Einige weitere Sätze über ebene Kurven

In dieser Vorlesung sei k ein beliebiger Körper. Die folgenden Sätze werden für das Verständnis elliptischer Kurven nützlich sein.

Satz: C und C' seien Kurven in $\mathbb{P}^2(k)$ vom Grad d, die sich in genau d^2 verschiedenen Punkten schneiden. Wenn genau de dieser Punkte auf einer irreduziblen Kurve C'' vom Grad e liegen, liegen die restlichen $d(d-e)$ auf einer (nicht notwendigerweise irreduziblen) Kurve vom Grad $d-e$.

Beweis: F und G seien homogene Polynom vom Grad d aus $k[X,Y,Z]$ mit $C = V(F)$ und $C' = V(G)$. Wir betrachten das Büschel $\mathcal{L}$ der Kurven (besser *Divisoren*) mit den Gleichungen

$$\lambda F(x,y,z) + \mu G(x,y,z) = 0 \qquad \text{mit} \qquad (\lambda : \mu) \in \mathbb{P}^1(k)\,.$$

Da F und G in allen Schnittpunkten von C und C' verschwinden, liegen die d^2 Schnittpunkte auf jedem der Divisoren aus $\mathcal{L}$. Für einen Punkt $Q = (x_0 : y_0 : z_0)$ aus $\mathbb{P}^2(k)$, der nicht auf C liegt, ist $F(x_0,y_0,z_0) \neq 0$; wir können daher einen Punkt $(\lambda : \mu) \in \mathbb{P}^1(k)$ finden, so daß $\lambda F(x_0,y_0,z_0) + \mu G(x_0,y_0,z_0)$ verschwindet, d.h. der Punkt Q liegt auf der Kurve $\widetilde{C} = V(\lambda F + \mu G)$ aus $\mathcal{L}$. Wir betrachten eine solche Kurve $\widetilde{C}$ speziell für einen Punkt Q, der zwar nicht auf C liegt, aber auf C''.

Da jeder Divisor aus $\mathcal{L}$ alle Schnittpunkte von C und C' enthält, schneiden sich $\widetilde{C}$ und C'' in den de Schnittpunkten von C und C'', außerdem haben sie noch den Punkt Q gemeinsam, der nicht auf C liegt, also keiner dieser de Punkte sein kann. Somit haben $\widetilde{C}$ und C'' mindestens $de + 1$ Punkte gemeinsam. $\widetilde{C}$ hat, wie jede Kurve aus $\mathcal{L}$, den Grad d, und C'' hat nach Voraussetzung den Grad $e < d$. Falls die beiden Kurven keine gemeinsame Komponente haben, kann es nach dem Satz von BÉZOUT höchstens de Schnittpunkte geben. Also haben die beiden eine gemeinsame Komponente, und wegen der Irreduzibilität von C'' kann das nur C'' selbst sein. C'' ist also eine Komponente von $\widetilde{C}$, das sich deshalb schreiben läßt als Vereinigung von C'' mit einer (nicht notwendigerweise irreduziblen) Kurve C''' vom Grad $d-e$. Da alle d^2

Schnittpunkte von C und C' auf $\widetilde{C}$ liegen und genau de davon auf C'', liegen die restlichen $d(d-e)$ auf C'''.

■

Zwei Kurven vom Grad drei schneiden sich nach dem Satz von BÉZOUT in höchstens neun Punkten; falls der Grundkörper algebraische abgeschlossen ist, sind es mit Vielfachheiten gezählt genau neun. Der folgende Satz besagt, daß im Falle von neun verschiedenen Schnittpunkte diese Punkte nicht beliebig in der projektiven Ebene liegen, sondern daß durch je acht dieser Punkte der neunte eindeutig festgelegt ist:

Satz: $E = V(F)$ und $E' = V(G)$ seien zwei Kurven vom Grad drei in der projektiven Ebenen, die sich in genau neun verschiedenen Punkten schneiden, und $\mathcal{L}$ sei das von E und E' erzeugte Büschel kubischer Kurven, d.h. also die Kurven

$$V(\lambda F + \mu G) \qquad \text{mit} \qquad (\lambda : \mu) \in \mathbb{P}^1(k)\,.$$

Sind dann $P_1, \ldots P_8$ irgendwelche acht der neun Schnittpunkte, so geht jede kubische Kurve durch $P_1, \ldots P_8$ auch durch den neunten Schnittpunkt P_9. Das lineare System $\mathcal{L}'$ aller kubischer Kurven durch $P_1, \ldots P_8$ ist gleich dem von E und E' erzeugten Büschel $\mathcal{L}$.

Beweis: Wir zeigen zunächst einige geometrische Eigenschaften der Menge der neun Schnittpunkte:

1. Keine vier der Punkte $P_1, \ldots, P_9$ liegen auf einer Geraden: Angenommen, die Gerade g enthalte vier der Punkte P_i. Dann haben E und g mindestens vier gemeinsame Punkte, was nach dem Satz von BÉZOUT nur möglich ist, wenn g eine Komponente von E ist. Entsprechend müßte g auch eine Komponente von E' sein, die beiden Kurven hätten also eine gemeinsame Komponente. Da sie nach Voraussetzung nur neun Punkte gemeinsam haben, ist das nicht möglich.

2. Keine sieben der Punkte $P_1, \ldots, P_9$ liegen auf einer Quadrik: Hier können wir genauso argumentieren: Eine Quadrik, also eine Kurve vom Grad zwei, hat mit einer kubischen Kurve nach BÉZOUT höchstens sechs Schnittpunkte – es sei denn, die beiden Kurven haben eine gemeinsame

Komponente. Im Falle einer irreduziblen Quadrik müßte das Q sein, d.h. Q wäre eine gemeinsame Komponente von E und E'. Eine nicht irreduzible Quadrik zerfällt in zwei Geraden, und bei sieben Schnittpunkten müßte mindestens eine der beiden vier oder mehr dieser Punkte enthalten, was wir bereits ausgeschlossen haben.

3. Durch je fünf der neun Schnittpunkte geht genau eine Quadrik: Eine Quadrik in $\mathbb{P}^2(k)$ ist gegeben als Nullstellenmenge eines homogenen quadratischen Polynoms

$$aX^2 + bXY + cXZ + dY^2 + eYZ + fZ^2 ;$$

da dieses sechs Koeffizienten hat, ist das lineare System aller Quadriken in $\mathbb{P}^2(k)$ fünfdimensional, Somit gibt es durch je fünf Punkte der projektiven Ebenen stets mindestens eine Quadrik, denn wenn wir die Koordinaten der Punkte in die Gleichung der Quadrik einsetzen, erhalten wir ein homogenes lineares Gleichungssystem aus fünf Gleichungen für die sechs Koeffizienten a, b, c, d, e, f.

Angenommen, fünf der P_i liegen auf zwei verschiedenen Quadrikens Q und Q'. Da zwei Quadriken ohne gemeinsame Komponente nach BÉZOUT höchstens vier Schnittpunkte haben können, müßten Q und Q' eine gemeinsame Komponente haben; diese könnte, da die beiden Quadriken verschieden sind, nur eine Gerade g sein. Es gäbe daher zwei verschiedene Geraden h und h', so daß $Q = g \cup h$ und $Q' = g \cup h'$ ist. Nach der ersten Aussage in diesem Beweis können auf g höchstens drei der P_i liegen, also lägen mindestens zwei der P_i sowohl auf h als auch auf h'. Das geht aber nur, wenn $h = h'$ und damit $Q = Q'$ ist.

4. Wäre $\mathcal{L} \neq \mathcal{L}'$ so wären keine drei der P_i kollinear: Natürlich ist $\mathcal{L} \subseteq \mathcal{L}'$, denn jeder Divisor aus $\mathcal{L}$ enthält alle neun Schnittpunkte und damit auch jede Teilmenge davon. Da $\mathcal{L}$ eindimensional ist, müßte $\mathcal{L}'$ daher im Fall $\mathcal{L} \neq \mathcal{L}'$ mindestens die Dimension zwei haben.

Angenommen, dies ist der Fall, und drei der P_i sind kollinear; o.B.d.A seien dies die Punkte P_1, P_2, P_3, und g sei die Gerade, auf der sie liegen. Wegen Aussage *3.* liegen die fünf Punkte P_4, P_5, P_6, P_7, P_8 auf genau einer Quadrik Q. $P \in g$ sei verschieden von P_1, P_2, P_3, und P' sei ein Punkt, der weder auf g noch auf Q liegt. Da dim $\mathcal{L}' \geq 2$ ist, gibt es

eine Kurve $\widehat{C} \in \mathcal{L}'$, die durch P und P' geht. Da $\widehat{C}$ als Kurve aus $\mathcal{L}'$ durch die Punkte $P_1, \ldots, P_8$ geht und g durch P_1, P_2, P_3, besteht $\widehat{C} \cap g$ mindestens aus den vier Punkten P_1, P_2, P_3 und P. Nun ist aber $\widehat{C}$ eine kubische Kurve und g eine Gerade; nach BÉZOUT kann es also nur dann mehr als drei Schnittpunkte geben, wenn g eine Komponente von $\widehat{E}$ ist. Somit ist $\widehat{E}$ die Vereinigung von g mit einer (nicht notwendigerweise irreduziblen) Quadrik Q'.

Die fünf Punkte $P_4, \ldots, P_8$ liegen auf $\widehat{C}$, können aber wegen Aussage *1.* nicht auf g liegen, da g bereits P_1, P_2 und P_3 enthält. Somit liegen sie auf Q', und da es nach *3.* durch fünf Schnittpunkte genau eine Quadrik gibt, ist $Q' = Q$ und damit $\widehat{E} = g \cup Q$. Das ist aber nicht möglich, denn P' ist ein Punkt von $\widehat{E}$, der weder auf Q noch auf g liegt. Damit ist klar, daß im Falle $\mathcal{L} \neq \mathcal{L}'$ keine drei der neun Schnittpunkte auf einer Geraden liegen können.

5. Falls $\mathcal{L} \neq \mathcal{L}'$ist, liegen keine sechs der P_i auf einer Quadrik: Angenommen $P_1, \ldots P_6$ liegen auf einer Quadrik Q. Wäre diese reduzibel, wäre sie Vereinigung zweier Geraden, von denen mindestens eine mindestens drei dieser Punkte enthalten müßte. Wie wir gerade gesehen haben, ist das nicht möglich, also muß Q irreduzibel sein.

g sei die Gerade durch P_7 und P_8. Wir wählen einen Punkte $P \in Q$, der nicht in $\{P_1, \ldots P_6\}$ liegt, sowie einen Punkt P', der weder auf Q noch auf g liegt. Da $\mathcal{L}'$ nach Voraussetzung von $\mathcal{L}$ verschieden ist und somit mindestens zweidimensional, gibt es eine Kurve $\widehat{C} \in \mathcal{L}'$, die durch P und P' geht. Als Element von $\mathcal{L}'$ enthält $\widehat{C}$ insbesondere die Punkte $P_1, \ldots P_8$; die Schnittmenge mit Q enthält also mindestens die sieben Punkte $P_1, \ldots, P_6$ und P. Wieder folgt aus dem Satz von BÉZOUT, daß $\widehat{E}$ und Q eine gemeinsame Komponente haben müssen, was wegen der Irreduzibilität von Q bedeutet, daß $Q \subset \widehat{E}$ ist. Die zweite Komponente muß aus Gradgründen eine Gerade sein, und auf dieser Geraden müssen die Punkte P_7 und P_8 liegen, denn sie liegen auf $\widehat{E}$, können aber wegen *2.* nicht auf Q liegen. Somit ist diese Gerade gleich g, d.h. $\widehat{E} = Q \cup g$. Das kann aber nicht sein, denn $P' \in \widehat{E}$ liegt weder auf g noch auf Q.

Nach diesen Vorbereitungen können wir nun beweisen, daß $\mathcal{L} = \mathcal{L}'$ ist:

Angenommen, dies wäre nicht der Fall. Wir betrachten die Gerade g durch P_1 und P_2 und wählen darauf zwei weitere Punkte P_1' und P_2'. Da $\mathcal{L}'$ nach unserer Annahme mindestens zweidimensional ist, gibt es eine Kurve $\widehat{E} \in \mathcal{L}'$, die durch P_1' und P_2' geht. Sie schneidet g mindestens in den vier Punkten P_1, P_2, P_1' und P_2', was für eine kubische Kurve nach BÉZOUT nur dann möglich ist, wenn g eine Komponente von $\widehat{E}$ ist. Somit ist $\widehat{E} = g \cup Q$ mit einer Quadrik Q. Da g wegen *4.* keinen der Punkte $P_3, \ldots, P_8$ enthalten kann, müssen diese sechs Punkte auf Q liegen, denn jede Kurve aus $\mathcal{L}'$ geht ja durch $P_1, \ldots, P_8$. Das widerspricht aber der Aussage *5.*

Somit ist $\mathcal{L}' = \mathcal{L}$, d.h. jede kubische Kurve, die durch acht der neun Schnittpunkte von E und E' geht, liegt im von E und E' erzeugten Büschel und geht daher auch durch den neunten Schnittpunkt. ∎