Lösungen zur

Modulprüfung zur Elementaren Algebra/Zahlentheorie II

Weiterbildung für Lehrer an der FU

Dozent: V.Schulze

Datum: 13 . 12 . 2019 Bearbeitungszeit: 90 Minuten

Name	Vorname	Unterschrift	Matr.Nr.

Aufgabe	1	2	3	4		Punktsumme	Note
Punkte							

Bearbeiten Sie drei der folgenden vier Aufgaben.
Anmerkung: Pro Aufgabenteil werden maximal 5 Punkte vergeben,
pro Aufgabe also maximal 10 Punkte; insgesamt also maximal 30 Punkte.
Zur vollständigen Bearbeitung einer Aufgabe gehört auch die stilistisch einwandfreie Darstellung des Gedankenganges.

Aufgabe 1

(i) Auf $\mathbb{Z}$ sei die Verknüpfung $\bigoplus$ definiert durch
$a \bigoplus b := 2 \cdot a + 2 \cdot b$ für alle $a, b \in \mathbb{Z}$.
Ist $(\mathbb{Z}, \bigoplus)$ eine Halbgruppe ?
Man zeige: 0 ist nicht neutrales Element von $(\mathbb{Z}, \bigoplus)$.
(ii) Gegeben sei die Permutation $\pi := (1,4)(2,3,1)$ aus der symmetrischen Gruppe vom Index 4.
Man stelle π als Produkt elementefremder Zyklen dar.
Sei U die von π erzeugte Untergruppe der symmetrischen Gruppe vom Index 4.
Man gebe eine Untergruppe N der Ordnung 2 von U an.
Ist N Normalteiler von U ?

Lösung

(i) Es gilt $(a \bigoplus b) \bigoplus c = (2 \cdot a + 2 \cdot b) \bigoplus c = 2 \cdot (2 \cdot a + 2 \cdot b) + 2 \cdot c$ und
$a \bigoplus (b \bigoplus c) = a \bigoplus (2 \cdot b + 2 \cdot c)) = 2 \cdot a + 2 \cdot (2 \cdot b + 2 \cdot c)$.
Für $a = 1, b = c = 0$ ergeben sich zum Beispiel verschiedene Ergebnisse.
Also ist $\bigoplus$ nicht assoziativ und $(\mathbb{Z}, \bigoplus)$ keine Halbgruppe.
Es gilt $0 \bigoplus b = 2 \cdot b \neq b$, falls $b \neq 0$. Also ist 0 nicht neutrales Element.
(ii) Es gilt $\pi = (1,2,3,4)$.
Es gilt $U = \{id, \pi, \pi^2, \pi^3\}$ und $N = \{id, \pi^2\}$ ist die gesuchte Untergruppe.

Ferner ist N Normalteiler in U, da der Index von N in U gleich 2 ist.
Man kann auch wie folgt argumentieren: Da U abelsche Untergruppe ist, ist jede Untergruppe von U Normalteiler von U.

Aufgabe 2

Die Teilmenge R von $\mathbb{Q}$ sei definiert durch
$R := \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}, b\, ungerade,\ ggT(a,b) = 1\}$.
(i) Man zeige: R ist Untergruppe von $(\mathbb{Q}, +)$.
Man zeige: R ist Unterring von $(\mathbb{Q}, +, \cdot)$.
(ii) Die Abbildung $f : \mathbb{Z} \longrightarrow \mathbb{Q}$ sei definiert durch $f(z) := \frac{z}{2}$ für alle $z \in \mathbb{Z}$.
Ist f relationstreu bezüglich + ?
Ist f ein Ringhomomorphismus ?

Lösung

(i)Folgendes ist leicht nachzurechnen.
Die Summe zweier Elemente aus R liegt wieder in R.
Das neutrale Element 0 liegt in R.
Mit einem Element liegt auch das Negative in R.
Also ist R Untergruppe.
Das Produkt zweier Elemente aus R liegt wieder in R.
Also ist $(R, \cdot)$ Halbgruppe.
Zusammen folgt: R ist Unterring.
(ii) Es gilt $f(a + b) = \frac{a+b}{2} = \frac{a}{2} + \frac{b}{2} = f(a) + f(b)$ für alle $a, b \in \mathbb{Z}$.
Also ist f relationstreu bezüglich + .
Es gilt $f(a \cdot b) = \frac{a \cdot b}{2}$,
$f(a) \cdot f(b) = \frac{a}{2} \cdot \frac{b}{2} = \frac{a \cdot b}{4}$ für alle $a, b \in \mathbb{Z}$.
Zum Beispiel für $a = b = 1$ ergeben sich unterschiedliche Ergebnisse.
Also ist f nicht relationstreu bezüglich $\cdot$ und f ist kein Ringhomomorphismus.

Aufgabe 3

(i) Läßt sich mit Hilfe der Dreierprobe entscheiden, ob die Gleichung $5381 \cdot 111 - 771^2 = 0$ richtig ist ?
Läßt sich mit Hilfe der Neunerprobe entscheiden, ob die Gleichung $5381 \cdot 111 - 771^2 = 0$ richtig ist ?
Ist $5381 \cdot 111 - 771^2$ durch 11 teilbar ?
(ii) Man zeige : Die Kongruenz $x^3 \equiv 3(mod 7)$ ist nicht lösbar.
Ist $x^{21} \equiv 10(mod 7)$ lösbar ?

Lösung

(i) Wir ersetzen die Zahlen durch ihre Quersumme und rechnen $mod 3$.
Es gilt $17 \cdot 3 - 15 \cdot 15 \equiv 0(mod 3)$

Also läßt sich mit Hilfe der Dreierprobe nicht entscheiden, ob die Gleichung $5381 \cdot 111 - 771^2 = 0$ richtig ist. Klar ist nur: Die Zahl auf der linken Seite ist Vielfaches von 3.
Wir ersetzen die Zahlen durch ihre Quersumme und rechnen $mod 9$.
Es gilt $17 \cdot 3 - 15 \cdot 15 \equiv 6 \not\equiv 0 (mod 9)$.
Aus der Neunerprobe folgt also: Die Gleichung kann nicht richtig sein.
Wir ersetzen die Zahlen durch ihre alternierende Quersumme und rechnen $mod 11$.
Es gilt $(1 - 8 + 3 - 5) \cdot (1 - 1 + 1) - (1 - 7 + 7) \cdot (1 - 7 + 7) \equiv 1 (mod 11)$.
Also ist $5381 \cdot 111 - 771^2 \equiv 1 (mod 11)$.
Es folgt: $5381 \cdot 111 - 771^2$ ist nicht durch 11 teilbar.
(ii) Die Behauptung ergibt sich durch das Einsetzen der Zahlen $0, 1, 2, 3, 4, 5, 6$.
Offenbar ist 0 keine Lösung.
Für $a \not\equiv 0 (mod 7)$ gilt nach Fermat $a^{21} \equiv a^3 (mod 7)$.
Ferner gilt $3 \equiv 10 (mod 7)$.
Also ist auch $x^{21} \equiv 10 (mod 7)$ nicht lösbar.

Aufgabe 4

(i) Man zeige : $f(x) := x^3 + 25 \cdot x - 5 \in \mathbb{Q}[x]$ ist irreduzibel.
Sei $\alpha \in \mathbb{R}$ Nullstelle von $f(x)$.
Man gebe eine Basis der Körpererweiterung $\mathbb{Q}(\alpha) : \mathbb{Q}$ an.
(ii) Man zeige : $g(x) := x^3 + 25 \cdot x - 5 \in \mathbb{Z}_2[x]$ ist irreduzibel.
Sei α Nullstelle von $g(x)$ in einer Körpererweiterung von $\mathbb{Z}_2$.
Wie viel Elemente besitzt der Körper $\mathbb{Z}_2(\alpha)$?

Lösung

(i)Das Polynom $f(x) := x^3 + 25 \cdot x - 5 \in \mathbb{Z}[x]$ ist irreduzibel nach Eisenstein (wähle $p = 5$).
Nach Vorlesung ist dann auch $f(x) := x^3 + 25 \cdot x - 5 \in \mathbb{Q}[x]$ irreduzibel.
(Alternativ: Das Polynom hat in $\mathbb{Q}$ keine Nullstelle, als Nullstelle kommen nur die Teiler von -5 in Frage,also nur $1, -1, 5, -5$).
Dann ist $f(x)$ das Minimalpolynom von α über $\mathbb{Q}$.
Da $f(x)$ den Grad 3 besitzt, gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ und $\{1, \alpha, \alpha^2\}$ ist eine Basis der Körpererweiterung $\mathbb{Q}(\alpha) : \mathbb{Q}$.
(ii) Durch Einsetzen von $0, 1$, ergibt sich: $g(x) := x^3+25 \cdot x-5 \in \mathbb{Z}_2[x]$ hat in $\mathbb{Z}_2$ keine Nullstelle. Da $g(x)$ den Grad 3 besitzt folgt: $g(x) := x^3+25 \cdot x-5 \in \mathbb{Z}_2[x]$ ist irreduzibel.
Dann ist $g(x)$ das Minimalpolynom von α über $\mathbb{Z}_2$.
Es fogt $[\mathbb{Z}_2(\alpha) : \mathbb{Z}_2] = 3$.

Also besitzt $\mathbb{Z}_2(\alpha) : \mathbb{Z}_2$ eine Basis mit 3 Elementen, die Anzahl der möglichen Linearkombinationen der Basisvektoren ist also 2^3.
Der Körper $\mathbb{Z}_3(\alpha)$ besitzt also genau 2^3 Elemente.