Prof. Dr. H. Brenner **Osnabrück SS 2011**

Körper- und Galoistheorie

Arbeitsblatt 7

Aufwärmaufgaben

Aufgabe 7.1. Bestimme die multiplikative Ordnung aller Einheiten im Restklassenkörper $\mathbb{Z}/(7)$.

Aufgabe 7.2. Berechne 3^{1457} in $\mathbb{Z}/(13)$.

Aufgabe 7.3. Bestimme im Polynomring $\mathbb{F}_5[X]$ alle irreduziblen Polynome vom Grad 3.

Aufgabe 7.4. Bestimme die fünf kleinsten Primzahlen p mit der Eigenschaft, dass das Polynom $X^6 - 1$ über $\mathbb{Z}/(p)$ in Linearfaktoren zerfällt.

Aufgabe 7.5. Betrachte den Körper $K = \mathbb{F}_4 = \mathbb{Z}/(2)[U]/(U^2 + U + 1)$. Führe im Polynomring $K[X]$ die Polynomdivision

$$X^4 + uX^3 + (u + 1)X + 1 \text{ durch } uX^2 + X + u + 1$$

aus, wobei u die Restklasse von U in K bezeichnet.

Aufgabe 7.6. a) Bestimmen Sie die Primfaktorzerlegung des Polynoms $F = X^3 + X + 2$ in $\mathbb{Z}/(5)[X]$.

b) Zeigen Sie, dass durch

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

ein Körper mit 25 Elementen gegeben ist.

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

Aufgabe 7.7. Bestimme sämtliche Primkörper.

Aufgabe 7.8. Sei p eine Primzahl. Beweise durch Induktion den kleinen Fermat, also die Aussage, dass $a^p - a$ ein Vielfaches von p ist für jede ganze Zahl a.

Aufgabe 7.9. Sei R ein kommutativer Ring und $p \in R$, $p \neq 0$. Zeige, dass p genau dann ein Primelement ist, wenn der Restklassenring $R/(p)$ ein Integritätsbereich ist.

Aufgabe 7.10. Sei X ein topologischer Raum und $R = \mathrm{C}^0(X, \mathbb{R})$ der Ring der stetigen Funktionen auf X. Es sei $T \subseteq X$ eine Teilmenge. Zeige, dass die Teilmenge

$$I = \{f \in R | \, f|_T = 0\}$$

ein Ideal in R ist. Definiere einen Ringhomomorphismus

$$R/I \longrightarrow \mathrm{C}^0(T, \mathbb{R}).$$

Ist dieser immer injektiv? Surjektiv?

Aufgabe 7.11. Zeige, dass die beiden kommutativen Gruppen $(\mathbb{Q}, 0, +)$ und $(\mathbb{Q}_+, 1, \cdot)$ nicht isomorph sind.

Aufgabe 7.12. Zeige, dass die Abbildung

$$\mathbb{Q}[i]^\times \longrightarrow (\mathbb{Q}_+, 1, \cdot), \, z = x + iy \longmapsto |z|^2 = x^2 + y^2,$$

ein Gruppenhomomorphismus ist.

Aufgabe 7.13. Zeige, dass die Menge

$$S^1_{\mathbb{Q}} = \{z \in \mathbb{Q}[i] | \, |z| = 1\}$$

mit der Multiplikation in $\mathbb{Q}[i]$ eine kommutative Gruppe ist.

Aufgabe 7.14. Es sei

$$S^1_{\mathbb{Q}} = \{z \in \mathbb{Q}[i] | \, |z| = 1\}$$

der rationale Einheitskreis mit der aus $\mathbb{Q}[i]^\times$ ererbten Gruppenstruktur. Berechne die ersten vier Potenzen von $\frac{3}{5} + \frac{4}{5}i \in S^1_{\mathbb{Q}}$.

Aufgaben zum Abgeben

Aufgabe 7.15. (3 Punkte)

Bestimme die multiplikative Ordnung aller Einheiten im Restklassenkörper $\mathbb{Z}/(11)$.

Aufgabe 7.16. (5 Punkte)

Bestimme im Polynomring $\mathbb{Z}/(3)[X]$ alle irreduziblen Polynome vom Grad 4.

Aufgabe 7.17. (4 Punkte)

Sei p eine Primzahl und sei $f(x)$ ein Polynom mit Koeffizienten in $\mathbb{Z}/(p)$ vom Grad $d \geq p$. Zeige, dass es ein Polynom $g(x)$ mit einem Grad $< p$ gibt derart, dass für alle Elemente $a \in \mathbb{Z}/(p)$ die Gleichheit

$$f(a) = g(a)$$

gilt.

Aufgabe 7.18. (4 Punkte)

Es sei

$$S^1_{\mathbb{Q}} = \{z \in \mathbb{Q}[i] \mid |z| = 1\}$$

der rationale Einheitskreis mit der aus $\mathbb{Q}[i]^\times$ ererbten Gruppenstruktur. Zeige, dass die Gruppen $S^1_{\mathbb{Q}}$ und $\mathbb{Q}/\mathbb{Z}$ nicht isomorph sind.

Aufgabe 7.19. (5 Punkte)

Zeige, dass der Gruppenhomomorphismus

$$\mathbb{Q}[i]^\times \longrightarrow (\mathbb{Q}_+, 1, \cdot),\ x + iy \longmapsto x^2 + y^2,$$

nicht surjektiv ist.

Abbildungsverzeichnis