Prof. Dr. H. Brenner **Osnabrück WS 2021/2022**

Elliptische Kurven

Arbeitsblatt 23

Aufgaben

AUFGABE 23.1. Es sei R ein kommutativer Ring, der einen Körper der positiven Charakteristik $p = 0$ enthalte (dabei ist p eine Primzahl). Zeige, dass die Abbildung

$$R \longrightarrow R,\ f \longmapsto f^p,$$

ein Ringhomomorphismus ist, den man den *Frobeniushomomorphismus* nennt.

AUFGABE 23.2. Es sei R ein kommutativer Ring, der einen Körper der positiven Charakteristik $p > 0$ enthalte. Zeige, dass die e-te Hintereinanderschaltung des Frobeniushomomorphismus

$$F\colon\ R \longrightarrow R,\ f \longmapsto f^p,$$

durch $f \mapsto f^q$ mit $q = p^e$ gegeben ist.

AUFGABE 23.3. Es sei R ein kommutativer Ring, der einen Körper der positiven Charakteristik $p = 0$ enthalte, und es sei A eine R-Algebra. Zeige, dass ein kommutatives Diagramm

$$\begin{array}{ccc} R & \stackrel{F}{\longrightarrow} & R \\ \downarrow & & \downarrow \\ A & \stackrel{F}{\longrightarrow} & A \end{array}$$

vorliegt, wobei F den Frobeniushomomorphismus bezeichnet.

Die in der vorstehenden Aufgabe ausgedrückte Vertauschbarkeit des Frobenius bringt mit sich, dass der Frobenius im Allgemeinen kein Algebrahomomorphismus ist. Dies ist insbesondere wenn der Grundring ein Körper ist nicht immer das, was man möchte, da man bei vielen Fragen die Elemente des Körpers, die „Konstanten“ eindeutig interpretieren möchte. Wenn der Grundkörper der Körper mit p Elementen ist, so ist dies unproblematisch, da darauf der Frobenius die Identität ist. Bei einem algebraisch abgeschlossenen Grundkörper konkurrieren aber verschiedene Frobenius-Konzepte.

Aufgabe 23.4. Es sei K ein Körper der positiven Charakteristik p. Sei $F\colon K \to K$ der Frobeniushomomorphismus. Zeige, dass genau die Elemente aus $\mathbb{Z}/(p)$ invariant unter F sind.

Aufgabe 23.5. Bestimme die Matrix des Frobeniushomomorphismus

$$\Phi\colon \mathbb{F}_q \longrightarrow \mathbb{F}_q$$

bezüglich einer geeigneten $\mathbb{F}_p$-Basis von $\mathbb{F}_q$ für $p = 2$ und $q = 4$ bzw. $q = 8$.

Aufgabe 23.6. Es sei p eine Primzahl mit $p = 3 \mod 4$ und sei

$$\mathbb{Z}/(p) \subseteq \mathbb{Z}/(p)[\mathrm{i}] = \mathbb{Z}/(p)[X]/\left(X^2+1\right) = \mathbb{F}_{p^2}$$

die quadratische Körpererweiterung von $\mathbb{Z}/(p)$. Zeige, dass die Konjugation $\mathrm{i} \mapsto -\mathrm{i}$ mit dem Frobeniushomomorphismus $f \mapsto f^p$ übereinstimmt.

In den nächsten Aufgaben verwenden wir die folgende Definition.

Ein Körper K heißt *vollkommen*, wenn jedes irreduzible Polynom $P \in K[X]$ separabel ist.

Aufgabe 23.7. Es sei K ein vollkommener Körper und $K \subseteq L$ eine endliche Körpererweiterung. Zeige, dass $K \subseteq L$ eine separable Körpererweiterung ist.

Aufgabe 23.8. Zeige, dass jeder Körper der Charakteristik 0 vollkommen ist.

Aufgabe 23.9. Zeige, dass jeder algebraisch abgeschlossene Körper vollkommen ist.

Aufgabe 23.10. Zeige, dass ein endlicher Körper vollkommen ist.

Aufgabe 23.11.*

Es sei K ein Körper der Charakteristik p. Zeige, dass K genau dann vollkommen ist, wenn der Frobeniushomomorphismus auf K surjektiv ist.

Aufgabe 23.12. Zeige, dass der Körper $\mathbb{F}_p(X)$ der rationalen Funktionen nicht vollkommen ist.

Aufgabe 23.13. Es sei $K = \mathbb{Z}/(p)$, wir betrachten den Frobeniushomomorphismus

$$K[X] \longrightarrow K[X]$$

und dadurch $K[X]$ als $K[X]$-Modul. Beschreibe die folgenden Polynome F als $K[X]$-Linearkombination bezüglich der Basis $X^0, X^1, \ldots, X^{p-1}$.

(1) $p = 3$ und $F = 2 + 2X^1 + X^2$
(2) $p = 5$ und $F = X^5$.
(3) $p = 2$ und $F = X^3 + X^4 + X^9$.
(4) $p = 3$ und $F = 2X^2 + X^3 + X^5 + 2X^7$.

Es ist sinnvoll, ein eigenes Zeichen, etwa $\bullet$, für die Skalarmultiplikation einzuführen.

Aufgabe 23.14. Es sei E die durch eine kurze Weierstraßgleichung

$$Y^2 = X^3 + aX + b$$

gegebene elliptische Kurve über einem Körper $\mathbb{Z}/(p)$ und es sei $Q(E)$ der zugehörige Funktionenkörper. Bestimme eine $Q(E)$-Basis für den Frobeniushomomorphismus

$$F\colon\ Q(E) \longrightarrow Q(E).$$

Aufgabe 23.15. Es sei $K = \mathbb{Z}/(p)$, wir betrachten den Frobeniushomomorphismus

$$K[X_1, \ldots, X_n] \longrightarrow K[X_1, \ldots, X_n]$$

und dadurch $K[X_1, \ldots, X_n]$ als $K[X_1, \ldots, X_n]$-Modul. Bestimme eine Basis für diesen Modul.

Aufgabe 23.16. Es sei K ein endlicher Körper mit $q = p^e$ Elementen und sei A eine K-Algebra mit dem e-ten Frobeniushomomorphismus

$$F^e\colon\ A \longrightarrow A.$$

Es sei $K \subseteq L$ eine Körpererweiterung. Zeige, dass

$$F^e \otimes_K L\colon\ A \otimes \mathrm{Id}_L \longrightarrow A \otimes_K L$$

im Allgemeinen nicht der e-te Frobenius auf $A \otimes_K L$ ist.

Aufgabe 23.17. Es sei R ein kommutativer Ring der positiven Charakteristik $p > 0$. Zeige, dass die Spektrumsabbildung zum Frobeniushomomorphismus

$$R \longrightarrow R,\ f \longmapsto f^p,$$

eine Homöomorphie ist.

AUFGABE 23.18. Es sei E eine elliptische Kurve über dem endlichen Körper $K = \mathbb{F}_q$ mit $q = p^e$ Elementen und es sei

$$\Phi\colon\ E_{\overline{K}} \longrightarrow E_{\overline{K}}$$

der e-te $\overline{K}$-lineare Frobenius.

(1) Zeige, dass es zu jedem $r \in \mathbb{N}$ ein $s \in \mathbb{N}$ gibt mit

$$\operatorname{Tor}_r\left(E(\overline{K})\right) \subseteq \operatorname{kern}\left(\operatorname{Id}_{E_{\overline{K}}} - \Phi^s\right).$$

(2) Zeige, dass es zu jedem $s \in \mathbb{N}$ ein $r \in \mathbb{N}$ gibt mit

$$\operatorname{kern}\left(\operatorname{Id}_{E_{\overline{K}}} - \Phi^s\right) \subseteq \operatorname{Tor}_r\left(E(\overline{K})\right).$$

AUFGABE 23.19. Zeige, dass in Beispiel 23.7 die Abbildung $\operatorname{Id}_{E_{\overline{\mathbb{Z}/(5)}}} - \Phi$ mit der Verdoppelungsabbildung übereinstimmt.

AUFGABE 23.20.*

Es sei E eine elliptische Kurve über einem endlichen Körper K, die durch eine Weierstraßgleichung $Y^2 = X^3 + aX + b$ mit $a, b \in K$ gegeben sei. Zeige, dass es zu jedem $x \in K$ ein Element $y \in L$ in einer quadratischen Körpererweiterung $K \subseteq L$ derart gibt, dass (x, y) ein L-rationaler Punkt der Kurve ist.

AUFGABE 23.21. Bestimme für die durch die Gleichung $Y^2 = X^3 + X$ gegebene elliptische Kurve (falls eine solche vorliegt) die Anzahl der Punkte für die Körper mit $p = 2, 3, 5, 7, 11, 13$ Elementen und vergleiche mit der Hasse-Schranke.

AUFGABE 23.22. Bestimme für die durch die Gleichung $Y^2 = X^3 + 2X - 3$ gegebene elliptische Kurve (falls eine solche vorliegt) die Anzahl der Punkte für die Körper mit $p = 2, 3, 5, 7, 11, 13$ Elementen und vergleiche mit der Hasse-Schranke.

AUFGABE 23.23.*

Es sei E eine elliptische Kurve über $\mathbb{Z}/(p)$, $p \geq 7$ eine Primzahl. Es gebe in $E(\mathbb{Z}/(p))$ ein Element der Ordnung p. Zeige, dass dann sämtliche Elemente $\neq \mathfrak{O}$ die Ordnung p besitzen.

Abbildungsverzeichnis