Einführung in die Algebra

Blatt 5

Jendrik Stelzner

16. 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, und insbesondere $\langle x \rangle H = H \langle x \rangle$. Es ist

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

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

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

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

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

mit abelschen Faktoren. Es folgt nun, dass

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

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

Aufgabe 5.2.

(i)

Sei $\sigma \in H$ eine ungerade Permutation. Es ist $H\mathfrak{A}_n = \mathfrak{S}_n$: Da $\mathfrak{A}_n \subseteq H\mathfrak{A}_n$ enthält $H\mathfrak{A}$ 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 $\pi \in H\mathfrak{A}_n$.
Wie aus der Vorlesung bekannt 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

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

Insbesondere ist daher

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

(ii)

Da $\operatorname{ord} H > 2$ enthält H eine $\pi \neq \mathrm{id}$ gerader Ordnung: Da H nichttrivial ist, gibt es ein $\sigma \in H$ mit $\sigma \neq \mathrm{id}$. 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 $\operatorname{ord} H > 2$ noch ein weiteres Element $\tau \in H - \{\mathrm{id}, \sigma\}$ 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 selbstinvers, so sei $\pi := \sigma\tau$.
Es folgt, dass $H \cap \mathfrak{A}_n \supseteq \{\mathrm{id}, \pi\}$ 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 1. 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 $0 \neq 1$. □

Bemerkung 2. Sei R ein kommutativer Ring und $a \in R$. Dann ist das von a erzeugte Ideal $\mathfrak{a} := (a)$ ein Ring ohne Eins (d.h. es ist möglich, aber nicht notwendig, dass $1 \in \mathfrak{a}$).

Beweis. Als Ideal ist $\mathfrak{a}$ eine additive Untergruppe der additiven Gruppe von R. Da $rs \in \mathfrak{a}$ für alle $r \in R$ und $s \in \mathfrak{a}$ ist $\mathfrak{a}$ inbesondere abgeschlossen bezüglich der Multiplikation. Die Assoziativität sowie Distributivität der Multiplikation vererben sich aus R. □

Es gilt zunächst zu bemerken, dass ein Ring, wie er in der Aufgabenstellung beschrieben ist, nicht existiert: Da R mindestens zwei Elemente besitzt, folgt aus Bemerkung 1, dass $0 \neq 1$. Jedoch muss $0 \subseteq R$ nach Aufgabenstellung das Einselement von R beinhalten, also $0 = 1$. Im Folgenden wird daher davon ausgegangen, dass die entsprechende Aussage für diesen Sonderfall ausgeschlossen wird.
Nach Aufgabenstellung ist R bereits ein kommutativer Ring mit 1. Da R mindestens zwei Elemente besitzt folgt aus Bemerkung 1, dass $0 \neq 1$. Es gilt also nur noch zu zeigen, dass es für jedes $a \in R$ mit $a \neq 0$ ein multiplikativ Inverses Element $b \in R$ mit $ab = 1$ gibt.
Sei $a \in R$ mit $a \neq 0$ beliebig aber fest. Es sei $\mathfrak{a} := (a)$ das von a erzeugte Ideal. Aus der Nullteilerfreiheit von R folgt, dass $\mathfrak{a} \neq 0$. Es ist $\mathfrak{a} = R$: Ist $\mathfrak{a} \neq R$, so folgt aus Bemerkung 2 und der Aufgabenstellung, dass $1 \in \mathfrak{a}$. Da $\mathfrak{a}$ ein Ideal ist, ist daher $r = r \cdot 1 \in \mathfrak{a}$ für alle $r \in R$. Da $aR = \mathfrak{a} = R$ gibt es insbesondere ein $b \in R$ mit $ab = 1$.
Man bemerke, dass die für den Beweis die aus der Aufgabenstellung ebenfalls folgende Endlichkeit von $\mathfrak{a} = R$ nicht benötigt wird: Ich kann nur vermuten, dass ursprünglich, d.h. bevor die Aufgabenstellung geändert wurde, die Nullteilerfreiheit in Kombination mit der Endlichkeit einer entsprechenden Teilmenge dazu genutzt werde sollte, aus der folgenden Injektivität der Linksmultiplikation mit a auch deren Surjektivität zu folgern, und damit dann analog zu oben die Existenz eines multiplikativ Inversen. In der jetzigen Version folgt aus der aus der Endlichkeit allerdings, dass $\mathfrak{a} = R$ endlich ist.

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 weiters Element in R gibt. Also ist $R = \{0, 1\}$. Betrachtet man die Verknüpfungstabellen von R,

$+$	0	1
0	0	1
1	1	0

und

$\cdot$	0	1
0	0	0
1	0	1

,

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

Aufgabe 5.5.

(i)

Da $\mathfrak{a}$ ein Ideal in R ist, ist $ar \in \mathfrak{a}$ für alle $a \in \mathfrak{a}$ und $r \in R$. Es ist daher

$$\begin{aligned}\mathfrak{b} = (\mathfrak{a}) &= \sum_{a\in\mathfrak{a}} a\, R[X] = \sum_{a\in\mathfrak{a}} \left\{ a \sum_{i=0}^{n} a_i X^i : n \geq 0, a_i \in R \right\} \\ &= \sum_{a\in\mathfrak{a}} \left\{ \sum_{i=0}^{n} a a_i X^i : n \geq 0, a_i \in R \right\} = \left\{ \sum_{i=0}^{n} a_i X^i : n \geq 0, a_i \in \mathfrak{a} \right\}. \quad (1)\end{aligned}$$

Dabei ergibt sich die Gleichheit bei (1) wie folgt:
Für alle $f = \sum_{i=0}^{n} a a_i X^i \in aR[X]$ ist $aa_i \in \mathfrak{a}$, da $a \in \mathfrak{a}$ und $\mathfrak{a}$ ein Ideal in R ist, also f ein Polynom mit Koeffizienten in $\mathfrak{a}$.
Andererseits ist jedes Polynom $f = \sum_{i=0}^{n} a_i X^i$ mit Koeffizienten $a_0, \ldots, a_n \in \mathfrak{a}$ die Summe der Monome $f_i := a_i X^i \in a_i R[X]$. Also ist $f \in \sum_{i=1}^{n} a_i R[X]$.

(ii)

Lemma 3. Seien R, R' Ringe und $\phi : R \to R'$ ein Ringhomomorphismus. Dann induziert ϕ einen Ringhomomorphismus $\psi : R[X] \to R'[X]$ mit

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

Dabei ist

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

und

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

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. Es seien $f, g \in R[X]$ mit $f = \sum_{i=0}^{n} a_i X^i$ und $g = \sum_{i=0}^{n} b_i X^i$. Es ist

$$\begin{aligned}\psi(f+g) &= \psi\left(\sum_{i=0}^{n}(a_i+b_i)X^i\right) = \sum_{i=0}^{n}\phi(a_i+b_i)X^i \\ &= \sum_{i=0}^{n}(\phi(a_i)+\phi(b_i))X^i = \sum_{i=0}^{n}\phi(a_i)X^i + \sum_{i=0}^{n}\phi(b_i)X^i \\ &= \psi\left(\sum_{i=0}^{n}a_iX^i\right) + \psi\left(\sum_{i=0}^{n}b_iX^i\right) = \psi(f)+\psi(g),\end{aligned}$$

sowie

$$\begin{aligned}\psi(fg) &= \psi\left(\sum_{i=0}^{2n}\left(\sum_{\mu+\nu=i}a_\mu b_\nu\right)X^i\right) = \sum_{i=0}^{2n}\phi\left(\sum_{\mu+\nu=i}a_\mu b_\nu\right)X^i \\ &= \sum_{i=0}^{2n}\left(\sum_{\mu+\nu=i}\phi(a_\mu)\phi(b_\nu)\right)X^i = \left(\sum_{i=0}^{n}\phi(a_i)X^i\right)\left(\sum_{i=0}^{n}\phi(b_i)X^i\right) \\ &= \psi\left(\sum_{i=0}^{n}a_iX^i\right)\psi\left(\sum_{i=0}^{n}b_iX^i\right) = \psi(f)\,\psi(g).\end{aligned}$$

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 $\operatorname{Ker}\psi$, wenn $\psi(f) = 0$, also $\phi(a_i) = 0$ für alle i, also $a_i \in \operatorname{Ker}\phi$ für alle i.
Andererseits ist $g = \sum_{i=0}^{n} b_i X^i \in R'[X]$ genau dann in $\operatorname{Im}\psi$, 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 $b_i \in \operatorname{Im}\phi$ für alle i. □

Bemerkung 4. Betrachtet man $R[X]$ als abzählbare direkte Summe der additiven Gruppe von R mit sich selbst, so folgt das obige Lemma fast direkt daraus, dass dann $\psi = \bigoplus_{n\in\mathbb{N}} \phi$. Nur dass ψ bezüglich $\cdot$ ein Monoidhomomorphismus ist, folgt dann nicht direkt, da die Multiplikation in $R[X]$ nicht komponentenweise ist.

Es sei $\pi : R \twoheadrightarrow R/\mathfrak{a}$ die kanonische Projektion. Da π ein Ringepimorphismus ist, folgt aus Lemma 3, dass π einen Ringepimorphismus $\psi : R[X] \twoheadrightarrow (R/\mathfrak{a})[X]$ induziert. Auch folgt wegen $\operatorname{Ker}\pi = \mathfrak{a}$ aus dem Lemma, dass $\operatorname{Ker}\psi$ genau aus den Polynomen besteht, deren Koeffizienten alle in $\mathfrak{a}$ liegen; wie im vorherigen Aufgabenteil gezeigt, ist dies gerade $\mathfrak{b}$. Es ist daher

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