Vorlesung „Algebraische Kurven“ (Sommersemester 2021)

Übungsblatt 14 (16.7.2021)

Aufgabe 66: Sei C eine Kurve vom Geschlecht 1 und $D_1, D_2 \in \mathrm{Div}(C)$.

(1) Zeige die Implikation:

$$\mathrm{grad}(D_1) \geq 2 \quad \text{und} \quad \mathcal{L}(D_1) = \mathcal{L}(D_2) \quad \Longrightarrow \quad D_1 = D_2.$$

(2) Zeige an Hand eines Beispiels:

$$\mathcal{L}(D_1) = \mathcal{L}(D_2) \quad \not\Longrightarrow \quad D_1 = D_2.$$

Aufgabe 67: Eine hyperelliptische Kurve C vom Geschlecht $g \geq 2$ werde über einem Körper K der Charakteristik $\neq 2$ definiert durch eine Gleichung

$$y^2 = f(x) \text{ mit } f(x) = a_0 x^{2g+2} + a_1 x^{2g+1} + \cdots + a_{2g+1} x + a_{2g+2},$$

wo $f(x)$ ein separables Polynom vom Grad $2g+2$ ist. C besitzt 2 zwei Punkte im Unendlichen, die mit ∞_1 und ∞_2 bezeichnet werden, und für die $\mathrm{ord}_{\infty_1}(x) = \mathrm{ord}_{\infty_2}(x) = -1$ gilt.
Zeige: Ist a_0 kein Quadrat in K, so gilt $\infty_1, \infty_2 \notin C(K)$.
Hinweis: Ist $P \in C(K)$, so gilt für alle $f \in \mathcal{O}_{C,P} \cap K(C)$ natürlich $f(P) \in K$.

Aufgabe 68: Gib Beispiele für hyperelliptische Kurven C vom Geschlecht 2 an, die über einem der folgenden Körper K definiert sind und keinen K-rationalen Punkt besitzen. Folgende Körper sollen betrachtet werden:

$$\mathbb{R}, \quad \mathbb{F}_3, \quad \mathbb{F}_5, \quad \mathbb{F}_7, \quad \mathbb{F}_{11}.$$

Aufgabe 69: Unter den Namen *Hasse-Weil Bound* [1] oder *Weil-Schranke* [2] ist folgende Abschätzung für die Anzahl der $\mathbb{F}_p$-rationalen Punkte einer über $\mathbb{F}_p$ definierten, absolut irreduziblen, nichtsingulären, projektiven Kurve vom Geschlecht g bekannt:

$$|\#C(\mathbb{F}_p) - (p+1)| \leq 2g\sqrt{p}.$$

Zeige mit Hilfe dieser Abschätzung folgende Aussagen:

(1) Jede über $\mathbb{F}_p$ definierte Kurve vom Geschlecht 1 hat mindestens einen $\mathbb{F}_p$ rationalen Punkt.
(2) Ist C eine über $\mathbb{F}_p$ definierte Kurve vom Geschlecht 2 mit $C(\mathbb{F}_p) = \emptyset$, so gilt $p \in \{2, 3, 5, 7, 11, 13\}$.

Aufgabe 70: Sei C eine über einem algebraisch abgeschlossenen Körper K mit von 2 verschiedener Charakteristik durch die Gleichung $y^2 = f(x)$ definierte hyperelliptische Kurve vom Geschlecht g, wobei $f(x) \in K[x]$ ein separables Polynom vom Grad $2g+1$ ist. Mit der *Mumford representation* erhält man eine Beschreibung der Divisorenklassengruppe $\mathrm{Pic}^0(C)$ durch eine Menge von Polynompaaren:

$$\mathrm{Pic}^0(C) = \{(a, b) : a, b \in K[x], a \text{ normiert}, \mathrm{grad}(b) < \mathrm{grad}(a) \leq g, a \mid f - b^2\}.$$

[1] J. W. P. Hirschfeld, G. Korchmaros, F. Torres. Algebraic Curves over a Finite Field. Princeton University Press, 2008. S.343, Theorem 9.18 (Hasse-Weil Bound)

[2] W. Lütkebohmert. Codierungstheorie. Vieweg, 2003. S.162, Satz 7.4.1 (Weil-Schranke)

Die Addition in $\mathrm{Pic}^0(C)$ wird dann durch den *Algorithmus von Cantor* beschrieben [3]:

Eingabe: $(a_1, b_1), (a_2, b_2) \in \mathrm{Pic}^0(C)$
Ausgabe: $(a, b) \in \mathrm{Pic}^0(C)$ mit $(a, b) = (a_1, b_1) + (a_2, b_2)$ in $\mathrm{Pic}^0(C)$

1: $d_1 \leftarrow \mathrm{ggT}(a_1, a_2)$ und e_1, e_2 mit $d_1 = e_1 a_1 + e_2 a_2$
2: $d \leftarrow \mathrm{ggT}(d_1, b_1 + b_2)$ und c_1, c_2 mit $d = c_1 d_1 + c_2(b_1 + b_2)$
3: $s_1 \leftarrow c_1 e_1$, $s_2 \leftarrow c_1 e_2$, $s_3 \leftarrow c_2$
4: $a \leftarrow \frac{a_1 a_2}{d^2}$, $b \leftarrow \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} \bmod a$
5: **while** $\mathrm{grad}(b) > g$ **do**
6: $\quad a \leftarrow \frac{f - b^2}{a}$
7: $\quad b \leftarrow (-b) \bmod a$
8: **end while**
9: Dividiere a durch den höchsten Koeffizienten, sodass a dann normiert ist
10: **return** (a, b)

Mit der angegebenen Identifikation ist $(1, 0)$ das neutrale Element in $\mathrm{Pic}^0(C)$.

(1) Zeige, dass $(a, b) + (a, -b) = (1, 0)$ gilt.
(2) Zeige, dass $2 \cdot (a, b) = (1, 0)$ genau dann gilt, wenn $b = 0$ gilt.
(3) Welche Elemente in $\mathrm{Pic}^0(C)$ haben die Gestalt $(a, 0)$?
(4) Beschreibe die Untergruppe der 2-Torsionselemente

$$A = \{(a, b) \in \mathrm{Pic}^0(C) : 2 \cdot (a, b) = (1, 0)\}$$

von $\mathrm{Pic}^0(C)$.
(5) Zeige folgende Isomorphie von Gruppen

$$A \simeq (\mathbb{Z}/2\mathbb{Z})^{2g},$$

und damit $\#A = 2^{2g}$.

[3] Henri Cohen, Gerhard Frey et al. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman & Hall/CRC, 2006. S.308, Algorithm 14.7