Lösungen zur
Modulprüfung zur
Elementaren Algebra/Zahlentheorie II

Weiterbildung für Lehrer an der FU

Dozent: V.Schulze Datum: 5.1.2017 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 Permutationen $\pi_1 := (1,2)(3,4), \pi_2 := (1,3)(2,4), \pi_3 := (1,4)(2,3)$ und die Identität id aus der symmetrischen Gruppe $(S_4, \circ)$.
Es sei $U := \{id, \pi_1, \pi_2, \pi_3\}$.
(i) Man ergänze die folgende Verknüpfungstafel:

$\circ$	id	π_1	π_2	π_3
id	id	π_1	π_2	π_3
π_1	π_1	id	π_3	
π_2	π_2		id	π_1
π_3	π_3	π_2	π_1	

Man zeige: $(U, \circ)$ ist eine Halbgruppe.
Man zeige: $(U, \circ)$ ist eine Untergruppe von S_4.
(ii) Man zeige: Die von $(1,2,3)$ erzeugte Linksnebenklasse von U ist gleich der von $(1,2,3)$ erzeugten Rechtsnebenklasse von U.
Ist U Normalteiler in der alternierenden Gruppe A_4 vom Index 4 ?

Lösung

(i)Die Verknüpfungstafel lautet:

$\circ$	id	π_1	π_2	π_3
id	id	π_1	π_2	π_3
π_1	π_1	id	π_3	π_2
π_2	π_2	π_3	id	π_1
π_3	π_3	π_2	π_1	id

Die Hintereinanderschaltung von Abbildungen ist stets assoziativ.
Das Verknüpfungsergebnis zweier Elemente aus U liegt nach der Verknüpfungstafel stets wieder in U .
Also ist $(U, \circ)$ Halbgruppe.
In jeder Zeile und jeder Spalte der Verknüpfungstafel tritt jedes Element aus U auf.
Also ist $(U, \circ)$ Untergruppe von S_4.
(ii) Es gilt $(1,2,3) \circ U = \{(1,2,3) \circ id, (1,2,3) \circ \pi_1, (1,2,3) \circ \pi_2, (1,2,3) \circ \pi_3\} = \{(1,2,3), (1,3,4), (2,4,3), (1,4,2)\}$,
$U \circ (1,2,3) = \{(1,2,3), (2,4,3), (1,4,2), (1,3,4)\}$.
Nach Lagrange besitzt U in A_4 drei Nebenklassen. Da zwei der Rechts- und Linksnebenklassen gleich sind , gilt dies auch für die dritte Nebenklasse.
Also ist U Normalteiler in A_4 .

Aufgabe 2

Es sei $f(x) := x^5 + 4x^3 - 10 \in \mathbb{Q}[x]$ und α eine reelle Nullstelle von $f(x)$.
(i)Man zeige: $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ ist eine Basis von $\mathbb{Q}(\alpha) : \mathbb{Q}$.
Ist $\frac{\alpha^2+4}{10}$ zu α^3 multiplikativ invers?
(ii) Ist α bei gegebener Einheitsstrecke mit Zirkel und Lineal konstruierbar?
Ist $\frac{1}{\sqrt{\alpha}} + 1$ bei gegebener Einheitsstrecke mit Zirkel und Lineal konstruierbar?

Lösung

Es handelt sich um eine Basis, da das Polynom $f(x)$ nach Eisenstein in $\mathbb{Z}[x]$ (wähle $p = 2$) irreduzibel ist, also auch in $\mathbb{Q}[x]$.
Es gilt $\alpha^3 \frac{\alpha^2+4}{10} = \frac{\alpha^5+4\alpha^3}{10} = 1$. Das letzte Gleichheitszeichen ergibt sich, da α Nullstelle von $f(x)$ ist.
(ii) Da $f(x)$ in $\mathbb{Q}[x]$ irreduzibel ist, folgt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. Der Grad ist nicht Potenz von 2, also ist α nicht konstruierbar.
Annahme: $\frac{1}{\sqrt{\alpha}} + 1$ ist bei gegebener Einheitsstrecke mit Zirkel und Lineal konstruierbar. Dann ist auch α konstruierbar. Widerspuch.

Aufgabe 3

Der Ring $\mathbb{Z}[\sqrt{3}]$ sei definiert durch $\mathbb{Z}[\sqrt{3}] := \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$.
(i) Es sei $f : \mathbb{Z}[\sqrt{3}] \to \mathbb{Z}[\sqrt{3}]$ definiert durch $f(a + b\sqrt{3}) := a - b\sqrt{3}$.

Man zeige: f ist bezüglich + ein Gruppen-Homomorphismus.
Ist f auch ein Ring-Homomorphismus ?
(ii) Es sei $g : \mathbb{Z}[\sqrt{3}] \to \mathbb{Z}_3$ definiert durch $g(a + b\sqrt{3}) := a(mod3)$.
Man zeige: g ist bezüglich + ein Gruppen-Homomorphismus.
Ist g auch ein Ring-Homomorphismus ?

Lösung

(i)Es gilt $f((a+b\sqrt{3})+(c+d\sqrt{3})) = f((a+c)+(b+d)\sqrt{3}) = (a+c)-(b+d)\sqrt{3}$.
Es gilt $f((a+b\sqrt{3})+f(c+d\sqrt{3})) = (a-b\sqrt{3})+(c-d\sqrt{3}) = (a+c)-(b+d)\sqrt{3}$.
Also handelt es sich um einen Gruppen-Homomorphismus.
Es gilt $f((a+b\sqrt{3})(c+d\sqrt{3})) = f((ac+3bd)+(ad+cb)\sqrt{3}) = (ac+3bd)-(ad+cb)\sqrt{3}$.
Es gilt $f((a+b\sqrt{3})f((c+d\sqrt{3}) = (a-b\sqrt{3})(c-d\sqrt{3}) = (ac+3bd)-(ad+cb)\sqrt{3}$.
Also handelt es sich um einen Ring-Homomorphismus.
(ii) Es gilt $g((a + b\sqrt{3}) + (c + d\sqrt{3}) = f((a + c) + (b + d)\sqrt{3}) = (a + c)(mod3)$.
Es gilt $f((a + b\sqrt{3}) + f(c + d\sqrt{3})) = a(mod3) + c(mod3) = (a + c)(mod3)$.
Also handelt es sich um einen Gruppen-Homomorphismus.
Es gilt $f((a + b\sqrt{3})(c + d\sqrt{3})) = f((ac + 3bd) + (ad + cb)\sqrt{3}) = ac(mod3)$.
Es gilt $f((a + b\sqrt{3})f((c + d\sqrt{3}) = a(mod3)c(mod3) = ac(mod3)$.
Also handelt es sich um einen Ring-Homomorphismus.

Aufgabe 4

(i) Man zeige: Die Kongruenz $x^2 - 3x + 2 \equiv 0(mod7)$ ist lösbar.
Ist die Kongruenz $3^6x^8 - 3x + 9 \equiv 0(mod7)$ ebenfalls lösbar ?
(ii) Man bestimme eine Lösung der Kongruenz $(x-5)^2 \equiv 2(mod7)$ und verwende das Ergebnis zur Berechnung einer Lösung von $x^2-3x+2 \equiv 0(mod7)$ durch Anwendung der (p,q)-Formel (quadratische Ergänzung).

Lösung

(i) Offenbar ist 1 eine Lösung.
Es gilt $2 \equiv 9(mod7)$ und $3^6 \equiv 1(mod7)$ und nach dem Satz von Fermat ist 1 wieder eine Lösung.
Man kann auch direkt einsetzen.
(ii) Durch probieren ergibt sich 1 als Lösung.
Es gilt $x^2 - 3x + 2 \equiv x^2 - 3x + (4 \cdot 3)^2 - (4 \cdot 3)^2 + 2 \equiv (x - 4 \cdot 3)^2 - (4 \cdot 3)^2 + 2 \equiv (x - 5)^2 - 2(mod7)$, also ist 1 Lösung.