Rational points on elliptic curves

Weierstrass Normal Form

- Warum
  - einfachere Beweise
  - weniger freie Variablen
- Was
  - Nimmt eine kubische Kurve C zu einem Polynom $P \in \mathbb{Q}[x, y]$ von Totalgrad drei rein und gibt eine einfachere Version aus
  - $P = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j$
  - klassische WNF $C : P = 0 \to C' : y^2 = 4x^3 - g_2x - g_1$
  - allgemeinere WNF $C : P = 0 \to C' : y^2 = x^3 + a'x^2 + b'x + c'$
- Wie
  - $C \subset \mathbb{PR}^2$ ein kubische Kurve in projektiver Ebene
    - Angenommen $\mathcal{O} \in C$ rationaler Punkt
  - PLAN: Wähle Achsen von $\mathbb{PR}^2$ so, dass wir WNF erhalten
    - Achsentransformationen sind Achsen Transformationen $Av + b$ mit A linear und $b \in \mathbb{PR}^2$
  - Bestimmen der neuen Achsen
    1. $Z = 0$ als Tangente an $\mathcal{O}$ wählen
    2. Z schneidet C an einem weiteren Punkt. (siehe Seminar Daniel) Tangente hier ist $X = 0$
       - Wenn $\mathcal{O}$ ein Wendepunkt ist, kann $X = 0$ beliebige Gerade sein, welche nicht $\mathcal{O}$ beinhaltet
    3. Wähle $Y = 0$ eine beliebige andere Gerade durch $\mathcal{O}$
  - Liefern neue Achsen (erreichbar durch Achsen Transformationen) WNF?
    - $\mathbb{PR}^2 \supset C : aX^3+bX^2Y+cXY^2+dY^3+eX^2Z+fXYZ+gY^2Z+hXZ^2+iYZ^2+jZ^3 = 0$
    - $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$
    - $\mathbb{AR}^2 \supset C' : ax^3+bx^2y+cxy^2+dy^3+ex^2+fxy+gy^2+hx+iy+j = 0$
- Beispiel 1: $u^3 + v^3 = \alpha$
  1. Projektivieren: $U^3 + V^3 = \alpha W^3$ mit $\mathcal{O} = (1 : -1 : 0)$
     - $1^3 + (-1)^3 = 0 \cdot \alpha$
     - $\mathcal{O}$ ist ein Wendepunkt, somit $X = 0$ beliebige Gerade, die nicht durch $\mathcal{O}$ geht
  2. Wähle $Z = 0$ als Tangente am Punkt $\mathcal{O}$
  3. Wähle $Y = 0$ als weitere Gerade durch $\mathcal{O}$
  4. $x = \frac{X}{Z} = \frac{12\alpha}{u+v}$, $y = \frac{Y}{Z} = 36\alpha\frac{u-v}{u+v}$
  5. $y^2 = x^3 - 432\alpha$

Birationale Transformationen erhalten Gruppenstruktur

Aufgrund der Achsen Transformationen, welche injektiv sind, gibt es eine *1:1 Korrespondenz* der rationalen Punkte auf der einen Kurve und der anderen.

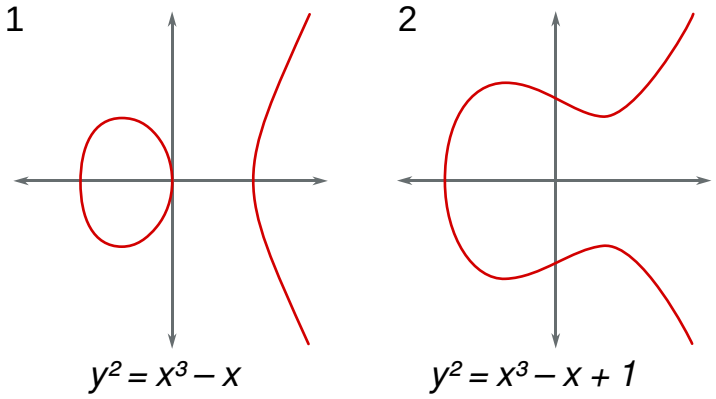
Auch wenn gerade Linien durch Achsentransformationen nicht erhalten bleiben, ist Achsentransformationen ein Gruppenhomomorphismus zwischen den Gruppen auf den jeweiligen Kurven. (nicht trivial: *Additionsgesetz ist invariant unter birationaler transformation*)

Geschichte hinter dem Namen der "Elliptische Kurve"

- Wenn g birational äquivalent zu einer elliptischen Kurve ist, so wird auch g als elliptische Kurve gesehen
- Elliptische Kurve ist keine Ellipse
  - Wenn h eine Ellipse ist und man möchte die Länge herausfinden, so muss man ein Integral mit $y = \sqrt{f(x)}$ lösen
  - daher "elliptische Kurve" für $y^2 = f(x)$

Komponenten

- Elliptische Kurve $y^2 = f(x) = x^3 + ax^2 + bx + c, \quad a, b, c, \in \mathbb{Q}$
  - f hat mindestens eine reelle Komponente
    - Weil alle Koeffizienten a, b, c von f rational, also rell sind, muss es mindestens eine relle Wurzel geben



    -
    - links, zwei Komponenten
      - drei reelle Wurzeln für f
    - rechts eine Komponente
      - eine reelle Wurzel für f

Explicit Formulas For The Group Law