M. Künzer

Algebra für Lehramt, SoSe 20

Scheinklausur

als Hausarbeit

Lösung

Aufgabe 1 (2+2+2 Punkte)

(1) Man bestimme das Minimalpolynom $\mu_{2-\zeta_3,\mathbb{Q}}(X) \in \mathbb{Q}[X]$.

(2) Man bestimme $(2-\zeta_3)^{-1}$ in $\mathbb{Q}(\zeta_3)$.

(3) Man finde eine Primfaktorzerlegung von 7 in $\mathbb{Z}[\zeta_3]$.

Lösung. Wir schreiben $\zeta := \zeta_3$. Es ist $0 = \Phi_3(\zeta) = \zeta^2 + \zeta + 1$.

Zu (1). Es ist $(2-\zeta)^2 = \zeta^2 - 4\zeta + 4 = -\zeta - 1 - 4\zeta + 4 = -5\zeta + 3$.

Also ist $(2-\zeta)^2 - 5(2-\zeta) + 7 = 0$.

Da $2 - \zeta \notin \mathbb{Q}$, ist $\deg(\mu_{2-\zeta,\mathbb{Q}}(X)) \geqslant 2$.

Folglich ist $\mu_{2-\zeta,\mathbb{Q}}(X) = X^2 - 5X + 7$.

> Alternativ kann man auch $\mu_{\zeta,\mathbb{Q}}(X) = \Phi_3(X) = X^2 + X + 1$ und $\mu_{2-\zeta,\mathbb{Q}}(X) = \mu_{\zeta,\mathbb{Q}}(2-X) = (2-X)^2 + (2-X) + 1 = X^2 - 5X + 7$ verwenden.

Zu (2). In (1) haben wir $(2-\zeta)^2 - 5(2-\zeta) + 7 = 0$ erhalten. Also wird $(2-\zeta) - 5 = \frac{-7}{\zeta-2}$ und somit $(2-\zeta)^{-1} = \frac{1}{-7}((2-\zeta) - 5) = \frac{1}{7}(\zeta + 3)$.

Zu (3). Dank (2) ist $7 = (\zeta+3)(2-\zeta)$. Es ist $|\zeta+3|^2 = (3+\zeta)(3+\zeta^2) = 7$. Es ist $|2-\zeta|^2 = (2-\zeta)(2-\zeta^2) = 7$. Da $7 \in \mathbb{Z}$ prim ist, sind $\zeta+3$ und $2-\zeta$ in $\mathbb{Z}[\zeta]$ irreduzibel und damit prim. Folglich ist $7 = (\zeta+3)(2-\zeta)$ eine Primfaktorzerlegung.

Aufgabe 2 (1+1+2 Punkte) Sei $G = \mathrm{S}_5$.

(1) Gibt es in G eine zyklische Untergruppe der Ordnung 5?

(2) Gibt es in G eine Untergruppe der Ordnung 8?

(3) Gibt es in G eine abelsche Untergruppe der Ordnung 8?

Lösung.

Zu (1). Ja. Z.B. ist $\langle(1,2,3,4,5)\rangle$ zyklisch von Ordnung 5.

Zu (2). Ja. Es ist $\mathrm{Syl}_2(G) \neq \emptyset$. Und für $P \in \mathrm{Syl}_2(G)$ gilt $|P| = 2^{\mathrm{v}_2(|G|)} = 2^{\mathrm{v}_2(120)} = 2^3 = 8$.

Zu (3). Nein. Es ist $\mathrm{D}_8 = \langle(1,2,3,4),(2,4)\rangle \leqslant \mathrm{S}_4 \leqslant \mathrm{S}_5 = G$. Es ist D_8 nichtabelsch, da ${}^{(2,4)}(1,2,3,4) = (1,4,3,2) \neq (1,2,3,4)$ ist. Eine Untergruppe von Ordnung 8 in G ist eine 2-Sylowgruppe in G, und alle 2-Sylowgruppen in G sind konjugiert, insbesondere isomorph. Somit sind alle Untergruppen von Ordnung 8 in G nichtabelsch.

Aufgabe 3 (1+1+3 Punkte) Sei $G := \langle (1,2,3),\ (4,5) \rangle \leqslant \mathrm{S}_5$.

(1) Man bestimme $|G|$.

(2) Ist $\{1,2,3,4,5\}$ eine transitive G-Menge?

(3) Man bestimme die Bahn $G \cdot 1$.
Man bestimme die Untergruppe $\mathrm{Stab}_G(1)$.
Man bestätige die Aussage des Bahnenlemmas in diesem Fall.

Lösung.

Zu (1). Wir schreiben $a := (1,2,3)$ und $b := (4,5)$. Es ist

$$\begin{array}{rcl} G & = & \{\, a^i b^j \,:\, i \in [0,2],\ j \in [0,1] \,\} \;=\; \{1, a, a^2, b, ab, a^2 b\} \\ & = & \{\mathrm{id}, (1,2,3), (1,3,2), (4,5), (1,2,3)(4,5), (1,3,2)(4,5)\}\ . \end{array}$$

Also ist $|G| = 6$.

Zu (2). Nein. Z.B. gibt es kein $g \in G$ mit $g \cdot 1 = 4$; vgl. (1).

Zu (3). Es ist $G \cdot 1 = \{\, g \cdot 1 \,:\, g \in G \,\} = \{1,2,3,1,2,3\} = \{1,2,3\}$; vgl. (1).

Es ist $\mathrm{Stab}_G(1) = \{\mathrm{id}, (4,5)\}$; vgl. (1).

Die G-Abbildung

$$\begin{array}{rcl} G/\,\mathrm{Stab}_G(1) & \to & G \cdot 1 \\ g\,\mathrm{Stab}_G(1) & \mapsto & g \cdot 1 \end{array}$$

ist bijektiv, da von $G/\,\mathrm{Stab}_G(1) = \{\mathrm{id}\,\mathrm{Stab}_G(1), (1,2,3)\,\mathrm{Stab}_G(1), (1,3,2)\,\mathrm{Stab}_G(1)\}$ nach $G \cdot 1 = \{1,2,3\}$ wie folgt abgebildet wird.

$$\begin{array}{rcll} \mathrm{id}\,\mathrm{Stab}_G(1) & \mapsto & \mathrm{id} \cdot 1 & = \ 1 \\ (1,2,3)\,\mathrm{Stab}_G(1) & \mapsto & (1,2,3) \cdot 1 & = \ 2 \\ (1,3,2)\,\mathrm{Stab}_G(1) & \mapsto & (1,3,2) \cdot 1 & = \ 3 \end{array}$$

Aufgabe 4 (2+3+1 Punkte) Sei G eine Gruppe mit $|G| = 30$. Sei G nicht zyklisch.

(1) Ist G abelsch?

(2) Ist G einfach?

(3) Man gebe ein Beispiel einer nichtabelschen Gruppe von Ordnung 30 an.

Lösung.

Zu (1). *Annahme,* G ist abelsch. Wegen $30 = 2^1 \cdot 3^1 \cdot 5^1$ ist jede Zerlegung von $30 = x_1 \cdot \ldots \cdot x_k$ in $\mathbb{Z}_{\geqslant 1}$, für welche $x_1 \,|\, \ldots \,|\, x_k$ gilt, von der Form $x_1 = \ldots = x_{k-1} = 1$, $x_k = 30$. Also ist G isomorph zu C_{30} . Somit ist G zyklisch, was aber nicht der Fall ist. *Widerspruch.*

Also ist G nicht abelsch.

Zu (2). *Annahme,* G ist einfach.

Es ist $|\,\mathrm{Syl}_5(G)| \equiv_5 1$ und ein Teiler von 6. Da G keine normale 5-Sylowgruppe haben kann wegen G einfach, ist $|\,\mathrm{Syl}_5(G)| = 6$. Da die 5-Sylowgruppen paarweise Schnitt 1 haben, gibt es also $6 \cdot 4 = 24$ Elemente der Ordnung 5 in G.

Es ist $|\operatorname{Syl}_3(G)| \equiv_3 1$ und ein Teiler von 10. Da G keine normale 3-Sylowgruppe haben kann wegen G einfach, ist $|\operatorname{Syl}_3(G)| = 10$. Da die 3-Sylowgruppen paarweise Schnitt 1 haben, gibt es also $10 \cdot 2 = 20$ Elemente der Ordnung 3 in G.

Folglich ist $30 = |G| \geqslant 24 + 20 = 44$. Wir haben einen *Widerspruch.*

Also ist G nicht einfach.

Zu (3). Z.B. ist die Diedergruppe D_{30} nichtabelsch und von Ordnung 30.

Aufgabe 5 (2+2+2 Punkte)

(1) Man finde alle irreduziblen normierten Polynome von Grad 2 in $\mathbb{F}_2[X]$.

(2) Ist $X^4 + X^3 + 1 \in \mathbb{F}_2[X]$ irreduzibel? Man entscheide dies unter Verwendung von (1).

(3) Ist $X^4 + 5X^3 - 7 \in \mathbb{Q}[X]$ irreduzibel? Man entscheide dies unter Verwendung von (2).

Lösung.

Zu (1). Da der konstante Term nicht 0 sein darf, haben wir nur $X^2 + 1$ und $X^2 + X + 1$ auf Irreduzibilität zu untersuchen.

Es ist $X^2 + 1 = (X + 1)^2$ nicht irreduzibel.

Es ist $X^2 + X + 1$ mangels Nullstelle in $\mathbb{F}_2$ irreduzibel.

Also ist $X^2 + X + 1$ das einzige irreduzible normierte Polynome von Grad 2 in $\mathbb{F}_2[X]$.

Zu (2). Es hat $X^4 + X^3 + 1$ keine Nullstelle in $\mathbb{F}_2$, also keinen Faktor von Grad 1.

Bleibt noch die Frage, ob $X^4 + X^3 + 1$ ein Produkt zweier irreduzibler Faktoren von Grad 2 ist.

Dafür gibt es aber nach (1) nur die Möglichkeit $(X^2 + X + 1)^2 = X^4 + X^2 + 1$. Und dieses Polynom ist nicht $X^4 + X^3 + 1$.

Also ist $X^4 + X^3 + 1 \in \mathbb{F}_2[X]$ irreduzibel.

Zu (3). *Annahme,* es zerfällt $X^4 + 5X^3 - 7$ in $\mathbb{Q}[X]$ in die Faktoren

$$X^4 + 5X^3 - 7 \;=\; f(X) \cdot g(X),$$

wobei $f(X),\ g(X) \in \mathbb{Q}[X]$ von Grad $\geqslant 1$ sind.

O.E. sind $f(X)$ und $g(X)$ normiert.

Es sind dann $f(X),\ g(X) \in \mathbb{Z}[X]$.

Wir bilden nun von $\mathbb{Z}[X]$ nach $\mathbb{F}_2[X]$ ab durch koeffizientenweises Bilden von Restklassen modulo 2. Es wird $X^4+5X^3-7 \in \mathbb{Z}[X]$ nach $X^4+5X^3-7 = X^4+X^3+1 \in \mathbb{F}_2[X]$ abgebildet. Das Bild von $f(X) \in \mathbb{Z}[X]$ heiße $\bar{f}(X) \in \mathbb{F}_2[X]$. Das Bild von $f(X) \in \mathbb{Z}[X]$ heiße $\bar{f}(X) \in \mathbb{F}_2[X]$. In $\mathbb{F}_2[X]$ ist dann

$$X^4 + X^3 + 1 \;=\; \bar{f}(X) \cdot \bar{g}(X).$$

Da aber auch $\bar{f}(X)$ und $\bar{g}(X)$ Grad $\geqslant 1$ haben, steht dies im *Widerspruch* zur in (2) festgestellten Irreduzibilität von $X^4 + X^3 + 1 \in \mathbb{F}_2[X]$.

Aufgabe 6 (2+2+1+1+1 Punkte)

(1) Man konstruiere einen Körper K mit $|K| = 25$.

(2) Man finde ein Element $y \in K$ mit $y^5 \neq y$.

(3) In wieviele irreduzible normierte Faktoren zerfällt $X^{24} - 1 \in K[X]$?

(4) Wir erinnern an $\Phi_{12}(X) = X^4 - X^2 + 1$.
In wieviele irreduzible normierte Faktoren zerfällt $X^4 - X^2 + 1 \in K[X]$?

(5) Gibt es in $K[X]$ ein irreduzibles normiertes Polynom von Grad $\geqslant 2$?

Lösung.

Zu (1). Es ist $X^2 - 2 \in \mathbb{F}_5[X]$ mangels Nullstelle irreduzibel. Also ist $K := \mathbb{F}_5[X]/(X^2 - 2)$ ein Körper mit $|K| = 5^2 = 25$.

Schreiben wir $w := X + (X^2 - 2)$, so gilt $w^2 = 2$. Jedes Element von K läßt sich eindeutig schreiben als $a + bw$ mit $a,\, b \in \mathbb{F}_5$.

Zu (2). Sei $y := w$. Es ist $y^5 = (w^2)^2 \cdot w = 4w \neq w = y$.

Zu (3). Es ist $\mathrm{U}(K) = K^\times$ eine Gruppe von Ordnung 24.

Es ist $\mathrm{U}(K) \simeq \mathrm{C}_{24}$, aber so genau brauchen wir es nicht.

Folglich ist $y^{24} = 1$ für $y \in K^\times$. Also jedes Element von $K^\times$ eine Nullstelle von $X^{24} - 1$. Es folgt

$$X^{24} - 1 \;=\; \prod_{y \in K^\times} (X - y)\;.$$

Insbesondere zerfällt $X^{24} - 1$ in $K[X]$ in 24 irreduzible normierte Faktoren von Grad 1.

Zu (4). Es ist $\Phi_{12}(X)$ ein Teiler von $X^{24} - 1$.

Da $X^{24} - 1$ in normierte Faktoren von Grad 1 zerfällt, gilt das auch für $\Phi_{12}(X)$.

Folglich zerfällt $X^4 - X^2 + 1$ in $K[X]$ in 4 irreduzible normierte Faktoren von Grad 1.

Zu (5). Es ist K endlich. Somit ist K nicht algebraisch abgeschlossen. Also gibt es in $K[X]$ ein normiertes irreduzibles Polynom von Grad $\geqslant 2$.

Es hat $X^{25} - X + 1 \in K[X]$ keine Nullstelle. In seiner Zerlegung in irreduzible normierte Faktoren treten also nur irreduzible normierte Polynom von Grad $\geqslant 2$ auf. Tatsächlich zerfällt es in 5 irreduzible normierte Faktoren von Grad 5.