Prof. Dr. H. Brenner **Osnabrück SS 2025**

Zahlentheorie

Arbeitsblatt 19

Übungsaufgaben

AUFGABE 19.1. Konstruiere einen Körper $\mathbb{F}_9$ mit 9 Elementen.

AUFGABE 19.2. Bestimme in $\mathbb{F}_9$ für jedes Element $\neq 0$ die multiplikative Ordnung. Man gebe insbesondere die primitiven Einheiten an.

AUFGABE 19.3. Es sei p eine Primzahl und F ein Körper mit p^2 Elementen. Welche Ringhomomorphismen zwischen $\mathbb{Z}/(p^2)$ und F gibt es? Man betrachte beide Richtungen.

AUFGABE 19.4. 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 19.5. Es sei K ein Körper der positiven Charakteristik p. Sei

$$\varphi = F^e\colon K \longrightarrow K,\, x \longmapsto x^{p^e}$$

die e-te Iteration des Frobeniushomomorphismus. Zeige, dass es maximal p^e Elemente gibt, die unter φ invariant sind, und dass diese Elemente einen Unterkörper von K bilden.

AUFGABE 19.6. Gehe zur Seite

Endliche Körper/Nicht Primkörper/Einige Operationstafeln

und erstelle für einen der dort angegebenen Körper Additions- und Multiplikationstafeln.

AUFGABE 19.7. Konstruiere endliche Körper mit $4, 8, 9, 16, 25, 27, 32, 49, 64, 81, 121, 125$ und 132 Elementen.

Aufgabe 19.8. Es sei $K \subseteq L$ eine Körpererweiterung von endlichen Körpern. Zeige, dass dies eine einfache Körpererweiterung ist.

Aufgabe 19.9.*

a) Zeige, dass durch

$$K = \mathbb{Z}/(7)[T]/(T^3 - 2)$$

ein Körper mit 343 Elementen gegeben ist.

b) Berechne in K das Produkt $(T^2 + 2T + 4)(2T^2 + 5)$.

c) Berechne das (multiplikativ) Inverse zu $T + 1$.

Aufgabe 19.10. a) Bestimme die Primfaktorzerlegung des Polynoms $F = X^3 + X + 2$ in $\mathbb{Z}/(5)[X]$.

b) Zeige, dass durch

$$K = \mathbb{Z}/(5)[T]/(T^2 - 2)$$

ein Körper mit 25 Elementen gegeben ist.

c) Bestimmen die Primfaktorzerlegung von $F = X^3 + X + 2$ über $K = \mathbb{Z}/(5)[T]/(T^2 - 2)$.

Aufgabe 19.11.*

Bestimme die Matrix des Frobeniushomomorphismus

$$\Phi\colon \mathbb{F}_{49} \longrightarrow \mathbb{F}_{49}$$

bezüglich einer geeigneten $\mathbb{F}_7$-Basis von $\mathbb{F}_{49}$.

Aufgabe 19.12.*

Es sei $\mathbb{F}_q$ ein endlicher Körper der Charakteristik ungleich 2. Zeige unter Verwendung der Isomorphiesätze, dass genau die Hälfte der Elemente aus $\mathbb{F}_q^\times$ ein Quadrat in $\mathbb{F}_q$ ist.

Aufgabe 19.13. Formuliere und beweise eine Version des Eulerschen Kriteriums für beliebige endliche Körper.

Aufgabe 19.14. Es sei K ein endlicher Körper der Charakteristik $p \neq 2$.

a) Zeige, dass es in K Elemente gibt, die keine Quadratwurzel besitzen.

b) Zeige, dass es eine endliche nichttriviale Körpererweiterung $K \subseteq L$ vom Grad zwei gibt.

Aufgabe 19.15. Es sei p eine Primzahl und $q = p^n$, $n \geq 2$. Zeige, dass $\mathbb{Z}/(p^n)$ kein Vektorraum über $\mathbb{Z}/(p)$ sein kann.

Aufgabe 19.16. Betrachte die kommutativen Ringe $\mathbb{Z}/(13)$, $\mathbb{Z}/(169)$ und $\mathbb{F}_{169}$. Bestimme alle Ringhomomorphismen zwischen diesen drei Ringen.

Aufgabe 19.17.*

Man gebe eine vollständige Liste aller kommutativer Ringe mit 6 Elementen.

Aufgabe 19.18.*

Es sei R ein Zahlbereich und es sei $\mathfrak{p} \neq 0$ ein Primideal. Zeige, dass die Norm von $\mathfrak{p}$ eine echte Primzahlpotenz ist.

Aufgabe 19.19.*

Es sei p eine Primzahl, $q = p^e$ mit $e \geq 1$ und sei $\mathbb{F}_q$ der Körper mit q Elementen und $R = \mathbb{F}_q[X]$ der Polynomring darüber. Zeige, dass jeder Restklassenring $R/\mathfrak{a}$ zu einem Ideal $\mathfrak{a} \neq 0$ endlich ist.

Aufgabe 19.20. Bestimme alle Lösungen der Gleichung

$$x^2 + y^2 + xy = 1$$

für die Körper $K = \mathbb{F}_2$, $\mathbb{F}_4$ und $\mathbb{F}_8$.

Aufgabe 19.21.*

Es sei K ein endlicher Körper mit q Elementen.

(1) Zeige, dass die Polynomfunktionen

$$\varphi_d \colon K \longrightarrow K,\ x \longmapsto x^d,$$

mit $0 \leq d < q$ linear unabhängig sind.

(2) Zeige, dass die Exponentialfunktionen

$$\psi_b \colon K \longrightarrow K,\ x \longmapsto b^x,$$

mit $0 \leq b < q$ linear unabhängig sind.

Aufgaben zum Abgeben

Aufgabe 19.22. (3 Punkte)

Es sei R ein Zahlbereich und sei $f_1, \ldots, f_n \in R$ eine $\mathbb{Z}$-Basis von R mit Diskriminante

$$\triangle(f_1, \ldots, f_n) .$$

Es sei $h \in R$. Zeige, dass $hf_1, \ldots, hf_n$ eine $\mathbb{Z}$-Basis des Hauptideals (h) bildet und dass gilt:

$$\min\{|\triangle(b_1, \ldots, b_n)| \, : \, (b_1, \ldots, b_n) \, \mathbb{Z}\text{-Basis von } (h)\} = N(h)^2 \, |\triangle(f_1, \ldots, f_n)| \, .$$

Aufgabe 19.23. (3 Punkte)

Finde möglichst viele (nicht isomorphe) kommutative Ringe mit vier Elementen. Beweise, dass die Liste vollständig ist.

Aufgabe 19.24. (4 Punkte)

Es sei p eine Primzahl und $e, d \in \mathbb{N}_+$. Zeige: $\mathbb{F}_{p^d}$ ist genau dann ein Unterkörper von $\mathbb{F}_{p^e}$, wenn e ein Vielfaches von d ist.

Aufgabe 19.25. (4 Punkte)

Sei q eine echte Primzahlpotenz und $\mathbb{F}_q$ der zugehörige endliche Körper. Zeige, dass in $\mathbb{F}_{q^2}$ jedes Element aus $\mathbb{F}_q$ ein Quadrat ist.

Aufgabe 19.26. (7 Punkte)

Es sei K ein Körper und $K \subseteq L$ eine Ringerweiterung vom Grad drei. Klassifiziere die möglichen Typen von L, ähnlich wie in Lemma 19.9.

Abbildungsverzeichnis