Lösungen zur
Modulprüfung zur
Elementaren Algebra/Zahlentheorie II

Weiterbildung für Lehrer an der FU
Dozent: V.Schulze
Datum: 13.12.2018 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

Gegeben seien die beiden Permutationen $\pi := (1,2,3,4)$, $\sigma := (2,4)$ und die Untergruppe $G := \{id, \pi, \pi^2, \pi^3, \sigma, \sigma \circ \pi, \sigma \circ \pi^2, \sigma \circ \pi^3\}$ der symmetrischen Gruppe S_4 vom Index 4.
(i) Man zeige: $\sigma \circ \pi \neq \pi \circ \sigma$.
Ist die von π erzeugte Untergruppe $\{id, \pi, \pi^2, \pi^3\}$ von G
Normalteiler von G?
(ii) Man betrachte die Untergrupe $U := \{id, \sigma\}$ von G.
Man zeige: $\sigma \circ \pi \notin \pi \circ U$.
Ist U Normalteiler in G ?

Lösung

(i) Es gilt $\sigma \circ \pi = (1,4)(2,3) \neq \pi \circ \sigma = (1,2)(4,3)$.
Die von π erzeugte Untergruppe $\{id, \pi, \pi^2, \pi^3\}$ besitzt in G genau zwei Nebenklassen, nach Vorlesung ist sie also Normaleiler in G.
Nach Definition einer Nebenklasse ist $\pi \circ U := \{\pi, \pi \circ \sigma\}$.
Nach (i) ist $\sigma \circ \pi \neq \pi \circ \sigma$.
Ferner gilt $\sigma \circ \pi = (1,4)(2,3) \neq \pi$.
Damit folgt $\sigma \circ \pi \notin \pi \circ U$.
Wegen $\sigma \circ \pi \notin \pi \circ U$, aber $\sigma \circ \pi \in U \circ \pi$ ist $\pi \circ U \neq \circ U\pi$.

Also ist U nicht Normalteilervon G.

Aufgabe 2

Der Unterring $\mathbb{Q}[\sqrt{5}]$ von $\mathbb{R}$ sei definiert durch $\mathbb{Q}[\sqrt{5}] := \{a+b\sqrt{5} \mid a, b \in \mathbb{Q}\}$.
Der Unterring $\mathbb{Q}[\sqrt{-5}]$ von $\mathbb{C}$ sei definiert durch
$\mathbb{Q}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Q}\}$.
Sei $f : \mathbb{Q}[\sqrt{5}] \longrightarrow \mathbb{Q}[\sqrt{-5}]$ definiert durch $f(a+b\sqrt{5}) := (a-b)+(a-b)\sqrt{-5}$ für alle $a, b \in \mathbb{Q}$.
(i) Man zeige: f ist bezüglich + ein Gruppenhomomorphismus.
Ist f auch ein Ringhomomorphismus ?
(ii) Man bestimme den Kern des Gruppenhomomorphismus f .
Ist f surjektiv ?

Lösung

(i)Für alle $a, b, c, d \in \mathbb{Q}$ gilt
$f((a + b\sqrt{5}) + (c + d\sqrt{5})) = (a + c - b - d) + (a + c - b - d)\sqrt{-5}) = f(a + b\sqrt{5}) + f(c + d\sqrt{5}) = (a - b) + (a - b)\sqrt{-5}) + (c - d) + (c - d)\sqrt{-5}$.
Also ist f relationstreu bzgl. + , also ein Gruppenhomomorphismus .
Es gilt $f(\sqrt{5} \cdot \sqrt{5}) = f(5) = 5 + 5 \cdot \sqrt{-5}$.
Andererseits ist $f(\sqrt{5}) \cdot f(\sqrt{5}) = (-1 - \sqrt{-5}) \cdot (-1 - \sqrt{-5}) = -4 + 2 \cdot \sqrt{-5}$.
Also ist f nicht rlationstreu bezüglich $\cdot$ und damit auch kein Ringhomomorphismus.
(ii) Es gilt $Kern(f) := \{a + b\sqrt{5} | f(a + b\sqrt{5}) = 0\} = \{a + a\sqrt{5}| \mid a \in \mathbb{Q}\}$.
f ist nicht surjektiv, da zum Beispiel $1 \in \mathbb{Q}[\sqrt{-5}]$ nicht als Bild eines Elementes aus $\mathbb{Q}[\sqrt{5}]$ auftritt.

Aufgabe 3

(i) Man zeige: Die Kongruenz $5x \equiv 1(mod 62)$ ist lösbar.
Man bestimme eine Lösung der Kongruenz $5x \equiv 1(mod 62)$.
Man bestimme die Ordnung von $5(mod 62)$ im Restklassenring $\mathbb{Z}_{62}$.
(ii) Man zeige: $x^2 \equiv -1(mod 7)$ ist nicht lösbar.
Ist die Kongruenz $x^6 \equiv -1(mod 7)$ lösbar ?

Lösung

Wegen $ggT(5, 62) = 1$ ist $5x \equiv 1(mod 62)$ lösbar.
Eine Lösung wird mit Hilfe des Euklidischen Algorithmus bestimmt.
Es gilt $62 = 12 \cdot 5 + 2; 5 = 2 \cdot 2 + 1$;
also $1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (62 - 12 \cdot 5) = 25 \cdot 5 - 2 \cdot 62$.
Modulo 62 ergibt sich $5 \cdot 25 \equiv 1(mod 62)$, also ist 25 eine Lösung der Kongruenz $5x \equiv 1(mod 62)$.
Ferner sind $1(mod 62), 5(mod 62), 5^2(mod 62)$ in $\mathbb{Z}_{62}$ paarweise verschieden, und es gilt $5^3(mod 62) = 1(mod 62)$.

Also besitzt $5(mod62)$ im Restklassenring $\mathbb{Z}_{62}$ die Ordnung 3.
(ii) Die Kongruenz $x^2 \equiv -1(mod7)$ ist nicht lösbar, da $1, 2, 3, 4, 5, 6$ keine Lösungen sind.
Ist x_0 eine Lösung von $x^6 \equiv -1(mod7)$, so ist x_0^3 eine Lösung von $x^2 \equiv -1(mod7)$.
Also ist die Kongruenz $x^6 \equiv -1(mod7)$ nicht lösbar.

Aufgabe 4

(i)Sei $\alpha \in \mathbb{C}$ Nullstelle von $x^3 + 3x - 1 \in \mathbb{Q}[x]$.
Man zeige: $\{1, \alpha, \alpha^2\}$ ist eine Basis von $\mathbb{Q}(\alpha) : \mathbb{Q}$.
Ist $\alpha^2 + 3$ zu α in $\mathbb{Q}(\alpha)$ multiplikativ invers ?
(ii) Sei E ein Erweiterungskörper von $\mathbb{Z}_2$ und $\beta \in E$ Nullstelle von $x^3 + 3x - 1 \in \mathbb{Z}_2[x]$.
Ist $\{1, \beta, \beta^2\}$ eine Basis von $\mathbb{Z}_2(\beta)$?

Lösung

(i) Das Polynom $x^3 + 3x - 1$ besitzt in $\mathbb{Q}$ keine Nullstelle, denn als mögliche Nullstellen kommen nach Vorlesung nur Teiler von -1, also nur $1, -1$ in Frage.
Also ist nach Vorlesung $\{1, \alpha, \alpha^2\}$ ist eine Basis von $\mathbb{Q}(\alpha) : \mathbb{Q}$.
Da α Nullstelle von $x^3 + 3x - 1$ ist, folgt $(\alpha^2 + 3) \cdot \alpha = 1$.
Also ist $\alpha^2 + 3$ zu α in $\mathbb{Q}(\alpha)$ multiplikativ invers.
(ii) Offenbar sind 0 und 1 keine Nullstelle von $x^3 + 3x - 1 \in \mathbb{Z}_2[x]$.
Da $x^3 + 3x - 1 \in \mathbb{Z}_2[x]$ in $\mathbb{Z}_2$ keine Nullstelle hat, ist das Polynom $x^3 + 3x - 1 \in \mathbb{Z}_2[x]$ irreduzibel und $\{1, \beta, \beta^2\}$ ist eine Basis von $\mathbb{Z}_2(\beta)$.