

EINFÜHRUNG IN DIE ALGEBRA

BLATT 5

Jendrik Stelzner

17. November 2013

Aufgabe 5.1.

(i)

Nach Definition von N_H ist $gH = Hg$ für alle $g \in N_H$. Da $x \in N_H$, ist $\langle x \rangle \subseteq N_H$ eine Untergruppe, also $\langle x \rangle H = H \langle x \rangle$. Es ist

$$1 = 1 \cdot 1 \in \langle x \rangle H,$$

und für $a, b \in \langle x \rangle H$ mit $a = x^n h$ und $b = x^m \tilde{h}$ ist

$$ab^{-1} = x^n h \tilde{h}^{-1} x^{-m} \in \langle x \rangle H \langle x \rangle = \langle x \rangle \langle x \rangle H = \langle x \rangle H,$$

also $\langle x \rangle H$ eine Untergruppe. Da $\langle x \rangle, H \subseteq N_H$ ist $\langle x \rangle H$ eine Untergruppe von N_H , also insbesondere von G .

(ii)

Angenommen, es ist $N_H \neq H$. Dann gibt es ein $x \in N_H$ mit $x \notin H$. Wie oben gezeigt ist $\langle x \rangle H$ eine Untergruppe von N_H . Offenbar ist $H \subsetneq \langle x \rangle H$ eine echte Untergruppe, und da H normal in N_H ist, ist H auch normal in $\langle x \rangle H$. Auch ist

$$\langle x \rangle H / H \cong \langle x \rangle / H \cap \langle x \rangle$$

zyklisch, da $\langle x \rangle$ zyklisch ist, und somit insbesondere abelsch. Da H auflösbar ist, gibt es eine Normalreihe

$$1 = H_0 \subsetneq H_1 \subsetneq \dots \subsetneq H_n = H$$

mit abelschen Faktoren. Da $\langle x \rangle H / H$ abelsch ist, ist daher

$$1 = H_0 \subsetneq H_1 \subsetneq \dots \subsetneq H_n \subsetneq H_{n+1} =: \langle x \rangle H$$

eine Normalreihe von $\langle x \rangle H$ mit abelschen Faktoren. Das steht aber im Widerspruch zur maximalen Auflösbarkeit von H , da H eine echte Untergruppe von $\langle x \rangle H$ ist. Also ist bereits $N_H = H$.

Aufgabe 5.2.

(i)

Bemerkung 1. Sei $n \geq 2$. Dann ist $(\mathfrak{S}_n : \mathfrak{A}_n) = 2$. Insbesondere ist \mathfrak{A}_n normal in \mathfrak{S}_n (dies folgt auch aus $\mathfrak{A}_n = \text{Ker sgn}$).

Beweis. Sei $\tau = (1\ 2) \in \mathfrak{S}_n$ und φ die Linkstranslation mit τ . Aufgrund der Injektivität von φ induziert φ eine injektive Abbildung von der Menge aller gerader Permutationen \mathfrak{A} in die Menge aller ungerader Permutationen $\mathfrak{S}_n - \mathfrak{A}_n$, sowie eine injektive Abbildung von $\mathfrak{S}_n - \mathfrak{A}_n$ nach \mathfrak{A} . Da φ involutiv ist, ist es auch die induzierte Abbildung, also

$$\text{ord } \mathfrak{A}_n = |\mathfrak{S}_n - \mathfrak{A}_n| = \text{ord } \mathfrak{S}_n - \text{ord } \mathfrak{A}_n,$$

da \mathfrak{S}_n endlich ist, und somit $\text{ord } \mathfrak{S}_n = 2 \text{ord } \mathfrak{A}_n$. \square

Es ist $H\mathfrak{A}_n = \mathfrak{S}_n$: Sei $\sigma \in H$ eine ungerade Permutation. Da $\mathfrak{A}_n \subseteq H\mathfrak{A}_n$ enthält $H\mathfrak{A}_n$ alle geraden Permutationen. Jede ungerade Permutation $\pi \in \mathfrak{S}_n$ lässt sich als

$$\pi = \sigma \cdot \sigma\pi$$

schreiben, wobei $\sigma \in H$ und $\sigma\pi$ als Produkt zweier ungerader Permutationen gerade ist, also in \mathfrak{A}_n ist. Also ist $\pi \in H\mathfrak{A}_n$.

Nach Bemerkung 1 ist \mathfrak{A}_n normal in \mathfrak{S}_n mit $(\mathfrak{S}_n : \mathfrak{A}_n) = 2$. Also ist $\mathfrak{A}_n \cap H$ normal in H mit

$$H/\mathfrak{A}_n \cap H \cong H\mathfrak{A}_n/\mathfrak{A}_n = \mathfrak{S}_n/\mathfrak{A}_n.$$

Insbesondere ist daher

$$(H : \mathfrak{A}_n \cap H) = \text{ord } H/\mathfrak{A}_n \cap H = \text{ord } \mathfrak{S}_n/\mathfrak{A}_n = (\mathfrak{S}_n : \mathfrak{A}_n) = 2.$$

(ii)

Da $\text{ord } H > 2$ enthält H ein $\pi \neq \text{id}$ gerader Ordnung: Da H nichttrivial ist, gibt es ein $\sigma \in H$ mit $\sigma \neq \text{id}$. Ist σ gerade, so sei $\pi := \sigma$. Ist σ ungerade so wird zwischen zwei Fällen unterschieden: Ist σ nicht selbstinvers, so sei $\pi := \sigma^2$. Ist σ selbstinvers, so muss H wegen $\text{ord } H > 2$ noch ein weiteres Element $\tau \in H - \{\text{id}, \sigma\}$ beinhalten. Wiederholt man die oberen Schritte für τ , so findet man entweder ein entsprechendes Element π oder auch τ ist selbstinvers. Sind σ und τ beide ungerade und selbstinvers, so sei $\pi := \sigma\tau$.

Es folgt, dass $H \cap \mathfrak{A}_n \supseteq \{\text{id}, \pi\}$ nichttrivial ist. Da \mathfrak{A}_n normal in \mathfrak{S}_n ist, ist $H \cap \mathfrak{A}_n$ normal in H . Da H einfach ist, folgt, dass $H \cap \mathfrak{A}_n = H$ ist. Also ist $H \subseteq \mathfrak{A}_n$ eine Untergruppe.

Aufgabe 5.3.

Bemerkung 2. Sei R ein Ring mit mindestens zwei Elementen. Dann ist sind Null- und Einselement in R verschieden.

Beweis. Da R mindestens zwei Elemente besitzt, gibt es ein $a \in R$ mit $a \neq 0$. Es ist

$$1 \cdot a = a \neq 0 = 0 \cdot a,$$

also $0 \neq 1$. \square

Bemerkung 3. Sei R ein Integritätsring und $b \in R$. Gibt es ein $a \in R$ mit $a \neq 0$ und $ab = a$ oder $ba = a$, so ist $b = 1$. Insbesondere gilt für jede Ringerweiterung $R' \subseteq R$ mit $R' \neq 0$, dass R' genau dann ein Einselement hat, wenn $1 \in R'$.

Beweis. Da $a \neq 0$ impliziert die Nullteilerfreiheit von R die Injektivität der Links-, bzw. Rechtsmultiplikation mit a . Da $1 \cdot a = a = a \cdot 1$ ist daher $b = 1$. \square

Nach Aufgabenstellung ist R ein kommutativer Ring mit Einselement. Da R mindestens zwei Elemente besitzt folgt aus Bemerkung 2, dass $0 \neq 1$. Es gilt also nur noch zu zeigen, dass für jedes $a \in R$ mit $a \neq 0$ ein multiplikativ Inverses $b \in R$ mit $ab = 1$ existiert.

Sei $a \in R$ mit $a \neq 0$ beliebig aber fest und $\mathfrak{a} := (a)$ das von a erzeugte Ideal in R . Da $a \in \mathfrak{a}$ ist $\mathfrak{a} \neq 0$.

Behauptung 4. Es ist $\mathfrak{a} = R$.

Aus der Behauptung folgt wegen $aR = \mathfrak{a} = R$, dass es insbesondere ein $b \in R$ mit $ab = 1$ gibt.

Beweis der Behauptung. Als Ideal ist \mathfrak{a} eine Untergruppe von der additiven Gruppe von R , sowie unter Multiplikation abgeschlossen, wobei sich Assoziativität, Kommutativität und Distributivität der Multiplikation von R auf \mathfrak{a} vererben. Aus der entsprechenden Eigenschaft von R folgt, dass \mathfrak{a} ein Ring mit Einselement bildet. Aus Bemerkung 3 folgt damit, dass $1 \in \mathfrak{a}$, und daher bereits $\mathfrak{a} = R$. \square

Aufgabe 5.4.

(ii)

Für alle $a \in R$ ist

$$a^2 + 1 = a + 1 = (a + 1)^2 = a^2 + 2a + 1,$$

also $2a = 0$. Insbesondere ist $a = -a$.

(i)

Für alle $a, b \in R$ ist

$$ab - ba = ab + ba = (a + b)^2 - a^2 - b^2 = a + b - a - b = 0,$$

also $ab = ba$, und daher R kommutativ.

(iii)

Seien $a, b \in R$ mit $a \neq b$. Es ist

$$(a - b)ab = a^2b - ab^2 = ab - ab = 0.$$

Da $a \neq b$ ist $a - b \neq 0$, wegen der Nullteilerfreiheit von R also $ab = 0$. Wegen der Nullteilerfreiheit ist also $a = 0$ oder $b = 0$. Aus der Beliebigkeit von a und b folgt,

dass es neben 0 nur ein weiteres Element in R gibt. Da aus Bemerkung 2 folgt, dass $0 \neq 1$, ist also $R = \{0, 1\}$. Betrachtet man die Verknüpfungstabellen von R ,

+	0	1
0	0	1
1	1	0

und

·	0	1
0	0	0
1	0	1

,

so ist R offenbar isomorph zu \mathbb{F}_2 .

Aufgabe 5.5.

(i)

Es bezeichne

$$\mathfrak{a}[X] := \left\{ f \in R[X] : f = \sum_{i=0}^n a_i X^i \text{ mit } n \geq 0, a_i \in \mathfrak{a} \text{ für alle } i \right\}$$

die Menge aller Polynome in $R[X]$ mit Koeffizienten in \mathfrak{a} . Da \mathfrak{a} als Ideal abgeschlossen unter Addition ist, ist es auch $\mathfrak{a}[X]$. Das von \mathfrak{a} in $R[X]$ erzeugte Ideal \mathfrak{b} hat die Form

$$\mathfrak{b} = \sum_{a \in \mathfrak{a}} aR[X] = \sum_{a \in \mathfrak{a}} \{af : f \in R[X]\}$$

Sei $f \in \mathfrak{a}[X]$. Dann hat f die Form $f = \sum_{i=0}^n a_i X^i$ mit $a_i \in \mathfrak{a}$ für alle i . Es ist $a_i X^i \in a_i R[X]$ für alle i , und daher $f \in \sum_{i=0}^n a_i R[X] \subseteq \mathfrak{b}$. Also ist $\mathfrak{a}[X] \subseteq \mathfrak{b}$.

Sei $a \in \mathfrak{a}$ und $f \in aR[X]$. Dann hat f die Form $f = \sum_{i=0}^n (aa_i) X^i$ mit $a_i \in R$ für alle i . Da $a \in \mathfrak{a}$ und \mathfrak{a} ein Ideal ist, ist $aa_i \in \mathfrak{a}$ für alle i . Es ist daher $f \in \mathfrak{a}[X]$. Also ist $aR[X] \subseteq \mathfrak{a}[X]$ für alle $a \in \mathfrak{a}$. Da $\mathfrak{a}[X]$ abgeschlossen unter Addition ist, ist daher auch $\mathfrak{b} = \sum_{a \in \mathfrak{a}} aR[X] \subseteq \mathfrak{a}[X]$.

(ii)

Lemma 5. Seien R, R' Ringe und $\phi : R \rightarrow R'$ ein Ringhomomorphismus. Dann induziert ϕ einen Ringhomomorphismus $\psi : R[X] \rightarrow R'[X]$ mit

$$\psi \left(\sum_{i=0}^n a_i X^i \right) := \sum_{i=0}^n \phi(a_i) X^i.$$

Dabei ist

$$\text{Ker } \psi = \left\{ f \in R[X] : f = \sum_{i=0}^n a_i X^i \text{ mit } n \geq 0 \text{ und } a_i \in \text{Ker } \phi \text{ für alle } i \right\}$$

und

$$\text{Im } \psi = \left\{ g \in R'[X] : g = \sum_{i=0}^n b_i X^i \text{ mit } n \geq 0 \text{ und } b_i \in \text{Im } \phi \text{ für alle } i \right\}.$$

Insbesondere ist ψ genau dann injektiv, wenn ϕ injektiv ist, und ψ genau dann surjektiv, wenn ϕ surjektiv ist.

Beweis. Es gilt zunächst zu zeigen, dass ψ ein Ringhomomorphismus ist. Hierfür bemerken wir, dass sich ψ auch als

$$\psi : R[X] \rightarrow R'[X], f \mapsto \phi \circ f = \phi f$$

schreiben lässt, indem $f \in R[X]$ als Abbildung $f : \mathbb{N} \rightarrow R$ gesehen wird. Da ϕ ein Ringhomomorphismus ist und die Addition in $R[X]$ komponentenweise verläuft, ist für alle $f, g \in R[X]$

$$\psi(f + g) = \phi(f + g) = \phi f + \phi g = \psi(f) + \psi(g).$$

Auch ist für alle $i \in \mathbb{N}$

$$\begin{aligned} \psi(f \cdot g)(i) &= \phi(f \cdot g)(i) = \phi \left(\sum_{\mu+\nu=i} f(\mu) \cdot g(\nu) \right) \\ &= \sum_{\mu+\nu=i} (\phi f)(\mu) \cdot (\phi g)(\nu) = ((\phi f) \cdot (\phi g))(i) = (\psi(f) \cdot \psi(g))(i), \end{aligned}$$

also $\psi(f \cdot g) = \psi(f) \cdot \psi(g)$. ψ ist auch unitär, da

$$\psi(1) = \psi(1 \cdot X^0) = \phi(1) \cdot X^0 = 1 \cdot X^0 = 1.$$

Dies zeigt, dass ψ ein Ringhomomorphismus ist.

Es ist $f = \sum_{i=0}^n a_i X^i \in R[X]$ genau dann in $\text{Ker } \psi$, wenn $\psi(f) = 0$, also $\phi(a_i) = 0$ für alle i , also $a_i \in \text{Ker } \phi$ für alle i .

Andererseits ist $g = \sum_{i=0}^n b_i X^i \in R'[X]$ genau dann in $\text{Im } \psi$, wenn es ein $f = \sum_{i=0}^n a_i X^i \in R[X]$ mit $\psi(f) = g$ gibt, also $\phi(a_i) = b_i$ für alle i , also $b_i \in \text{Im } \phi$ für alle i . \square

Es sei $\pi : R \twoheadrightarrow R/\mathfrak{a}$ die kanonische Projektion. Da π ein Ringepimorphismus ist, folgt aus Lemma 5, dass π einen Ringepimorphismus $\psi : R[X] \twoheadrightarrow (R/\mathfrak{a})[X]$ induziert. Auch folgt wegen $\text{Ker } \pi = \mathfrak{a}$ aus dem Lemma, dass $\text{Ker } \psi$ genau aus den Polynomen besteht, deren Koeffizienten alle in \mathfrak{a} liegen, also $\mathfrak{a}[X]$; wie im vorherigen Aufgabenteil gezeigt, ist dies gerade \mathfrak{b} . Es ist daher

$$R[X]/\mathfrak{b} = R[X]/\text{Ker } \psi \cong \text{Im } \psi = (R/\mathfrak{a})[X].$$