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

Körper- und Galoistheorie

Arbeitsblatt 9

Aufwärmaufgaben

Aufgabe 9.1. Finde primitive Einheiten in den Restklassenkörpern $\mathbb{Z}/(2)$, $\mathbb{Z}/(3)$, $\mathbb{Z}/(5)$, $\mathbb{Z}/(7)$ und $\mathbb{Z}/(11)$.

Aufgabe 9.2.*

Bestimme sämtliche primitive Einheiten im Restklassenkörper $\mathbb{Z}/(13)$.

Aufgabe 9.3.*

Wie viele Quadrate und wie viele primitive Elemente besitzt $\mathbb{Z}/(31)$?

Wie viele Elemente besitzt $\mathbb{Z}/(31)$, die weder primitiv noch ein Quadrat sind?

Sei x ein primitives Element von $\mathbb{Z}/(31)$. Liste explizit alle Elemente x^i auf, die weder primitiv noch ein Quadrat sind.

Aufgabe 9.4. Sei $K = \mathbb{Z}/(59)$ der Körper mit 59 Elementen.

a) Bestimme die Anzahl der primitiven Elemente in K.

b) Berechne in K die Zweierpotenzen 2^4, 2^8 und 2^{16}.

c) Berechne 2^{29} in K.

d) Man gebe für jede mögliche (multiplikative) Ordnung in $K^\times$ ein Element an, das diese Ordnung besitzt.

Aufgabe 9.5. Sei p eine ungerade Primzahl und $\mathbb{Z}/(p)$ der zugehörige Restklassenkörper. Zeige, dass das Produkt von zwei primitiven Einheiten niemals primitiv ist.

Aufgabe 9.6. Bestimme die Einheiten von $\mathbb{Z}/(8)$.

Aufgabe 9.7. Konstruiere einen Körper $\mathbb{F}_9$ mit 9 Elementen.

Aufgabe 9.8.*

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 9.9.*

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 9.10.*

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

Aufgabe 9.12. Wie viele primitive Elemente besitzt der Körper mit 529 Elementen?

Aufgabe 9.13.*

Es sei $\mathbb{Z}/(p) \subseteq \mathbb{F}_q$ eine Erweiterung endlicher Körper mit $q = p^e$ und es sei u eine primitive Einheitswurzel von $\mathbb{F}_q$. Was ist die erste Potenz u^n, $n \geq 1$, die zu $\mathbb{Z}/(p)$ gehört? Ist dieses u^n ein primitives Element von $(\mathbb{Z}/(p))^\times$?

Aufgabe 9.14. 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 9.15. a) Sei K ein Körper. Zeige, dass die Einheitengruppe von K nicht zyklisch unendlich ist.

b) Sei R ein kommutativer Ring, dessen Charakteristik nicht zwei ist. Zeige, dass die Einheitengruppe von R nicht zyklisch unendlich ist.

c) Beschreibe einen kommutativen Ring, dessen Einheitengruppe zyklisch unendlich ist.

Aufgabe 9.16. Bestimme den Rest von 44! modulo 47.

Aufgabe 9.17. Bestimme die Zerlegung von $X^{p-1} - 1$ in irreduzible Polynome im Polynomring $\mathbb{Z}/(p)[X]$. Beweise aus dieser Zerlegung den Satz von Wilson.

Aufgabe 9.18.*

Sei p eine Primzahl. Man gebe einen Körper der Charakteristik p an, der unendlich viele Elemente besitzt.

Aufgabe 9.19.*

Zeige, dass die Matrizen

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

eine kommutative Gruppe bilden, in der jedes Element zu sich selbst invers ist.

Zeige insbesondere, dass die Gruppe in der vorstehenden Aufgabe nicht zyklisch ist.

Aufgaben zum Abgeben

Aufgabe 9.20. (3 Punkte)

Finde primitive Einheiten in den Restklassenkörpern $\mathbb{Z}/(13)$, $\mathbb{Z}/(17)$ und $\mathbb{Z}/(19)$.

Aufgabe 9.21. (5 Punkte)

Konstruiere zu einer Primzahl p einen Körper mit p^2 Elementen.

Aufgabe 9.22. (4 Punkte)

Konstruiere endliche Körper mit $4, 8, 9, 16, 25, 27, 32$ und 49 Elementen.

Aufgabe 9.23. (4 Punkte)

Es sei $\mathbb{F}_9 = \mathbb{Z}/(3)[Z]/(Z^2+1)$ der Körper mit 9 Elementen (z bezeichne die Restklasse von Z). Führe in $\mathbb{F}_9[X]$ die Division mit Rest „P durch T“ für die beiden Polynome $P = X^4 + (1+2z)X^3 + zX^2 + 2X + 2 + z$ und $T = (z+1)X^2 + zX + 2$ durch.

Aufgabe 9.24. (4 Punkte)

Finde einen Erzeuger der Einheitengruppe eines Körpers mit 25 Elementen. Wie viele solche Erzeuger gibt es?

Abbildungsverzeichnis