Prof. Dr. H. Brenner **Osnabrück WS 2016/2017**

Zahlentheorie

Arbeitsblatt 15

Übungsaufgaben

AUFGABE 15.1. Sei R ein Integritätsbereich und K ein Körper mit $R \subseteq K$. Zeige, dass dann auch $Q(R) \subseteq K$ gilt.

AUFGABE 15.2. Sei R ein faktorieller Bereich mit Quotientenkörper $K = Q(R)$. Zeige, dass jedes Element $f \in K$, $f \neq 0$, eine im Wesentlichen eindeutige Produktzerlegung

$$f = up_1^{r_1} \cdots p_n^{r_n}$$

mit einer Einheit $u \in R$ und ganzzahligen Exponenten r_i besitzt.

AUFGABE 15.3. Sei R ein faktorieller Bereich mit Quotientenkörper $K = Q(R)$. Es sei $a \in K$ ein Element mit $a^n \in R$ für eine natürliche Zahl $n \geq 1$. Zeige, dass dann schon a zu R gehört.

AUFGABE 15.4. Betrachte die rationalen Zahlen $(\mathbb{Q}, +, 0)$ als kommutative Gruppe. Zeige, dass sie nicht endlich erzeugt ist.

AUFGABE 15.5. Betrachte die rationalen Zahlen $(\mathbb{Q}, +, 0)$ als kommutative Gruppe. Es sei $G \subseteq \mathbb{Q}$ eine endlich erzeugte Untergruppe. Zeige, dass G zyklisch ist.

AUFGABE 15.6. Bestimme einen Erzeuger für die Untergruppe $H \subseteq (\mathbb{Q}, +, 0)$, die durch die rationalen Zahlen

$$\frac{8}{7}, \frac{5}{11}, \frac{7}{10}$$

erzeugt wird.

Eine solche Untergruppe von $\mathbb{Q}$ nennt man auch ein *gebrochenes Ideal*.

Aufgabe 15.7.*

Bestimme einen Erzeuger für das gebrochene Ideal $\mathfrak{f} \subseteq \mathbb{Q}$, das durch die rationalen Zahlen

$$\frac{3}{7}, \frac{5}{6}, \frac{3}{10}$$

erzeugt wird.

Aufgabe 15.8. Es sei $\mathbb{P}$ die Menge der Primzahlen und

$$\alpha \colon \mathbb{P} \longrightarrow \mathbb{Z}$$

eine Abbildung. Zeige, dass die Menge

$$G_\alpha = \left\{ q \in \mathbb{Q}^\times \mid \exp_p(q) \geq \alpha(p) \text{ für alle } p \right\} \cup \{0\}$$

eine Untergruppe von $(\mathbb{Q}, 0, +)$ ist.

Aufgabe 15.9. Es sei

$$\varphi \colon (\mathbb{Q}, 0, +) \longrightarrow (\mathbb{Q} \setminus \{0\}, 1, \cdot)$$

ein Gruppenhomomorphismus. Zeige, dass φ trivial ist.

Aufgabe 15.10. Es sei

$$\varphi \colon (\mathbb{Q} \setminus \{0\}, 1, \cdot) \longrightarrow (\mathbb{Q}, 0, +)$$

ein Gruppenhomomorphismus. Zeige, dass φ nicht injektiv ist.

Aufgabe 15.11. Zeige, dass es einen surjektiven Gruppenhomomorphismus

$$\varphi \colon (\mathbb{Q} \setminus \{0\}, 1, \cdot) \longrightarrow (\mathbb{Q}, 0, +)$$

gibt.

Aufgabe 15.12. Zeige, dass die Definition . der Spur einer linearen Abbildung unabhängig von der gewählten Matrix ist.

Aufgabe 15.13. Zeige, dass $2^{1/5} \in \mathbb{R}$ algebraisch über $\mathbb{Q}$ ist und bestimme das Minimalpolynom davon.

Aufgabe 15.14. Zeige, dass es nur abzählbar viele algebraische Zahlen gibt.

Aufgabe 15.15. Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung. Zeige, dass es einen (injektiven) Ringhomomorphismus $L \to \mathbb{C}$ gibt.

Aufgabe 15.16. Es seien $\mathbb{Q} \subseteq K \subset \mathbb{C}$ und $\mathbb{Q} \subseteq L \subset \mathbb{C}$ zwei endliche Körpererweiterungen von $\mathbb{Q}$ vom Grad d bzw. e. Es seien d und e teilerfremd. Zeige, dass dann

$$K \cap L = \mathbb{Q}$$

ist.

Aufgabe 15.17. Bestimme das Inverse von $2x^2+3x-1$ im Körper $\mathbb{Q}[X]/(X^3 - 5)$ (x bezeichnet die Restklasse von X).

Aufgabe 15.18. Sei K ein endlicher Körper und $K \subseteq L$ eine endliche Körpererweiterung. Zeige direkt, dass für diese Körpererweiterung der Satz vom primitiven Element gilt.

Aufgabe 15.19. Sei $K \subseteq L$ eine endliche Körpererweiterung. Zeige, dass jedes Element $f \in L$ algebraisch über K ist.

Aufgabe 15.20.*

Es sei $z = a + bi \in \mathbb{C}$, $a, b \in \mathbb{R}$, eine algebraische Zahl. Zeige, dass auch die konjugiert-komplexe Zahl $\overline{z} = a - bi$ sowie der Real- und der Imaginärteil von z algebraisch sind. Man bestimme den Grad der Körpererweiterung

$$\mathbb{A} \cap \mathbb{R} \subseteq \mathbb{A}\,.$$

Aufgabe 15.21. Es sei K ein Körper und $L = K(X)$ der Quotientenkörper des Polynomrings $K[X]$. Zeige, dass $K \subset L$ eine einfache, aber keine endliche Körpererweiterung ist.

Aufgaben zum Abgeben

Aufgabe 15.22. (4 Punkte)

Sei K ein Körper und A eine kommutative K-Algebra, die außerdem ein Integritätsbereich sei. Es sei $f \in A$ ein über K algebraisches Element. Sei $P \in K[X]$ ein normiertes Polynom mit $P(f) = 0$. Dann ist P das Minimalpolynom von f genau dann, wenn es irreduzibel ist.

Aufgabe 15.23. (8 Punkte)

Sei p eine Primzahl und sei

$$L = \mathbb{Q}[X]/(X^3 - p)$$

der durch das irreduzible Polynom $X^3 - p$ definierte Erweiterungskörper von $\mathbb{Q}$. Es sei

$$f = 2 + 3x - 4x^2 .$$

Finde die Matrix bezüglich der $\mathbb{Q}$-Basis $1, x, x^2$ von L der durch die Multiplikation mit f definierten $\mathbb{Q}$-linearen Abbildung.

Berechne die Norm und die Spur von f.

Bestimme das Minimalpolynom von f.

Finde das Inverse von f.

Berechne die Diskriminante der Basis $1, f, f^2$.

Aufgabe 15.24. (3 Punkte)

Sei K ein Körper und sei $P = X^n - c \in K[X]$ ein irreduzibles Polynom. Es sei

$$f = a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1X + a_0$$

ein Element in der einfachen endlichen Körpererweiterung $K \subseteq L = K[X]/(P)$ vom Grad n. Zeige, dass die Spur von f gleich na_0 ist.

In der folgenden Aufgabe werden verschiedene äquivalente Bedingungen an ein Polynom gestellt, die man alle als Definition eines separablen Polynoms nehmen kann. Man darf verwenden, dass es zu jedem Körper einen Erweiterungskörper gibt, in dem ein vorgegebenes Polynom in Linearfaktoren zerfällt.

Aufgabe 15.25. (4 Punkte)

Sei K ein Körper und sei $F \in K[X]$ ein Polynom vom Grad n. Zeige, dass die folgenden Aussagen äquivalent sind:

(1) F und die (formale) Ableitung F' sind teilerfremd.
(2) F und die (formale) Ableitung F' erzeugen das Einheitsideal.
(3) F besitzt in keinem Erweiterungskörper $K \subseteq L$ mehrfache Nullstellen.
(4) Es gibt einen Erweiterungskörper $K \subseteq L$, so dass F als Polynom in $L[X]$ in n verschiedene Linearfaktoren zerfällt.

Aufgabe 15.26. (3 Punkte)

Sei K ein Körper und sei $F \in K[X]$ ein irreduzibles Polynom. Man gebe eine einfache Charakterisierung dafür, dass F separabel ist.

Zeige, dass in Charakteristik null jedes irreduzible Polynom separabel ist.

Man gebe ein Beispiel, dass das in positiver Charakteristik nicht immer stimmen muss.