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

Körper- und Galoistheorie

Arbeitsblatt 11

Aufwärmaufgaben

Aufgabe 11.1. Zeige, dass der Körper der komplexen Zahlen $\mathbb{C}$ der Zerfällungskörper des Polynoms $X^2 + 1 \in \mathbb{R}[X]$ ist.

Aufgabe 11.2. Es sei K ein Körper und seien $F_1, \ldots, F_r \in K[X]$ Polynome. Zeige, dass es eine Körpererweiterung $K \subseteq L$ gibt derart, dass diese Polynome in $L[X]$ in Linearfaktoren zerfallen.

Aufgabe 11.3. Sei $K \subseteq L$ eine Körpererweiterung von endlichen Körpern. Zeige, dass dies eine einfache Körpererweiterung ist.

Aufgabe 11.4. 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 *Frobenius-Homomorphismus* nennt.

Aufgabe 11.5. Sei K ein Körper der positiven Charakteristik p. Sei $F : K \to K$ der Frobenius-Homomorphismus. Zeige, dass genau die Elemente aus $\mathbb{Z}/(p)$ invariant unter F sind.

Aufgabe 11.6. 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 11.7. Bestimme die formale Ableitung von

$$2X^7 + X^6 + 2X^5 + X^4 + X^3 + X^2 + 2 \in \mathbb{Z}/(3)[X]\,.$$

Aufgabe 11.8. Sei K ein Körper der positiven Charakteristik $p > 0$. Bestimme die Menge der Polynome $F \in K[T]$ mit formaler Ableitung $F' = 0$.

Die folgenden fünf Aufgaben waren schon mal Klausuraufgaben (es gibt dazu auch Lösungen).

AUFGABE 11.9. Bestimme in der Einheitengruppe $\mathbb{Z}/(17)^\times$ zu jeder möglichen Ordnung k ein Element $x \in \mathbb{Z}/(17)^\times$, das die Ordnung k besitzt. Man gebe auch eine Untergruppe

$$H \subseteq \mathbb{Z}/(17)^\times$$

an, die aus vier Elementen besteht.

AUFGABE 11.10. Sei p eine Primzahl und $x \in (\mathbb{Z}/(p))^\times$ eine Einheit. Es sei a die Ordnung von x in der additiven Gruppe $(\mathbb{Z}/(p), +, 0)$ und es sei b die Ordnung von x in der multiplikativen Gruppe $((\mathbb{Z}/(p))^\times, \cdot, 1)$. Zeige, dass a und b teilerfremd sind.

AUFGABE 11.11. 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 11.12. Beschreibe den Körper mit neun Elementen $\mathbb{F}_9$ als einen Restklassenkörper von $\mathbb{Z}/(3)[X]$. Man gebe eine primitive Einheit in $\mathbb{F}_9$ an.

AUFGABE 11.13. Beschreibe den Körper mit acht Elementen $\mathbb{F}_8$ als einen Restklassenkörper von $\mathbb{Z}/(2)[X]$. Man gebe eine primitive Einheit in $\mathbb{F}_8$ an.

Aufgaben zum Abgeben

AUFGABE 11.14. (4 Punkte)

Konstruiere endliche Körper mit $64, 81, 121, 125$ und 128 Elementen.

AUFGABE 11.15. (4 Punkte)

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

AUFGABE 11.16. (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 11.17. (4 Punkte)

Finde einen Erzeuger der Einheitengruppe eines Körpers mit 27 Elementen. Wie viele solche Erzeuger gibt es?

Aufgabe 11.18. (3 Punkte)

Sei K ein Körper und sei $K[X]$ der Polynomring über K. Beweise die folgenden Rechenregeln für das formale Ableiten $F \mapsto F'$:

(1) Die Ableitung eines konstanten Polynoms ist null.
(2) Die Ableitung ist K-linear.
(3) Es gilt die *Produktregel*, also

$$(FG)' = FG' + F'G\,.$$

Es sei K ein Körper. Ein Element $a \in K$ heißt *mehrfache Nullstelle* eines Polynoms $P \in K[X]$, wenn in der Primfaktorzerlegung von P das lineare Polynom $X - a$ mit einem Exponenten ≥ 2 vorkommt.

Aufgabe 11.19. (4 Punkte)

Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $F \in K[X]$ und $a \in K$. Zeige, dass a eine mehrfache Nullstelle von F genau dann ist, wenn $F'(a) = 0$ ist, wobei F' die formale Ableitung von F bezeichnet.

Abbildungsverzeichnis