C. Dietzel, M. Künzer

Algebra für Lehramt, SoSe 20

Lösung 8

Aufgabe 29

Man entscheide, ob es eine einfache Gruppe der Ordnung n gibt.

(1) $n = 24$

(2) $n = 23$

(3) $n = 42$

(4) $n = 360$

Lösung zu Aufgabe 29:

(1) *Annahme,* es gibt eine einfache Gruppe G mit $|G| = 24$. Es ist $24 = 2^3 \cdot 3$, folglich gibt es eine 2-Sylowgruppe $P \leqslant G$, welche die Ordnung $|P| = 8$ besitzt. Wir setzen $X = G/P$. Dies ist eine transitive G-Menge (siehe Beispiel 116(3)). Außerdem ist $|X| = \frac{24}{8} = 3$. Daraus erhalten wir einen Gruppenmorphismus $\varphi : G \to \mathrm{S}_X$.

Da X eine nichttriviale G-Menge ist, können wir $\mathrm{Kern}(\varphi) = G$ ausschließen. Da $\mathrm{Kern}(\varphi)$ ein Normalteiler in G ist, kann nur $\mathrm{Kern}(\varphi) = 1$ sein. Damit wäre φ dann aber injektiv, im *Widerspruch* zu $|G| = 24 > 6 = |\mathrm{S}_X|$.

Somit gibt es keine einfache Gruppe der Ordnung 24.

(2) Sei $G = C_{23}$. Für jede Untergruppe $H \leqslant G$ gilt $|H| \mid 23$ nach Lagrange (Lemma 87). Entweder ist also $|H| = 1$ oder $|H| = 23$, sprich: es ist $H = 1$ oder $H = G$. Da diese Folgerung natürlich insbesondere dann gilt, wenn H ein Normalteiler ist, ist G eine einfache Gruppe.

(3) Sei G eine Gruppe mit $|G| = 42$. Wir haben die Faktorisierung $42 = 7 \cdot 6$, woraus wir folgern, dass einerseits $|\mathrm{Syl}_7(G)| \mid 6$ gelten muss, andererseits $|\mathrm{Syl}_7(G)| \equiv_7 1$, was nur möglich ist, wenn $|\mathrm{Syl}_7(G)| = 1$ ist. Nach Korollar 142 gibt es also einen Normalteiler der Ordnung 7 in G, folglich ist G nicht einfach.

(4) Sei $G = \mathrm{A}_6$. Es ist $|G| = \frac{6!}{2} = 360$. Nach Satz 168 ist G eine einfache Gruppe.

Aufgabe 30

(1) Gibt es in A_5 eine Untergruppe der Ordnung 15 ?

(2) Sei G eine Gruppe, in welcher $x^2 = 1$ ist für $x \in G$. Ist G abelsch?

(3) Sei $n \in \mathbb{Z}_{\geqslant 1}$. Ist jede nichtabelsche Gruppe von Ordnung $2n$ isomorph zu D_{2n} ?

(4) Sei $n \in \mathbb{Z}_{\geqslant 5}$. Hat S_n außer 1, A_n und S_n noch weitere Normalteiler?

Lösung zu Aufgabe 30:

(1) *Annahme*, es gibt eine Untergruppe $|H| \leqslant \mathrm{A}_5$ mit $|H| = 15$. Dann ist $X := \mathrm{A}_5/H$ eine transitive A_5-Menge mit $|X| = \frac{|\mathrm{A}_5|}{|H|} = \frac{60}{15} = 4$. Daraus erhalten wir einen nichttrivialen Gruppenmorphismus $\varphi : \mathrm{A}_5 \to \mathrm{S}_X$. Es ist $\mathrm{Kern}(\varphi) \neq \mathrm{A}_5$. Da A_5 einfach ist (Satz 168), muss also $\mathrm{Kern}(\varphi) = 1$ sein. Demzufolge ist φ injektiv, im *Widerspruch* zu $|\mathrm{S}_X| = 24$ und $|\mathrm{A}_5| = 60$.

(2) Eine solche Gruppe ist immer abelsch. Die Gleichung $x^2 = 1$ ist äquivalent zu $x = x^{-1}$. Damit gilt für beliebige $x, y \in G$, dass

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

(3) Nein. Ein Gegenbeispiel der Ordnung $2n = 12$ ist die nichtabelsche Gruppe $G = \mathrm{A}_4$. Diese enthält einen Normalteiler der Ordnung 4, nämlich die Untergruppe

$$V = \langle (1,2)(3,4), (1,3)(2,4) \rangle \trianglelefteqslant G\ .$$

Damit ist $|\,\mathrm{Syl}_2(\mathrm{A}_4)| = 1$. Für die Diedergruppe D_{12} ist hingegen $|\,\mathrm{Syl}_2(\mathrm{D}_{12})| = 3$ (siehe Aufgabe 25).

Folglich sind die Gruppen nicht isomorph zueinander.

(4) Sei $N \trianglelefteqslant \mathrm{S}_n$ ein Normalteiler mit $N \notin \{1, \mathrm{A}_n, \mathrm{S}_n\}$. Dann ist $N \cap \mathrm{A}_n \trianglelefteqslant \mathrm{A}_n$, was aber nur möglich ist, wenn $N \cap \mathrm{A}_n = 1$ oder $N \cap \mathrm{A}_n = \mathrm{A}_n$ ist.

Ist $N \cap \mathrm{A}_n = \mathrm{A}_n$, so gilt $\mathrm{A}_n \leqslant N \leqslant \mathrm{S}_n$. Aus dem Satz von Lagrange folgen die Teilbarkeiten $\frac{n!}{2} \mid |N|$ und $|N| \mid n!$, die nur mit $|N| = \frac{n!}{2}$ oder $|N| = n!$ erfüllbar sind, d.h. mit $N = \mathrm{A}_n$ oder $N = \mathrm{S}_n$.

Im Fall, dass $N \cap \mathrm{A}_n = 1$ ist, gilt

$$|\mathrm{A}_n N| = \frac{|\mathrm{A}_n| \cdot |N|}{|N \cap \mathrm{A}_n|} = \frac{n!}{2} \cdot |N| \ \mid\ n! = |\mathrm{S}_n|\,.$$

Ist $N \neq 1$, so muss $|N| = 2$ sein. Dann enthält N ein eindeutiges nichttrivales Element π, welches Ordnung 2 hat. Es hat π in Zykelschreibweise mindestens einen Zykel der Länge 2. Sei (k_1, k_2) ein solcher Zykel. Da $n \geqslant 3$ ist, können wir ein Element $f \in \mathrm{S}_n$ wählen mit $f(k_1) = k_1$ und $f(k_2) \neq k_2$. Dann enthält ${}^f\pi$ den Zykel $(f(k_1), f(k_2)) = (k_1, f(k_2)) \neq (k_1, k_2)$. Damit muss aber ${}^f\pi \notin N$ sein. Folglich kann es keinen solchen Normalteiler geben.

Somit umfasst die Menge $\{1, \mathrm{A}_n, \mathrm{S}_n\}$ bereits alle Normalteiler in S_n.

Aufgabe 31

Wir betrachten die Körpererweiterung $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$.

(1) Man bestimme das Minimalpolynom $\mu_{\sqrt{2},\mathbb{Q}}(X)$.
Man bestimme eine $\mathbb{Q}$-lineare Basis von $\mathbb{Q}(\sqrt{2})$.
Man bestimme den Grad $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ der Körpererweiterung.

(2) Man bestimme ein Ideal $I \trianglelefteqslant \mathbb{Q}[X]$ mit $\mathbb{Q}[X]/I \simeq \mathbb{Q}(\sqrt{2})$.

(3) Sei $c := a_0 + a_1\sqrt{2}$, wobei $a_0\,,\ a_1 \in \mathbb{Q}$. Falls $c \neq 0$ ist, so berechne man c^{-1}.
Hinweis: $(a_0 + a_1\sqrt{2})(a_0 - a_1\sqrt{2}) = a_0^2 - 2a_1^2$.

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

Lösung zu Aufgabe 31:

(1) Wir bestimmen zunächst $\mu_{\sqrt{2},\mathbb{Q}}(X)$. Es ist $\sqrt{2} \notin \mathbb{Q}$, somit muss $\deg(\mu_{\sqrt{2},\mathbb{Q}}(X)) > 1$ sein. Da $\sqrt{2}^2 = 2$ bzw. $\sqrt{2}^2 - 2 = 0$ ist, ist $\sqrt{2}$ eine Nullstelle des normierten Polynoms $X^2 - 2$. Da es kein Polynom kleineren Grades über $\mathbb{Q}$ mit $\sqrt{2}$ als Nullstelle gibt, folgt mit Bemerkung 184, dass $\mu_{\sqrt{2},\mathbb{Q}}(X) = X^2 - 2$ ist.

Es ist $\deg(\mu_{\sqrt{2},\mathbb{Q}}(X)) = 2$.

Nach Lemma 182 ist $\{\sqrt{2}^0, \sqrt{2}^1\} = \{1, \sqrt{2}\}$ eine $\mathbb{Q}$-lineare Basis von $\mathbb{Q}(\sqrt{2})$. Nach dem selben Lemma ist auch $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = n = 2$.

(2) Nach Teil (1) der Aufgabe und Beispiel 187 ist

$$\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[X]/(\mu_{\sqrt{2},\mathbb{Q}}(X)) = \mathbb{Q}[X]/(X^2 - 2).$$

(3) Da $1, \sqrt{2}$ linear unabhängig über $\mathbb{Q}$ sind (Teil (1) der Aufgabe), ist $a_0 + a_1\sqrt{2} = 0$ nur dann, wenn $a_0 = a_1 = 0$.

Ist $c = a_0 + a_1\sqrt{2} \neq 0$, so ist also auch $a_0 - a_1\sqrt{2} \neq 0$. Demzufolge ist

$$(a_0 + a_1\sqrt{2})(a_0 - a_1\sqrt{2}) = a_0^2 - 2a_1^2 \neq 0.$$

Außerdem ist $a_0^2 - 2a_1^2 \in \mathbb{Q}$. Wir dürfen also im Folgenden durch dieses Element teilen.

$$(a_0 + a_1\sqrt{2})(a_0 - a_1\sqrt{2}) = a_0^2 - 2a_1^2 \qquad | \cdot \frac{1}{a_0^2 - 2a_1^2}$$

$$\Rightarrow (a_0 + a_1\sqrt{2}) \cdot \left(\frac{a_0}{a_0^2 - 2a_1^2} - \frac{a_1}{a_0^2 - 2a_1^2}\sqrt{2} \right) = 1$$

$$\Rightarrow (a_0 + a_1\sqrt{2})^{-1} = \left(\frac{a_0}{a_0^2 - 2a_1^2} - \frac{a_1}{a_0^2 - 2a_1^2}\sqrt{2} \right).$$

(4) Da $1 - 2\sqrt{2} \notin \mathbb{Q}$ ist, muss $\deg(\mu_{1-2\sqrt{2},\mathbb{Q}}(X)) > 1$ sein. Setzen wir $x := 1 - 2\sqrt{2}$, so haben wir

$$x - 1 = 2\sqrt{2} \rightsquigarrow (x-1)^2 = (2\sqrt{2})^2 = 8 \rightsquigarrow (x-1)^2 - 8 = x^2 - 2x - 7 = 0.$$

Also ist $1 - 2\sqrt{2}$ eine Nullstelle des Polynoms $X^2 - 2X - 7$. Ein Polynom kleineren Grades mit dieser Nullstelle gibt es nicht. Also ist $\mu_{1-2\sqrt{2},\mathbb{Q}}(X) = X^2 - 2X - 7$.

Aufgabe 32

(1) Man konstruiere einen Körper $\mathbb{F}_9$ mit 9 Elementen. (Vorsicht: $\mathbb{Z}/(9)$ ist kein Körper.)

(2) Man erstelle die Additionstafel von $\mathbb{F}_9$.

(3) Man erstelle die Multiplikationstafel von $\mathbb{F}_9$.

(4) Man gebe zu jedem Element in $\mathbb{F}_9^\times$ das multiplikativ Inverse an.

Lösung zu Aufgabe 32:

(1) Wir konstruieren uns einen Körper $\mathbb{F}_9$ als Körpererweiterung von $\mathbb{F}_3$.

Das Polynom $p(X) = X^2 + 1 \in \mathbb{F}_3[X]$ ist irreduzibel – jeder nichttriviale Teiler von $p(X)$ wäre ein Linearfaktor, $p(X)$ besitzt aber keine Nullstellen in $\mathbb{F}_3$.

Wir bilden nun $L := \mathbb{F}_3[X]/(p(X))$. Lemma 183 garantiert uns, dass $L|\mathbb{F}_3$ in der Tat eine Körpererweiterung ist. Setzen wir $\iota := X + (p(X))$, so haben wir nach demselben Lemma $L = \mathbb{F}_3(\iota)$ und $\mu_{\iota,\mathbb{F}_3}(X) = X^2 + 1$. Es ist also $[L : \mathbb{F}_3] = 2$, woraus $|L| = 9$ folgt.

Wir können also $\mathbb{F}_9 := L$ setzen.

(2) Es ist $\deg(\mu_{\iota,\mathbb{F}_3}(X)) = 2$. Wir können also jedes Element von $\mathbb{F}_9$ eindeutig darstellen als $a + b\iota$ mit $a, b \in \mathbb{F}_3$ (Lemma 182).

Die Addition in dieser Darstellung erfolgt koeffizientenweise; eine Additionstabelle ist also gegeben durch:

$(+)$	0	1	-1	ι	$1+\iota$	$-1+\iota$	$-\iota$	$1-\iota$	$-1-\iota$
0	0	1	-1	ι	$1+\iota$	$-1+\iota$	$-\iota$	$1-\iota$	$-1-\iota$
1	1	-1	0	$1+\iota$	$-1+\iota$	ι	$1-\iota$	$-1-\iota$	$-\iota$
-1	-1	0	1	$-1+\iota$	ι	$1+\iota$	$-1-\iota$	$-\iota$	$1-\iota$
ι	ι	$1+\iota$	$-1+\iota$	$-\iota$	$1-\iota$	$-1-\iota$	0	1	-1
$1+\iota$	$1+\iota$	$-1+\iota$	ι	$1-\iota$	$-1-\iota$	$-\iota$	1	-1	0
$-1+\iota$	$-1+\iota$	ι	$1+\iota$	$-1-\iota$	$-\iota$	$1-\iota$	-1	0	1
$-\iota$	$-\iota$	$1-\iota$	$-1-\iota$	0	1	-1	ι	$1+\iota$	$-1+\iota$
$1-\iota$	$1-\iota$	$-1-\iota$	$-\iota$	1	-1	0	$1+\iota$	$-1+\iota$	ι
$-1-\iota$	$-1-\iota$	$-\iota$	$1-\iota$	-1	0	1	$-1+\iota$	ι	$1+\iota$

(3) Da $\mu_{\iota,\mathbb{F}_3}(X) = X^2 + 1$ ist, gilt $\iota^2 = -1$. Folglich gilt für alle $a, b, c, d \in \mathbb{F}_3$

$$(a + b\iota)(c + d\iota) = (ac - bd) + (ad + bc)\iota.$$

Damit lässt sich nun die folgende Tabelle aufstellen:

$(\cdot)$	0	1	-1	ι	$1+\iota$	$-1+\iota$	$-\iota$	$1-\iota$	$-1-\iota$
0	0	0	0	0	0	0	0	0	0
1	0	1	-1	ι	$1+\iota$	$-1+\iota$	$-\iota$	$1-\iota$	$-1-\iota$
-1	0	-1	1	$-\iota$	$-1-\iota$	$1-\iota$	ι	$-1+\iota$	$1+\iota$
ι	0	ι	$-\iota$	-1	$-1+\iota$	$-1-\iota$	1	$1+\iota$	$1-\iota$
$1+\iota$	0	$1+\iota$	$-1-\iota$	$-1+\iota$	$-\iota$	1	$1-\iota$	-1	ι
$-1+\iota$	0	$-1+\iota$	$1-\iota$	$-1-\iota$	1	ι	$1+\iota$	$-\iota$	-1
$-\iota$	0	$-\iota$	ι	1	$1-\iota$	$1+\iota$	-1	$-1-\iota$	$-1+\iota$
$1-\iota$	0	$1-\iota$	$-1+\iota$	$1+\iota$	-1	$-\iota$	$-1-\iota$	ι	1
$-1-\iota$	0	$-1-\iota$	$1+\iota$	$1-\iota$	ι	-1	$-1+\iota$	1	$-\iota$

(4) Wir können in der Tabelle nun die multiplikativ inversen Elemente ablesen:

x	x^{-1}
1	1
-1	-1
$\imath$	$-\imath$
$1+\imath$	$-1+\imath$
$-1+\imath$	$1+\imath$
$-\imath$	$\imath$
$1-\imath$	$-1-\imath$
$-1-\imath$	$1-\imath$

`pnp.mathematik.uni-stuttgart.de/lexmath/kuenzer/alg20/`