Prof. Dr. Daniel Plaumann
M. Sc. Dimitri Manevich
Sommersemester 2017/2018

technische universität dortmund

ÜBUNGEN ZUR ALGEBRAISCHEN GEOMETRIE I

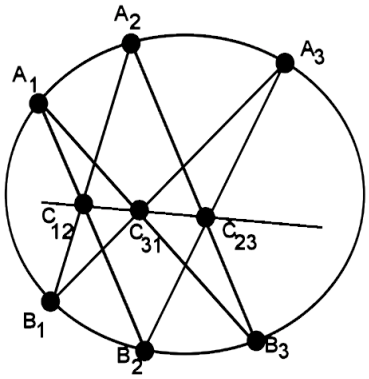
Blatt 23
Abgabe bis Dienstag, 3. Juli, 12:00 Uhr in Briefkasten 11

Lektüre: Lesen Sie Kapitel 18 über den Satz von Cayley-Bacharach zu Ende.

51. Verwenden Sie den Satz von Cayley-Bacharach, um den Satz von Pascal erneut zu beweisen (vgl. Aufgabe 38). Gegeben eine irreduzible Konik Q in $\mathbb{P}^2$ und sechs Punkte $a_1, a_2, a_3, b_1, b_2, b_3 \in Q$, dann sind die Punkte

$$c_{12} = \overline{a_1 b_2} \cap \overline{a_2 b_1}, \quad c_{13} = \overline{a_1 b_3} \cap \overline{a_3 b_1}, \quad c_{23} = \overline{a_2 b_3} \cap \overline{a_3 b_2}$$

kollinear.



Bildquelle: https://terrytao.wordpress.com

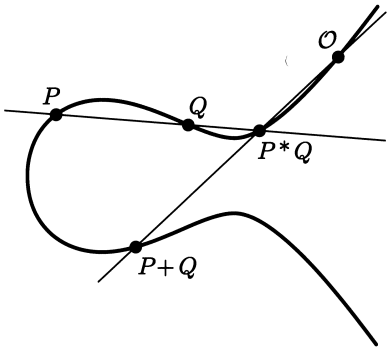
52. In dieser Aufgabe konstruieren wir die *Gruppenstruktur auf einer elliptischen Kurve*.

Es sei C eine glatte (insbesondere irreduzible) kubische Kurve in $\mathbb{P}^2$. Gegeben Punkte $p, q \in C$, sei $L_{p,q}$ die Verbindungsgerade $\overline{pq}$, falls $p \neq q$ und $L_{p,p}$ die Tangente an C im Punkt p. Dann schneidet $L_{p,q}$ die Kurve C in p, q und einem weiteren Punkt, den wir mit $p * q$ bezeichnen.

Angenommen $\mathcal{O}$ ist ein Wendepunkt von C, was bedeutet, dass die Tangente $L_{\mathcal{O},\mathcal{O}}$ die Kurve C nur in $\mathcal{O}$ schneidet (mit Vielfachheit 3). Dann gilt also $\mathcal{O} * \mathcal{O} = \mathcal{O}$. Definiere nun

$$p + q = (p * q) * \mathcal{O}$$

für $p, q \in C$.



Bildquelle: Silverman, Tate: Rational Points on Elliptic Curves, Fig. 1.6

Zeigen Sie, dass $(C, +)$ eine abelsche Gruppe mit neutralem Element $\mathcal{O}$ ist, indem Sie die folgenden Aussagen für alle $p, q, r \in C$ beweisen:

(a) $p + q = q + p$;
(b) $\mathcal{O} + p = p + \mathcal{O} = p$;
(c) Zu $p \in C$ gibt es $-p \in C$ mit $(-p) + p = p + (-p) = \mathcal{O}$;
(d) $(p + q) + r = p + (q + r)$.

Hinweis zu (d): Nehmen Sie an, dass die neun Punkte

$$p,\ q,\ r,\ \mathcal{O},\ p * q,\ p + q,\ q * r,\ q + r,\ (p + q) * r$$

alle verschieden sind. Verwenden Sie nun den Satz von Cayley-Bacharach.

Bemerkung. Wir haben nicht gezeigt, dass jede glatte Kubik einen Wendepunkt besitzt. Angenommen C ist durch eine Gleichung der Form

$$y^2z = ax^3 + bx^2z + cxz^2 + dz^3$$

gegeben (*Weierstraß-Normalform*). Dann ist $[0, 1, 0]$ ein Wendepunkt.