z$ nicht verschwindet (Charakteristik $\neq 2$), und $(1,0,1)$ ein Punkt des Schnittes ist, an dem $X+Z$ nicht verschwindet. Die Komponenten des Schnittes werden vielmehr beschrieben durch

$$\mathfrak{b}_1=\mathfrak{a}+(X-Z) \text{ und } \mathfrak{b}_2=\mathfrak{a}+(X+Z)\,.$$

Das sind beides Primideale, der Restklassenring ist

$$K[X,Y,Z]/(\mathfrak{b}_1)=K[X,Y,Z]/(\mathfrak{a}+(X-Z))\cong K[X,Y](X^2+Y^2-1)\,.$$

Um dies zu sehen, eliminiert man Z mit der hinteren Gleichung, und die beiden Zylindergleichungen werden dann identisch. Ebenso ist die Argumentation für das andere Ideal. Geometrisch gesprochen heißt dies, dass ein Punkt des Durchschnittes $S_1\cap S_2$ in der Ebene $E_1=V(Z-X)$ oder in der Ebene $E_2=V(Z+X)$ liegt. Es ist

$$E_1\cap S_1=E_1\cap S_1\cap S_2=E_1\cap S_2$$

und ebenso für E_1, da auf diesen Ebenen die beiden Zylindergleichungen identisch werden.

Wie sehen die Durchschnitte in den Ebenen aus? Wir betrachten die Ebene E_1 mit den Koordinaten Y und $U=Z+X$. Es ist dann $X=\frac{1}{2}((Z+X)-(Z-X))$ und damit kann man die erste Zylindergleichung als

$$\Big(\frac{1}{2}((Z+X)-(Z-X))\Big)^2+Y^2=1$$

schreiben. Auf der Ebene E_1, die ja durch $Z=X$ festgelegt ist, wird aus dieser Gleichung

$$(\frac{1}{2}U)^2+Y^2=1\,,$$

also $\frac{1}{4}U^2+Y^2=1$. Dies ist die Gleichung einer *Ellipse*, was auch anschaulich klar ist. Man beachte, dass in der obigen Berechnung des Restklassenringes $K[X,Y,Z]/(\mathfrak{b}_1)$ aber eine Kreisgleichung auftritt. Dies sollte deshalb nicht überaschen, da Kreis und Ellipse durch eine lineare Variablentransformation

ineinander überführbar sind und dass daher insbesondere die Restklassenringe isomorph sind. Als „metrisches Gebilde“ sind Kreis und Ellipse verschieden, und der Durchschnitt der beiden Zylinder besteht aus zwei Ellipsen. Bei einer *orthonormalen Variablentransformation* bleibt die metrische Struktur erhalten. Die Variablen $Y, X+Z, X-Z$ definieren eine orthogonale Transformation, so dass zumindest die Winkel und Formen erhalten bleiben, obwohl die Längen sich ändern.

Halten wir also fest: Der Durchschnitt der beiden Zylinder ist

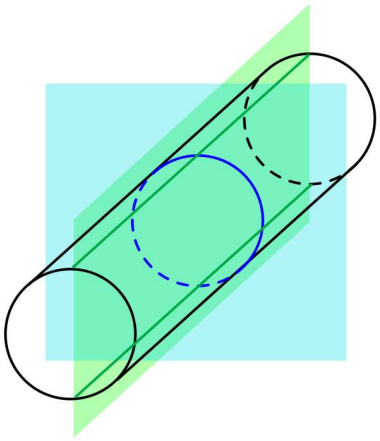
$$S_1 \cap S_2 = V(\mathfrak{b}_1) \cup V(\mathfrak{b}_2)\,,$$

wobei $\mathfrak{b}_1 = (X^2+Y^2-1, X-Z)$ und $\mathfrak{b}_2 = (X^2+Y^2-1, X+Z)$ zwei Ellipsen beschreiben.

Wie liegen diese beiden Ellipsen zueinander? Dazu berechnen wir ihren Durchschnitt, der durch die Summe von $\mathfrak{b}_1$ und $\mathfrak{b}_2$ beschrieben wird. Es ist

$$\mathfrak{b}_1 + \mathfrak{b}_2 = (X^2 + Y^2 - 1, X - Z, X + Z) = (Y^2 - 1, X, Z)\,.$$

Die Lösungsmenge davon besteht aus den beiden Punkten $(0, 1, 0)$ und $(0, -1, 0)$.



Zur Anzahl der Punkte auf Kurven

Wir haben bereits gesehen, dass der Schnitt einer Kurven mit einer Geraden nur aus endlich vielen Punkte besteht, es sei denn die Gerade sei selbst eine Komponente der Kurve (siehe Lemma 1.3. Dies wollen wir zunächst auf den Schnitt von zwei beliebigen ebenen Kurven verallgemeinern. Als Hilfsmittel benötigen wir die folgende Definition.

Definition 7. Sei K ein Körper und $K[X]$ der Polynomring in einer Variablen über K. Dann nennt man den Quotientenkörper $Q(K[X])$ den *rationalen Funktionenkörper* über K (oder *Körper der rationalen Funktionen über* K). Er wird mit $K(X)$ bezeichnet.

Satz 8. *(Schnitt von ebenen Kurven) Sei K ein Körper und seien $F, G \in K[X,Y]$ zwei Polynome ohne gemeinsamen nichtkonstanten Faktor. Dann gibt es nur endlich viele Punkte $P_1, \ldots, P_n$ mit $P_i \in V(F,G)$.*

Beweis. Wir betrachten $F, G \in K[X,Y]$ als Elemente in $K(X)[Y]$, wobei $K(X)$ den Körper der rationalen Funktionen in X bezeichne. Es haben dann nach Aufgabe 4.8 auch F und G keinen gemeinsamen Teiler in $K(X)[Y]$. Da dieser Ring ein Hauptidealbereich ist, erzeugen sie zusammen das Einheitsideal, d.h. es gibt Polynome $A, B \in K(X)[Y]$ mit $AF + BG = 1$. Multiplikation mit dem Hauptnenner von A und B ergibt in $K[X,Y]$ die Gleichung $\tilde{A}F + \tilde{B}G = H$ mit $H \in K[X]$. Eine gemeinsame Nullstelle in $\mathbb{A}^2_K$ von F und von G muss also eine Nullstelle von H sein. Es gibt also nur endlich viele Werte für X, für die eine gemeinsame Nullstelle vorliegt. Wenn man die Rollen von X und von Y vertauscht, so sieht man, dass es auch nur endlich viele Werte für Y gibt, an denen eine gemeinsame Nullstelle vorliegen kann. Damit kann es überhaupt nur endlich viele gemeinsame Nullstellen geben. □