C. Dietzel, M. Künzer

Algebra für Lehramt, SoSe 20

Lösung 3

Aufgabe 9 Sei R ein faktorieller Ring. Seien $x, y \in R^\times$.
Man zeige oder widerlege.

(1) Sei z ein größter gemeinsamer Teiler von x und y. Dann ist $(x, y) = (z)$.

(2) Liege $z \in R$ mit $(x, y) = (z)$ vor. Dann ist z ein größter gemeinsamer Teiler von x und y.

(3) Es ist $(x \cdot y) = (x) \cap (y)$.

(4) Ist 1 ein größter gemeinsamer Teiler von x und y, dann ist $(x \cdot y) = (x) \cap (y)$.

Lösung zu Aufgabe 9:

(1) Falsch. Gegenbeispiel: Sei K irgendein Körper. Es ist dann $K[X, Y]$ faktoriell (Korollar 66).

Es ist 1 ein größter gemeinsamer Teiler der X und Y, denn diese sind beide irreduzibel. Aber $(X, Y) \neq (1)$. Gäbe es nämlich $p(X, Y), q(X, Y) \in K[X, Y]$ so, dass $p(X, Y)X + q(X, Y)Y = 1$, so müsste $p(X, Y)X$ oder $q(X, Y)Y$ einen Summanden der Form $a_{0,0}X^0Y^0$ mit $a_{0,0} \neq 0$ enthalten. Sowohl $p(X, Y)X$ als auch $q(X, Y)Y$ haben aber konstanten Term 0.

(2) Richtig. Ist $(x, y) = (z)$, so gilt für alle $r \in R$:

$$(r|x) \wedge (r|y) \Leftrightarrow ((x) \subseteq (r)) \wedge ((y) \subseteq (r)) \Leftrightarrow (x, y) \subseteq (r) \Leftrightarrow (z) \subseteq (r) \Leftrightarrow r|z,$$

also ist z ein größter gemeinsamer Teiler von x, y.

(3) Falsch. Im faktoriellen Ring $\mathbb{Z}$ gilt $(2) \cap (2) = (2)$ und $(2 \cdot 2) = (4) \neq (2)$.

(4) Richtig. Es gilt immer $(x \cdot y) \subseteq (x) \cap (y)$, da $(x \cdot y) \subseteq (x)$ und $(x \cdot y) \subseteq (y)$ ist.

Wir legen nun eine vollständige Menge P paarweise nicht-assoziierter Primelemente in R fest. Da x, y teilerfremd sind, gelten für alle $p \in P$ die Implikationen $\mathrm{v}_p(x) \neq 0 \Rightarrow \mathrm{v}_p(y) = 0$ und $\mathrm{v}_p(y) \neq 0 \Rightarrow \mathrm{v}_p(x) = 0$ (sonst wäre p jeweils ein gemeinsamer Teiler).

Sei nun $z \in (x) \cap (y)$. Wegen $x|z$ gilt $\mathrm{v}_p(x) \leq \mathrm{v}_p(z)$ für alle $p \in P$, wegen $y|z$ gilt zudem $\mathrm{v}_p(y) \leq \mathrm{v}_p(z)$ für alle $p \in P$. Da $\mathrm{v}_p(x), \mathrm{v}_p(y)$ nie gleichzeitig > 0 sind, folgt daraus $\mathrm{v}_p(z) \geq \max\{\mathrm{v}_p(x), \mathrm{v}_p(y)\} = \mathrm{v}_p(x) + \mathrm{v}_p(y) = \mathrm{v}_p(xy)$. Folglich gilt $xy|z$ bzw. $z \in (xy)$.

Aufgabe 10 Sei R ein Integritätsbereich.

(1) Sei $x \in R^\times \setminus \mathrm{U}(R)$ gegeben, also weder null noch invertierbar.

Man zeige, daß x genau dann prim ist, wenn $R/(x)$ ein Integritätsbereich ist.

(2) Seien $x,\ y\ \in\ R$ gegeben mit $(x,y) = (1)$. Man zeige, daß der Ringmorphismus

$$\begin{array}{ccccc} R & \to & R/(x) & \times & R/(y) \\ r & \mapsto & (r+(x) & , & r+(y)) \end{array}$$

surjektiv ist. Man bestimme seinen Kern, in Abhängigkeit von x und y.

Lösung zu Aufgabe 10:

(1) Wir nehmen zunächst an, dass $x \in R$ prim ist. Wir wollen nun zeigen, dass $R/(x)$ ein Integritätsbereich ist:

Es gelten dann für alle $y, z \in R$ die folgenden Äquivalenzen:

$$\begin{aligned} (y+(x))(z+(x)) &= 0+(x) \\ \Leftrightarrow yz+(x) &= 0+(x) \\ \Leftrightarrow yz &\in (x) \\ \Leftrightarrow y \in (x) &\vee z \in (x) \\ \Leftrightarrow (y+(x) = 0+(x)) &\vee (z+(x) = 0+(x)), \end{aligned}$$

folglich ist $R/(x)$ ein Integritätsbereich.

Nun nehmen wir an, dass $R/(x)$ ein Integritätsbereich ist. Dann gelten für beliebige $y, z \in R$ die folgenden Äquivalenzen:

$$\begin{aligned} yz &\in (x) \\ \Leftrightarrow yz+(x) &= 0+(x) \\ \Leftrightarrow (y+(x))\cdot(z+(x)) &= 0+(x) \\ (y+(x) = 0+(x)) &\vee (z+(x) = 0+(x)) \\ \Leftrightarrow y \in (x) &\vee z \in (x), \end{aligned}$$

also ist x in diesem Fall prim.

(2) Wir bezeichnen den Ringmorphismus mit c.

Schreibe $1 = rx + sy$ mit geeigneten $r, s \in R$; dies ist wegen $(x,y) = (1)$ möglich. Dann ist $1 - rx = sy$ bzw. $1 - sy = rx$.

Wegen dieser Gleichungen haben wir

$$c(sy) = (sy+(x), sy+(y)) = (1-rx+(x), 0+(y)) = (1+(x), 0+(y))$$

sowie

$$c(rx) = (rx+(x), rx+(y)) = (0+(x), 1-sy+(y)) = (0+(x), 1+(y)).$$

D.h. die Elemente $(1,0)$ und $(1,0)$ in $R/(x)\times R/(y)$ werden auf jeden Fall durch c getroffen. Die Idee ist nun, jedes weitere Element von $R/(x)\times R/(y)$ als „Linearkombination“ dieser Elemente auszudrücken - wir konstruieren ein geeignetes Urbild in R als entsprechende Kombination von rx und sy.

Für beliebige $a, b \in R$ gilt nun

$$\begin{aligned} c(a \cdot sy + b \cdot rx) &= c(a \cdot sy) + c(b \cdot rx) \\ &= c(a) \cdot c(sy) + c(b) \cdot c(rx) \\ &= (a + (x), a + (y)) \cdot (1 + (x), 0 + (y)) \\ &\quad + (b + (x), b + (y)) \cdot (0 + (x), 1 + (y)) \\ &= (a + (x), 0 + (y)) + (0 + (x), b + (y)) \\ &= (a + (x), b + (y)). \end{aligned}$$

Folglich wird jedes Element in $R/(x) \times R/(y)$ durch c getroffen.

Nun bestimmen wir den Kern: wir haben $c(a) = (a+(x), a+(y)) = (0+(x), 0+(y))$ genau dann, wenn $a \in (x)$ und $a \in (y)$, d.h. $a \in (x) \cap (y)$ ist. Folglich ist $\ker(c) = (x) \cap (y)$.

Zusatzfrage: Was kann man mithilfe des Homomorphiesatzes aus dieser Aufgabe folgern?

Aufgabe 11 Sei p prim.

(1) Man weise $|\operatorname{GL}_2(\mathbb{F}_p)| = (p^2 - 1)(p^2 - p)$ nach.

(2) Man bestimme $e := \mathrm{v}_p(|\operatorname{GL}_2(\mathbb{F}_p)|)$.
Man bestimme eine Untergruppe von $\operatorname{GL}_2(\mathbb{F}_p)$ von Ordnung p^e.

(3) Man weise $|\operatorname{GL}_3(\mathbb{F}_p)| = (p^3 - 1)(p^3 - p)(p^3 - p^2)$ nach.

(4) Man bestimme $e := \mathrm{v}_p(|\operatorname{GL}_3(\mathbb{F}_p)|)$.
Man bestimme eine Untergruppe von $\operatorname{GL}_3(\mathbb{F}_p)$ von Ordnung p^e.

Lösung zu Aufgabe 11:

(1) Sei $A \in \mathbb{F}_p^{2\times 2}$. Wir schreiben $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} =: (a_{*1}\, a_{*2})$. Es ist $A \in \operatorname{GL}_2(\mathbb{F}_p)$ genau dann, wenn die Spaltenvektoren a_{*1}, a_{*2} eine Basis von $\mathbb{F}_p^2$ bilden. Folglich ist $|\mathrm{GL}_2(\mathbb{F}_p)|$ gleich der Anzahl aller Basen von $\mathbb{F}_p^2$. Wieviele gibt es?

Jede Basis a_{*1}, a_{*2} des $\mathbb{F}_p^2$ (wie auch jedes anderen zweidimensionalen Vektorraums) lässt sich nun folgendermaßen konstruieren: wähle einen Vektor $a_{*1} \in \mathbb{F}_p^2 \setminus \{0\}$; wähle dann $a_{*2} \in \mathbb{F}_p^2 \setminus \langle a_{*1} \rangle$. Es sind dann a_{*1}, a_{*2} nach Konstruktion linear unabhängige Vektoren eines 2-dimensionalen Vektorraums und somit eine Basis des selbigen.

Es ist $|\mathbb{F}_p^2| = p^2$. Für die Wahl eines $a_{*1} \in \mathbb{F}_p^2 \setminus \{0\}$ hat man folglich $p^2 - 1$ Option.

Es enthält $\langle a_{*1} \rangle$ als 1-dimensionaler $\mathbb{F}_p$-Vektorraum genau p Elemente.

Hat man nun ein a_{*1} festgelegt, so hat man für die Wahl eines $a_{*2} \in \mathbb{F}_p^2 \setminus \langle a_{*1} \rangle$ nun noch $p^2 - |\langle a_{*1} \rangle| = p^2 - p$ Optionen.

Es gibt also insgesamt $(p^2 - 1)(p^2 - p)$ Optionen, eine Basis des $\mathbb{F}_p^2$ zu konstruieren, entsprechend ist dies die gesuchte Anzahl aller Basen. Folglich ist

$$|\mathrm{GL}_2(\mathbb{F}_p)| = (p^2 - 1)(p^2 - p)\ .$$

(2) Es ist $(p^2-1)(p^2-p) = p(p^2-1)(p-1)$. Es teiltt p weder p^2-1 noch $p-1$, somit teilt p auch nicht $(p^2-1)(p-1)$. Folglich ist $e = 1$.

Wir müssen nun eine Untergruppe von $\mathrm{GL}_2(\mathbb{F}_p)$ von Ordnung p finden.

> Dafür gibt es mehrere Möglichkeiten. Daher motivieren wir zunächst unser Vorgehen: Ist $H \leqslant \mathrm{GL}_2(\mathbb{F}_p)$ eine Untergruppe mit $|H| = p$, so gilt für jede Matrix $A \in H$, dass $A^p = E_2$ ist, wobei E_2 die Einheitsmatrix in $\mathbb{F}_p^{2\times 2}$ bezeichnet. Da A und E_2 miteinander kommutieren, dürfen wir rechnen (vgl. Blatt 2): $(A-E_2)^p = A^p - E_2^p = E_2 - E_2 = 0$. D.h. $A - E_2$ ist eine nilpotente Matrix, ist also ähnlich („∼“) zur Matrix $\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$, folglich ist $A \sim B := \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$. Weiterhin ist für alle $k \in \mathbb{Z}$ die Matrix $A^k \in H$ und $A^k \sim B^k = \begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}$ vermöge der gleichen Ähnlichkeitstransformation. Das heißt, jede p-Untergruppe $H \leqslant \mathrm{GL}_2(\mathbb{F}_p)$ ist im Sinne der Linearen Algebra ähnlich zu einer Untergruppe, die alle Matrizen der Form $\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}$ enthält.

Sei $H := \left\{ \begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix} \in \mathbb{F}_p^{2\times 2} : x \in \mathbb{F}_p \right\}$. Wir behaupten, es ist H eine Untergruppe der gesuchten Art. Zunächst ist ist $|H| = |\mathbb{F}_p| = p$.

Außerdem ist $E_2 \in H$. Weiterhin gilt für alle $x, y \in \mathbb{F}_p$:

$$\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & y\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & x+y\\ 0 & 1\end{pmatrix}$$
$$\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}^{-1} = \begin{pmatrix}1 & -x\\ 0 & 1\end{pmatrix}.$$

Damit ist H abgeschlossen unter Multiplikation, Inversenbildung und enthält E_2. Sind also $A_1, A_2 \in H$, so ist $A_2^{-1} \in H$ und somit auch $A_1 A_2^{-1} \in H$. Folglich ist H eine Untergruppe.

Alternativ kann man auch $H = \langle \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \rangle$ überprüfen.

(3) Ähnlich wie in (1) schreiben wir eine Matrix $A \in \mathbb{F}_p^{3\times 3}$ als $A = (a_{*1}\, a_{*2}\, a_{*3})$. Die Matrix A ist invertierbar genau dann, wenn ihre Spalten a_{*1}, a_{*2}, a_{*3} eine Basis des $\mathbb{F}_p^3$ bilden.

Jede Basis des $\mathbb{F}_p^3$ lässt sich wie folgt konstruieren:

Wir wählen $a_{*1} \in \mathbb{F}_p^3 \setminus \{0\}$. Wegen $|\mathbb{F}_p^3| = p^3$ gibt es hierfür $p^3 - 1$ Optionen.

Nun wählen wir $a_{*2} \in \mathbb{F}_p^3 \setminus \langle a_{*1} \rangle$. Da $\langle a_{*1} \rangle$ ein 1-dimensionaler $\mathbb{F}_p$-Vektorraum ist, gilt $|\langle a_{*1} \rangle| = p$, somit hat man für die Wahl von a_{*2} genau $p^3 - p$ Optionen.

Schließlich wählen wir $a_{*3} \in \mathbb{F}_p^3 \setminus \langle a_{*1}, a_{*2} \rangle$. Da $\langle a_{*1}, a_{*2} \rangle$ ein 2-dimensionaler $\mathbb{F}_p$-Vektorraum ist, gilt $|\langle a_{*1}, a_{*2} \rangle| = p^2$, somit hat man für die Wahl von a_{*3} genau $p^3 - p^2$ Optionen.

Auf diese Weise lassen sich insgesamt $(p^3-1)(p^3-p)(p^3-p^2)$ verschiedene Basen von $\mathbb{F}_p^3$ konstruieren. Folglich ist $|\mathrm{GL}_3(\mathbb{F}_p)| = (p^3-1)(p^3-p)(p^3-p^2)$.

(4) Es ist $(p^3-1)(p^3-p)(p^3-p^2) = p \cdot p^2 \cdot (p^3-1)(p^2-1)(p-1) = p^3(p^3-1)(p^2-1)(p-1)$. Da p keine der Zahlen $(p^3-1), (p^2-1), (p-1)$ teilt, ist $e = 3$.

Wir suchen nun eine Untergruppe H von $\mathrm{GL}_3(\mathbb{F}_p)$ von Ordnung p^3.

Die Lösung von (2) legt nahe, wie folgt anzusetzen:

$$H := \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \in \mathbb{F}_p^{3\times 3} : x, y, z \in \mathbb{F}_p \right\}.$$

Da x, y, z in dieser Darstellung auf je p Optionen belegt werden können, ist $|H| = p^3$.

Außerdem ist $E_3 \in H$. Das Produkt zweier Matrizen in H liegt wieder in H, wie man an der Rechnung

$$\begin{pmatrix} 1 & x_1 & y_1 \\ 0 & 1 & z_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x_2 & y_2 \\ 0 & 1 & z_2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x_1 + x_2 & y_1 + y_2 + x_1 z_2 \\ 0 & 1 & z_1 + z_2 \\ 0 & 0 & 1 \end{pmatrix} \in H$$

erkennt. Außerdem ist H auch abgeschlossen unter Inversenbildung:

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x & xz - y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix} \in H.$$

Sind also $A_1, A_2 \in H$, so ist $A_2^{-1} \in H$ und demzufolge $A_1 A_2^{-1} \in H$. Da auch $E_3 \in H$ ist, ist H eine Untergruppe von $\mathrm{GL}_3(\mathbb{F}_p)$.

Aufgabe 12 In den Antworten ist die Zykelschreibweise für Elemente der symmetrischen Gruppe zu verwenden.

(1) Ist S_3 abelsch?

(2) Ist $\mathrm{S}_3 = \langle (1,2), (2,3) \rangle$?

(3) Gibt es in S_4 eine zyklische Untergruppe von Ordnung 6 ?

(4) Gibt es in S_4 eine nichtabelsche Untergruppe von Ordnung 8 ?

Lösung zu Aufgabe 12:

(1) Nein. Zum Beispiel ist $(1,2) \circ (2,3) = (1,2,3)$ und $(2,3) \circ (1,2) = (1,3,2)$, was nicht dasselbe ist.

(2) Ja. Wir zeigen dies, indem wir alle Elemente der S_3 als Produkt in $(1,2)$ und $(2,3)$ ausdrücken. Wir schreiben abkürzend $H := \langle (1,2), (2,3) \rangle$

In jedem Falle sind $\mathrm{id}, (1,2), (2,3) \in H$.

Es ist $(1,2,3) = (1,2) \circ (2,3) \in H$, außerdem ist $(1,3,2) = (2,3) \circ (1,2) \in H$. Letztendlich ist damit auch $(1,3) = (1,2) \circ (1,3,2) \in H$. Es folgt $H = S_3$.

(3) Nein. Gäbe es ein $\pi \in S_4$ mit $|\langle \pi \rangle| = 6$, dann wäre $\pi^6 = \mathrm{id}$, aber $\pi^k \neq \mathrm{id}$ für $0 < k < 6$. Wir werden zeigen, dass es kein solches π gibt.

Jedes $\pi \in S_4$ nimmt eine der folgenden Formen an:

(i) $\pi = \mathrm{id}$

(ii) $\pi = (a, b)$

(iii) $\pi = (a, b)(c, d)$

(iv) $\pi = (a, b, c)$

(v) $\pi = (a, b, c, d)$

Hierbei sind a, b, c, d jeweils mit paarweise verschiedenen Elementen aus $\{1, 2, 3, 4\}$ belegt. D.h. $\{a, b, c, d\} = \{1, 2, 3, 4\}$.

Nun prüft man nach, für welches $k > 0$ erstmals $\pi^k = \mathrm{id}$ gilt:

(i) $\mathrm{id}^1 = \mathrm{id} \Rightarrow k = 1$

(ii) $(a, b)^2 = \mathrm{id}$
$\Rightarrow k = 2$

(iii) $((a, b)(c, d))^2 = \mathrm{id}$
$\Rightarrow k = 2$

(iv) $(a, b, c)^2 = (a, c, b)$,
$(a, b, c)^3 = \mathrm{id}$
$\Rightarrow k = 3$

(v) $(a, b, c, d)^2 = (a, c)(b, d)$,
$(a, b, c, d)^3 = (a, d, c, b)$,
$(a, b, c, d)^4 = \mathrm{id}$
$\Rightarrow k = 4$.

Wir sehen, dass es kein $\pi \in S_4$ gibt, für das $\pi^k = \mathrm{id}$ erstmals bei $k = 6$ gilt. Also kann es auch keine zyklische Untergruppe der Ordnung 6 geben.

(4) Ja.

Sei $a := (1, 2, 3, 4)$. Es hat $\langle a \rangle$ Ordnung 4.

Wir suchen aber eine Untergruppe der Ordnung 8.

Sei dazu $b := (1, 3)$. Wir beobachten $b \circ a = (1, 3) \circ (1, 2, 3, 4) = (1, 2)(3, 4)$ und also $(b \circ a)^2 = \mathrm{id}$.

Insbesondere ist $b \circ a = (b \circ a)^{-1} = a^{-1} \circ b^{-1} = a^{-1} \circ b$.

Folglich ist für i, j, k, $\ell \in \mathbb{Z}$ auch

$$(a^i \circ b^j) \circ (a^k \circ b^\ell) \;=\; a^i \circ a^{(-1)^j \cdot k} \circ b^j \circ b^\ell \;=\; a^{i+(-1)^j \cdot k} \circ b^{j+\ell}$$

und

$$(a^i \circ b^j)^{-1} \;=\; b^{-j} \circ a^{-i} \;=\; b^j \circ a^{-i} \;=\; a^{(-1)^j \cdot (-i)} \circ b^j$$

Folglich ist

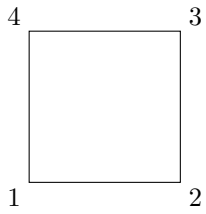
$$H \;:=\; \{\, a^i \circ b^j \;:\; i, j \in \mathbb{Z} \,\} \;=\; \{\, a^i \circ b^j \;:\; i \in [0, 3],\; j \in [0, 1] \,\}$$

eine Untergruppe von S_4. Sie hat auch höchstens 8 Elemente. Um sicherzustellen, daß $|H| = 8$ ist, listen wir die Elemente auf und überzeugen uns, daß sie paarweise verschieden sind.

$$\begin{array}{lcllcl} a^0 \circ b^0 & = & \mathrm{id} & a^0 \circ b^1 & = & (1,3) \\ a^1 \circ b^0 & = & (1,2,3,4) & a^1 \circ b^1 & = & (1,4)(2,3) \\ a^2 \circ b^0 & = & (1,3)(2,4) & a^2 \circ b^1 & = & (2,4) \\ a^3 \circ b^0 & = & (1,4,3,2) & a^3 \circ b^1 & = & (1,2)(3,4) \end{array}$$

Resultat: Es ist $H = \langle a, b \rangle \leqslant \mathrm{S}_4$ mit $|H| = 8$.

Anmerkung: Diese Untergruppe kann man geometrisch sichtbar machen – sie besteht aus allen Bewegungen des unten abgebildeten Quadrats in sich, genauer, den entsprechenden Permutationen der Beschriftungen.



Alternativlösung. Mit der später erst verfügbaren Bemerkung 109 kann man auch wie folgt argumentieren.

Es gibt den Normalteiler $N := \langle (1,2)(3,4), (1,3)(2,4) \rangle \trianglelefteqslant \mathrm{S}_4$ von Ordnung 4.

Es gibt die Untergruppe $U := \langle (1,3) \rangle \leqslant \mathrm{S}_4$ von Ordnung 2.

Es ist $U \cap N = 1$.

Es ist $UN \leqslant \mathrm{S}_4$. Es ist $|UN| = |U| \cdot |N| / |U \cap N| = 2 \cdot 4/1 = 8$.