Einführung in die Algebra und Diskrete Mathematik
Sommersemester 2015
2. Test, 18.05.2015

Vorname: ..... Nachname: .....

Matrikelnummer: ..... Übungsleiter: .....

Es sind keine Unterlagen und keine elektronischen Hilfsmittel erlaubt.

Aufgabe 1 Geben Sie explizit eine ganze Zahl $z \in \{1, 2, \ldots, 5119\}$ an, welche die folgende Kongruenz erfüllt:

$$513^z \equiv 1 \pmod{5120}.$$

Begründen Sie, dass die gefundene Zahl z diese Kongruenz tatsächlich löst. *(4)*

Lösung. Da $513 = 3^3 \cdot 19$ und $5120 = 2^{10} \cdot 5$, ist $\mathrm{ggT}(513, 5120) = 1$. Somit folgt aus dem Satz von Euler, dass $z = \varphi(5120) = 5120 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 2048$ die Kongruenz löst. □

Aufgabe 2 Wir betrachten die Restklassenringe $\mathbb{Z}_n$. Bearbeiten Sie folgende Aufgabenstellungen:

1. Ist das Element $[24]_{51}$ im Restklassenring $\mathbb{Z}_{51}$ invertierbar? Begründen Sie Ihre Antwort mit einem Kriterium aus der Vorlesung. *(2)*

2. Beweisen Sie, dass der Restklassenring $\mathbb{Z}_n$ genau dann ein Körper ist, wenn n eine Primzahl ist. *(4)*

Lösung. Wir wissen, dass $[a]_n$ in $\mathbb{Z}_n$ genau dann invertierbar ist, wenn $\mathrm{ggT}(a, n) = 1$, weil nur dann die Kongruenz $a \cdot x \equiv 1 \pmod{n}$ lösbar ist. Da $\mathrm{ggT}(24, 51) = 3$ ist, ist $[24]_{51}$ im Restklassenring $\mathbb{Z}_{51}$ nicht invertierbar. Wir zeigen (2.). Sei zunächst n zusammengesetzt, also $n = kl$ mit $1 \leq k, l \leq n - 1$. Dann ist $[k]_m[l]_n = [kl]_n = [n]_n = [0]_n$; also ist $\mathbb{Z}_n$ kein Integritätsbereich und somit kein Körper. Wenn aber $n \in \mathbb{P}$ ist, dann gilt $\mathrm{ggT}(a, n) = 1$ für alle $a \in \{1, \ldots, n - 1\}$, und somit sind alle Elemente ungleich $[0]_n$ invertierbar und $\mathbb{Z}_n$ ist ein Körper. □

Aufgabe 3 Wir betrachten den Ring $\mathbb{Z} \times \mathbb{Z} := \{(z_1, z_2) : z_1, z_2 \in \mathbb{Z}\}$ mit komponentenweiser Addition und Multiplikation (also das direkte Produkt von $\mathbb{Z}$ mit sich selbst).

1. In der Übung wurde gezeigt, dass jedes Ideal eines direkten Produkts zweier Ringe selbst ein direktes Produkt von Idealen der jeweiligen Ringe sein muss. Folgern Sie daraus, dass $\mathbb{Z} \times \mathbb{Z}$ ein Hauptidealring ist. *(3)*

2. Sei $I = \langle (4,3), (6,5) \rangle$ das von den Elementen $(4,3)$ und $(6,5)$ erzeugte Ideal in $\mathbb{Z} \times \mathbb{Z}$. Ist dieses Ideal I gleich dem ganzen Ring $\mathbb{Z} \times \mathbb{Z}$? Begründen Sie Ihre Antwort. *(2)*

Lösung. Zu (1.): Jedes Ideal I von $\mathbb{Z} \times \mathbb{Z}$ lässt sich also schreiben als $I = I_1 \times I_2$, wobei I_1, I_2 Ideale von $\mathbb{Z}$ sind. Da $\mathbb{Z}$ bekanntlich ein Hauptidealring ist, gibt es $c_1, c_2 \in \mathbb{Z}$, sodass $I_1 = (c_1)$ und $I_2 = (c_2)$. Also ist I gegeben durch

$$I = \{(c_1 z_1, c_2 z_2) : z_1, z_2 \in \mathbb{Z}\} = \{(c_1, c_2) z : z \in \mathbb{Z} \times \mathbb{Z}\}.$$

Somit erzeugt offenbar (c_1, c_2) das Ideal I. Damit ist bewiesen, dass jedes Ideal von $\mathbb{Z} \times \mathbb{Z}$ ein Hauptideal ist, was zu zeigen war.
Zu (2.): Das Ideal I ist gegeben durch

$$\begin{aligned} I &= \{(4,3)(z_1, z_2) + (6,5)(w_1, w_2) : z_1, z_2, w_1, w_2 \in \mathbb{Z}\} \\ &= \{(4z_1 + 6w_1, 3z_2 + 5w_2) : z_1, z_2, w_1, w_2 \in \mathbb{Z}\}. \end{aligned}$$

In der ersten Komponente können wir also nur gerade Zahlen erhalten; das Ideal I kann somit nicht ganz $\mathbb{Z} \times \mathbb{Z}$ sein. □

Aufgabe 4 Sei $(R, +, \cdot)$ ein (nicht zwingend kommutativer) Ring mit Einselement und $a \in R$ ein invertierbares Element. Wir definieren die Abbildung

$$h_a : R \to R : x \mapsto a^{-1}xa.$$

Zeigen Sie, dass es sich bei h_a um einen Isomorphismus handelt. Um welche besondere Abbildung handelt es sich bei h_a in dem Fall, dass R kommutativ ist? *(5)*

Lösung. Wir müssen die Eigenschaften eines Homomorphismus' nachrechnen:

- $h_a(0) = a^{-1} \cdot 0 \cdot a = 0$,
- $h_a(1) = a^{-1} \cdot 1 \cdot a = a^{-1}a = 1$,
- $h_a(-x) = a^{-1}(-x)a = -a^{-1}xa = -h_a(x)$,
- $h_a(x + y) = a^{-1}(x + y)a = a^{-1}xa + a^{-1}ya = h_a(x) + h_a(y)$,
- $h_a(xy) = a^{-1}(xy)a = a^{-1}(xaa^{-1}y)a = (a^{-1}xa)(a^{-1}ya) = h_a(x)h_a(y)$.

Also ist h_a ein Homomorphismus. Die Injektivität folgt aus

$$h_a(x) = h_a(y) \Rightarrow a^{-1}xa = a^{-1}ya \Rightarrow a(a^{-1}xa)a^{-1} = a(a^{-1}ya)a^{-1} \Rightarrow x = y$$

für $x, y \in R$. Für ein $r \in R$ gibt es ein Element x in R, das auf r abgebildet wird, nämlich $x = ara^{-1}$, wie man durch Einsetzen nachrechnet. Daher ist h_a auch surjektiv und insgesamt bijektiv. Falls R kommutativ ist, gilt offenbar $h_a(x) = a^{-1}xa = a^{-1}ax = x$; wir erhalten also in diesem Fall die Identität. □