Prof. Dr. H. Brenner **Osnabrück WS 2018/2019**

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 $P = X^2 + aX + b \in K[X]$ ein quadratisches Polynom über einem Körper K. Welche Möglichkeiten gibt es für den Zerfällungskörper von P?

Aufgabe 11.3. Es sei K ein Körper und seien $F_1, \ldots, F_r \in K[X]$ Polynome. Zeige, dass es eine endliche Körpererweiterung $K \subseteq L$ derart gibt, dass diese Polynome in $L[X]$ in Linearfaktoren zerfallen.

Aufgabe 11.4. Es sei K ein Körper, $F \in K[X]$ ein Polynom vom Grad n und $K \subseteq L$ der Zerfällungskörper von F. Zeige, dass die Abschätzung

$$\operatorname{grad}_K L \leq n!$$

gilt.

Aufgabe 11.5.*

Es sei $X^n - a \in \mathbb{Q}[X]$ mit $n \geq 4$ gerade. Zeige, dass der Zerfällungskörper von $X^n - a$ maximal den Grad $\frac{n!}{2}$ besitzt.

Aufgabe 11.6. Es sei $q \in \mathbb{Q}$ eine rationale Zahl und es sei L der Zerfällungskörper von $X^3 - q$. Welchen Grad besitzt L (über $\mathbb{Q}$)? Man gebe für jeden möglichen Grad Beispiele an.

Aufgabe 11.7.*

Das Polynom $F = X^3 - 3X + 1 \in \mathbb{Q}[X]$ ist irreduzibel nach Aufgabe 3.16 und definiert daher eine Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\left(X^3 - 3X + 1\right) =: L$$

vom Grad 3. Die Restklasse von X in L sei mit α bezeichnet. Zeige, dass auch die Elemente aus L

$$\beta = \alpha^2 - 2$$

und

$$\gamma = -\alpha^2 - \alpha + 2$$

Nullstellen von F sind.

Aufgabe 11.8.*

Es sei $F \in \mathbb{Q}[X]$ und $\mathbb{Q} \subseteq L \subseteq \mathbb{C}$ der Zerfällungskörper zu F. Zeige, dass die komplexe Konjugation den Körper L in sich überführt, also ein Element in der Galoisgruppe $\mathrm{Gal}\,(L|K)$ definiert.

Aufgabe 11.9. Sei $K \subseteq L$ eine Körpererweiterung von endlichen Körpern. Zeige, dass dies eine einfache Körpererweiterung ist.

Aufgabe 11.10. 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 11.11. 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 11.12. Sei K ein endlicher Körper der Charakteristik p. Zeige, dass der Frobeniushomomorphismus ein Körperautomorphismus ist.

Aufgabe 11.13. 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 11.14. Sei $\mathbb{F}_q$ der Körper mit $q = p^e$ Elementen. Bestimme die Ordnung des Frobeniushomomorphismus in der Automorphismengruppe von $\mathbb{F}_q$.

Aufgabe 11.15. 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 11.16. Bestimme die formale Ableitung von

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

AUFGABE 11.17. Sei K ein Körper der positiven Charakteristik $p > 0$. Bestimme die Menge der Polynome $F \in K[T]$ mit formaler Ableitung $F' = 0$.

AUFGABE 11.18.*

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 11.19. Zeige, dass das Polynom $X^9 - X \in \mathbb{Z}/(3)[X]$ die Zerlegung

$$\begin{aligned} X^9 - X &= \left(X^3 - X\right)\left(X^8 + X^6 + X^4 + X^2 + 1\right) \\ &= X(X-1)(X+1)\left(X^2+1\right)\left(X^2 + 2X + 1\right) \\ &\qquad \left(X^2 + X + 2\right)\left(X^2 + 2X + 2\right) \end{aligned}$$

besitzt, wobei die Faktoren in der zweiten Zerlegung irreduzibel sind. Zeige, dass die Restklassenkörper

$$\mathbb{Z}/(3)[X]/\left(X^2+1\right),\ \mathbb{Z}/(3)[X]/\left(X^2+2X+1\right),$$
$$\mathbb{Z}/(3)[X]/\left(X^2+X+2\right),\ \mathbb{Z}/(3)[X]/\left(X^2+2X+2\right)$$

untereinander isomorph sind.

AUFGABE 11.20.*

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.

AUFGABE 11.21.*

Es sei p eine ungerade Primzahl. Es sei $q = p^e$ und $c \in \mathbb{F}_q$ ein Nichtquadrat.

(1) Zeige
$$\mathbb{F}_{q^2} \cong \mathbb{F}_q[X]/\left(X^2 - c\right).$$
(2) Zeige, dass es eine Kette von rein-quadratischen Erweiterungen
$$\mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^4} \subseteq \mathbb{F}_{p^8} \subseteq \mathbb{F}_{p^{16}} \subseteq \dots$$
gibt.
(3) Zeige, dass die Restklasse von X in $\mathbb{Z}/(3)[X]/\left(X^2 - 2\right)$ ein Quadrat ist.
(4) Es sei nun $p = 1 \mod 4$. Zeige, dass die Restklasse x von X in $\mathbb{F}_q[X]/\left(X^2 - c\right)$ ein Nichtquadrat ist.
(5) Es sei $p = 1 \mod 4$ und sei $a \in \mathbb{Z}/(p)$ ein Nichtquadrat. Zeige, dass $Y^{2^n} - a$ für alle $n \geq 1$ irreduzibel ist.

Aufgabe 11.22.*

Finde ein primitives Element in $\mathbb{Z}/(11)$ und in $\mathbb{Z}/(121)$. Man gebe ferner ein Element der Ordnung 10 und ein Element der Ordnung 11 in $\mathbb{Z}/(121)$ an. Gibt es Elemente der Ordnung 10 und der Ordnung 11 auch in $\mathbb{F}_{121}$?

Aufgaben zum Abgeben

Aufgabe 11.23. (4 Punkte)

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

Aufgabe 11.24. (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 11.25. (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 11.26. (4 Punkte)

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

Aufgabe 11.27. (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 0.
(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 11.28. (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 genau dann eine mehrfache Nullstelle von F ist, wenn $F'(a) = 0$ ist, wobei F' die formale Ableitung von F bezeichnet.

Abbildungsverzeichnis