**Prof. Dr. H. Brenner** **Osnabrück SS 2025**

# Zahlentheorie

## Arbeitsblatt 5

## Übungsaufgaben

Aufgabe 5.1. Bestimme die multiplikative Ordnung aller Einheiten im Restklassenkörper $\mathbb{Z}/(11)$.

Aufgabe 5.2.*

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

Aufgabe 5.3. Bestimme sämtliche primitive Einheiten im Restklassenkörper $\mathbb{Z}/(23)$.

Aufgabe 5.4. Finde primitive Einheiten in den Restklassenkörpern $\mathbb{Z}/(13)$, $\mathbb{Z}/(17)$ und $\mathbb{Z}/(19)$.

Aufgabe 5.5.*

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

Aufgabe 5.7. Es sei $n \in \mathbb{N}_+$. Zeige, dass die Gruppe der $n$-ten Einheitswurzeln in $\mathbb{C}$ und die Gruppe $\mathbb{Z}/(n)$ isomorph sind.

Aufgabe 5.8. Beweise ausschließlich durch Anzahlbetrachtungen Lemma 5.9, dass also der kanonische Homomorphismus $(\mathbb{Z}/(p^r))^\times \to (\mathbb{Z}/(p))^\times$ surjektiv ist ($p$ Primzahl).

Aufgabe 5.9.*

Bestimme eine primitive Einheit $v \in \mathbb{Z}/(5)$ und ein Urbild $u \in \mathbb{Z}/(25)$ von $v$, das in $\mathbb{Z}/(25)$ nicht primitiv ist.

Aufgabe 5.10. a) Finde ein primitives Element in $\mathbb{Z}/(3)$, in $\mathbb{Z}/(9)$ und in $\mathbb{Z}/(27)$.

b) Finde eine ganze Zahl, die in $\mathbb{Z}/(3)$ primitiv ist, aber nicht in $\mathbb{Z}/(9)$.

c) Zeige, dass jede ganze Zahl, die in $\mathbb{Z}/(9)$ primitiv ist, auch in $\mathbb{Z}/(27)$ primitiv ist.

Aufgabe 5.11. Bestimme alle primitiven Elemente von $\mathbb{Z}/(27)$.

Aufgabe 5.12. Es sei $p$ eine Primzahl und $r \geq 2$. Beschreibe explizit die Elemente im Kern der Abbildung

$$(\mathbb{Z}/(p^r))^\times \longrightarrow \left(\mathbb{Z}/(p^{r-1})\right)^\times.$$

Aufgabe 5.13.*

Es sei $p$ eine Primzahl. Wir betrachten den kanonischen Ringhomomorphismus

$$\mathbb{Z}/(p^2) \longrightarrow \mathbb{Z}/(p)$$

und den zugehörigen Gruppenhomomorphismus

$$\left(\mathbb{Z}/(p^2)\right)^\times \longrightarrow (\mathbb{Z}/(p))^\times$$

der Einheitengruppen. Es sei $v$ eine primitive Einheit von $\mathbb{Z}/(p)$. Zeige, dass unter den Urbildern von $v$ in $\mathbb{Z}/(p^2)$ ein Element keine primitive Einheit von $\mathbb{Z}/(p^2)$ ist, und $p-1$ Elemente primitive Einheiten sind.

Aufgabe 5.14.*

Es sei $p$ eine ungerade Primzahl und $r \geq s \geq 2$ Wir betrachten den kanonischen Ringhomomorphismus

$$\mathbb{Z}/(p^r) \longrightarrow \mathbb{Z}/(p^s)$$

und den zugehörigen Gruppenhomomorphismus

$$(\mathbb{Z}/(p^r))^\times \longrightarrow (\mathbb{Z}/(p^s))^\times$$

der Einheitengruppen. Es sei $v$ eine primitive Einheit von $\mathbb{Z}/(p^s)$. Zeige, dass sämtliche Urbilder von $v$ in $\mathbb{Z}/(p^r)$ primitive Einheiten von $\mathbb{Z}/(p^s)$ sind.

In der folgenden Aufgabe bezeichnet $\mathbb{F}_{121}$ den Körper mit 121 Elementen. Darüber hinaus muss muss man nichts über ihn wissen.

Aufgabe 5.15.*

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 $\mathbb{F}_{121}$?

Aufgabe 5.16.*

In dieser Aufgabe geht es um den Restklassenring $\mathbb{Z}/(360)$.

a) Schreibe $\mathbb{Z}/(360)$ als Produktring (im Sinne des chinesischen Restsatzes).

b) Wie viele Einheiten besitzt $\mathbb{Z}/(360)$?

c) Schreibe das Element 239 in komponentenweiser Darstellung. Begründe, warum es sich um eine Einheit handelt und finde das Inverse in komponentenweiser Darstellung.

d) Berechne die Ordnung von 239 in $\mathbb{Z}/(360)$.

Aufgabe 5.17. Zeige, dass die eulersche Funktion $\varphi$ für natürliche Zahlen $n, m$ die Eigenschaft

$$\varphi(\mathrm{ggT}(m,n)) \cdot \varphi(\mathrm{kgV}(m,n)) \;=\; \varphi(n) \cdot \varphi(m)$$

erfüllt.

Aufgabe 5.18. Es sei $\varphi(n)$ die Eulersche Funktion. Zeige die Abschätzung

$$\varphi(n) \;\geq\; \frac{\sqrt{n}}{2}.$$

In den nächsten Aufgaben werden die folgenden Begriffe verwendet.

Ein Element $a$ eines kommutativen Ringes $R$ heißt *nilpotent*, wenn $a^n = 0$ für eine natürliche Zahl $n$ ist.

Ein Element $e$ eines kommutativen Ringes heißt *idempotent*, wenn $e^2 = e$ gilt.

Aufgabe 5.19.*

Es sei $p \in \mathbb{Z}$ eine Primzahl und $n \in \mathbb{N}$. Zeige, dass der Restklassenring $\mathbb{Z}/(p^n)$ nur die beiden trivialen idempotenten Elemente 0 und 1 besitzt.

Aufgabe 5.20. Bestimme die nilpotenten Elemente, die idempotenten Elemente und die Einheiten von $\mathbb{Z}/(60)$.

Aufgabe 5.21.*

a) Finde die Zahlen $z \in \{0,1,\ldots,9\}$ mit der Eigenschaft, dass die letzte Ziffer ihres Quadrates (in der Dezimaldarstellung) gleich $z$ ist.

b) Finde die Zahlen $z \in \{0,1,\ldots,99\}$ mit der Eigenschaft, dass die beiden letzten Ziffern ihres Quadrates (in der Dezimaldarstellung) gleich $z$ ist.

Aufgabe 5.22. Es sei $R$ ein kommutativer Ring und es seien $f,g \in R$ nilpotente Elemente. Zeige, dass dann die Summe $f+g$ ebenfalls nilpotent ist.

Aufgabe 5.23. Es sei $R$ ein kommutativer Ring und sei $f \in R$. Es sei $f$ sowohl nilpotent als auch idempotent. Zeige, dass $f = 0$ ist.

Aufgabe 5.24. Es sei $R$ ein kommutativer Ring und $f \in R$ ein nilpotentes Element. Zeige, dass $1+f$ eine Einheit ist.

Aufgabe 5.25.*

a) Es sei $K$ ein Körper. Zeige, dass die Einheitengruppe von $K$ nicht zyklisch unendlich ist.

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

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

## Aufgaben zum Abgeben

Aufgabe 5.26. (3 Punkte)

Beweise die *eulersche Formel* für die eulersche Funktion, das ist die Aussage, dass

$$\varphi(n) = n \cdot \prod_{p|n,\ p \text{ prim}} \left(1 - \frac{1}{p}\right)$$

gilt.

Aufgabe 5.27. (5 Punkte)

Bestimme die nilpotenten Elemente, die idempotenten Elemente und die Einheiten in $\mathbb{Z}/(72)$.

Aufgabe 5.28. (3 Punkte)

Zeige, dass für natürliche Zahlen $k$ und $n$ mit $k \mid n$ der kanonische Homomorphismus

$$(\mathbb{Z}/(n))^\times \longrightarrow (\mathbb{Z}/(k))^\times$$

surjektiv ist.

Aufgabe 5.29. (4 Punkte)

Es sei $n$ eine natürliche Zahl. Charakterisiere diejenigen Teiler $k$ von $n$ mit der Eigenschaft, dass für den kanonischen Ringhomomorphismus

$$\varphi\colon\ \mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(k)$$

gilt, dass $a$ in $\mathbb{Z}/(n)$ genau dann eine Einheit ist, wenn $\varphi(a)$ in $\mathbb{Z}/(k)$ eine Einheit ist.

Aufgabe 5.30. (3 Punkte)

Bestimme eine primitive Einheit $v \in \mathbb{Z}/(7)$ und ein Urbild $u \in \mathbb{Z}/(49)$ von $v$, das in $\mathbb{Z}/(49)$ nicht primitiv ist.

Aufgabe 5.31. (4 Punkte)

Es sei $p$ eine fixierte Primzahl. Zu jeder ganzen Zahl $n \neq 0$ bezeichne $\nu_p(n)$ den Exponenten, mit dem die Primzahl $p$ in der Primfaktorzerlegung von $n$ vorkommt.

a) Zeige: die Abbildung $\nu_p\colon\ \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ ist surjektiv.

b) Zeige: es gilt $\nu_p(nm) = \nu_p(n) + \nu_p(m)$.

c) Finde eine Fortsetzung $\nu_p\colon\ \mathbb{Q} \setminus \{0\} \to \mathbb{Z}$ der gegebenen Abbildung, die ein Gruppenhomomorphismus ist (wobei $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ mit der Multiplikation und $\mathbb{Z}$ mit der Addition versehen ist).

d) Beschreibe den Kern des unter c) beschriebenen Gruppenhomomorphismus.

# Abbildungsverzeichnis