Lösungen zur Modulprüfung zur Elementaren Algebra/Zahlentheorie II

Weiterbildung für Lehrer an der FU

Dozent: V.Schulze   Datum: 18.1.2018   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

Die Permutation π aus der symmetrischen Gruppe S_5 sei definiert durch $\pi := (1, 3, 5)$.
(i) Man zeige: $U := \{id, \pi, \pi^2\}$ ist die kleinste Untergruppe der symmetrischen Gruppe S_5, die π enthält.
Man bestimme die Elemente der Nebenklasse $(1, 2) \circ U$.
(ii) Man zeige: $\pi \circ (1, 2) \notin (1, 2) \circ U$.
Ist U Normalteiler in S_5 ?

Lösung zu Aufgabe 1

(i) Eine Untergruppe, die π enthält, enthält als Halbgruppe auch π^2 und jede Untergruppe enthält id.
Es bleibt zu zeigen: U ist Untergruppe.
Wegen $\pi^3 = id$ ist U die von π erzeugte Untergruppe.
Es gilt $(1, 2) \circ U = \{(1, 2), (1, 2) \circ \pi, (1, 2) \circ \pi^2\} = \{(1, 2), (1, 3, 5, 2), (1, 5, 3, 2)\}$.
(ii) Es gilt $\pi \circ (1, 2) = (1, 2, 3, 5)$.
Nach (i) folgt $\pi \circ (1, 2) \notin (1, 2) \circ U$.
Wegen $\pi \circ (1, 2) \in U \circ (1, 2)$ folgt $U \circ (1, 2) \neq (1, 2) \circ U$.
Also ist U nicht Normalteiler in S_5.

Aufgabe 2

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

Lösung zu Aufgabe 2

(i) $f((a + b\sqrt{5}) + (c + d\sqrt{5})) = f((a + c) + (b + d)\sqrt{5}) = a + c = f(a + b\sqrt{5}) + f(c + d\sqrt{5})$.
f ist kein Ringhomomorphismus; zum Beispiel gilt $f(\sqrt{5}\sqrt{5}) = f(5) = 5, f(\sqrt{5})f(\sqrt{5}) = 0$.
(ii) f ist surjektiv, da a ein Urbild von a ist.
Es gilt $Kern f = \{b\sqrt{5} \mid b \in \mathbb{Z}\}$.

Aufgabe 3

(i) Man zeige: $x^3 + x + 1 \equiv 0 (mod 5)$ ist nicht lösbar.
Ist $x^3 + x + 1 \equiv 0 (mod 135)$ lösbar?
Ist $x^3 + x + 1 = 5y^2$ in $\mathbb{Z}$ lösbar?
(ii) Man zeige: $5104x \equiv 1 (mod 10209)$ ist lösbar.
Man bestimme eine Lösung a der Kongruenz mit geradem a .
Man bestimme eine Lösung a der Kongruenz mit ungeradem a .

Lösung zu Aufgabe 3

(i) Durch Einsetzen der Werte $0, 1, 2, 3, 4$ erhält man keine Lösung.
$x^3 + x + 1 \equiv 0 (mod 135)$ ist nicht lösbar, eine Lösung wäre ja auch Lösung von $x^3 + x + 1 \equiv 0 (mod 5)$.
$x^3 + x + 1 = 5y^2$ ist in $\mathbb{Z}$ nicht lösbar, eine Lösung wäre ja auch Lösung von $x^3 + x + 1 \equiv 0 (mod 5)$.
(ii) Es gilt $10209 = 2 \cdot 5104 + 1$.
Also ist -2 eine Lösung.
Dann ist auch $-2 + 10209$ eine Lösung.

Aufgabe 4

(i) Man zeige: $x^3 + 2x + 2 \in \mathbb{Q}[x]$ ist irreduzibel .
Ist $x^3 + 2x + 2 \in \mathbb{Z}_2[x]$ irreduzibel ?
(ii) Sei $\alpha \in \mathbb{R}$ Nullstelle von $x^3 + 2x + 2 \in \mathbb{Q}[x]$.
Man gebe eine Basis von $\mathbb{Q}(\alpha) : \mathbb{Q}$ an.
Ist $\{1, \alpha, \alpha^3\}$ eine Basis von $\mathbb{Q}(\alpha) : \mathbb{Q}$?

Lösung zu Aufgabe 4

(i)$x^3 + 2x + 2 \in \mathbb{Z}[x]$ ist irreduzibel nach Eisenstein (wähle $p = 2$), nach Vorlesung ist dann auch $x^3 + 2x + 2 \in \mathbb{Q}[x]$ irreduzibel.
Zum Beweis kann man auch zeigen: $x^3 + 2x + 2$ hat in $\mathbb{Q}$ keine Nullstelle.Nach Vorlesung sind mögliche rationale Nullstellen in $\mathbb{Z}$ und Teiler von 2, also $1, -1, 2, -2$. Durch Einsetzen sieht man, daß dies keine Nullstellen sind.
$x^3 + 2x + 2 \in \mathbb{Z}_2[x]$ hat 0 als Nullstelle, ist also nicht irreduzibel.
(ii) Da $x^3 + 2x + 2 \in \mathbb{Q}[x]$ nach (i) irreduzibel ist, folgt aus der Vorlesung: Eine Basis ist $\{1, \alpha, \alpha^2\}$.
Wegen $\alpha^3 = -2\alpha - 2$ ist $\{1, \alpha, \alpha^3\}$ nicht linear unabhängig, also auch keine Basis.