Wolfgang K. Seiler
Tel. 2515

A5, C201

17. November 2015

0. Übungsblatt Algebra

Aufgabe 0: *(1 Punkte)*
U sei die kleinste Untergruppe der Diedergruppe D_4, die die beiden Spiegelungen an den Diagonalen des Quadrats enthält. Finden Sie die kleinste natürliche Zahl n, für die U in die symmetrische Gruppe $\mathfrak{S}_n$ eingebettet werden kann, und geben Sie eine Einbettung $U \to \mathfrak{S}_n$ explizit an!

Lösung: Jede Symmetrie des Quadrats ist durch ihren Effekt auf die Ecken eindeutig festgelegt; nummerieren wir die Ecken etwa im Uhrzeigersinn von eins bis vier, so gibt es also auf jeden Fall eine Einbettung $U \to \mathfrak{S}_4$. Die beiden Spiegelungen an der Diagonalen gehen auf die beiden Transpositionen $(1\ 3)$ und $(2\ 4)$, U insgesamt also auf die (zur Kleinschen Vierergruppe isomorphe) Untergruppe, die außer diesen beiden Transpositionen noch deren Produkt $(1\ 3)(2\ 4)$ (die Spiegelung am Nullpunkt) und die Identität enthält. Die Gruppe $\mathfrak{S}_3$ hat nur sechs Elemente; da die Ordnung einer Untergruppe nach Lagrange Teiler der Gruppenordnung ist, kann sie keine Untergruppe der Ordnung vier enthalten. Somit ist $\mathfrak{S}_4$ die kleinste symmetrische Gruppe, in die sich U einbetten läßt.

Aufgabe 1: *(6 Punkte)*

a) N, M seien zwei Normalteiler der Gruppe G. Zeigen Sie, daß dann auch $N \cap M$ ein Normalteiler ist und daß $G/(N \cap M)$ isomorph ist zu einer Untergruppe von $(G/N) \times (G/M)$!

Lösung: Sei $n \in N \cap M$; wir müssen zeigen, daß $g^{-1}ng$ für jedes Element $g \in G$ wieder in $N \cap M$ liegt. Da N ein Normalteiler ist, liegt $g^{-1}ng$ in N, und da M einer ist, liegt es auch in M, also im Durchschnitt $N \cap M$.
Ein Element $g \in G$ liegt genau dann im Kern der Abbildung

$$\varphi\colon \begin{cases} G \to (G/N) \times (G/M) \\ g \mapsto (gN, gM) \end{cases},$$

wenn gN das Neutralelement von G/N ist und gM das von G/M, wenn also g sowohl in N als auch in M liegt. Somit ist $N \cap M$ der Kern von φ, und nach dem Homomorphiesatz ist $G/(N \cap M)$ isomorph zum Bild von φ, das natürlich eine (nicht unbedingt echte) Untergruppe von $(G/N) \times (G/M)$ ist.

b) N sei ein Normalteiler der Gruppe G und M ein Normalteiler der Gruppe H. Zeigen Sie, daß das direkte Produkt $N \times M$ ein Normalteiler von $G \times H$ ist und daß $(G \times H)/(M \times N)$ isomorph ist zu $(G/N) \times (H/M)$!

Lösung: Wir müssen zeigen, daß für jedes Element $(g, h) \in G \times H$ und jedes (n, m) aus $N \times M$ gilt: $(g, h)^{-1}(n, m)(g, h)$ liegt in $N \times M$. Nach Definition der Gruppenoperation von $G \times H$ ist

$$(g, h)^{-1}(n, m)(g, h) = (g^{-1}, h^{-1})(n, m)(g, h) = (g^{-1}ng, h^{-1}mh),$$

und da N ein Normalteiler von G ist, liegt $g^{-1}ng$ in N; genauso folgt $h^{-1}mh \in M$. Also liegt das Element in $N \times M$.

Der Kern der Abbildung

$$\varphi: \begin{cases} G \times H \to (G/N) \times (H/M) \\ (g,h) \mapsto (gN, hM) \end{cases},$$

besteht aus allen (g,h) mit $gN = N$ und $hM = M$, ist also $N \times M$. Die Abbildung ist surjektiv, denn jedes Paar (gN, hM) hat (unter anderem) das Urbild (g,h). Daher ist nach dem Homomorphiesatz $(G \times H)/(M \times N) \cong G/N \times H/M$.

Aufgabe 2: *(6 Punkte)*

G sei eine Gruppe und $U \leq G$ eine Untergruppe. Zeigen Sie:

a) Für jedes $g \in G$ ist $U^g \underset{\text{def}}{=} g^{-1}Ug$ eine Untergruppe von G.

Lösung: Das Neutralelement e von G liegt wegen $g^{-1}eg = g^{-1}g = e$ in jeder der Mengen U^g, und weiter liegt zu je zwei Elementen $g^{-1}ug$ und $g^{-1}vg$ auch deren Produkt $g^{-1}ug \cdot g^{-1}vg = g^{-1}uvg$ dort. Außerdem ist

$$(g^{-1}ug) \cdot (g^{-1}u^{-1}g) = g^{-1}uu^{-1}g = g^{-1}g = e\,,$$

so daß zu jedem Element von U^g auch das Inverse dort liegt. Somit ist U^g eine Untergruppe von G.

b) Der Durchschnitt aller Untergruppen U^g ist ein Normalteiler von G.

Lösung: N sei dieser Durchschnitt, und h sei ein beliebiges Element von G. Wir müssen zeigen, daß $N^h = h^{-1}Nh$ in N liegt. N liegt in jeder der Gruppen U^g, also liegt N^h für jedes $g \in G$ in der Gruppe

$$(U^g)^h = h^{-1}U^g h = h^{-1}g^{-1}Ugh = (gh)^{-1}U(gh) = U^{gh}\,.$$

Mit g durchläuft aber auch gh die sämtlichen Elemente von G, denn die Multiplikation mit h ist in einer Gruppe bijektiv. Somit liegt N^h in jeder der Gruppen U^g, also in deren Durchschnitt N.

c) $H = \{g \in G \mid U^g = U\}$ ist eine Untergruppe von G.

Lösung: Da $U^e = U$, liegt das Neutralelement in H. Für zwei Elemente $g, h \in H$ ist allgemein (siehe *b)*) $U^{gh} = (U^g)^h$, hier also $U^{gh} = (U^g)^h = U^h = U$, so daß auch gh in H liegt. Schließlich liegt mit g auch g^{-1} in H, denn für $g \in H$ ist

$$U^{(g^{-1})} = gUg^{-1} = gU^g g^{-1} = gg^{-1}Ugg^{-1} = U\,.$$

d) U ist ein Normalteiler von H.

Lösung: Natürlich ist $U \leq H$, denn für jedes Element $u \in U$ ist $u^{-1}Uu = U$. Für ein beliebiges $h \in H$ ist nach Definition $U^h = U$, und genau das muß gelten, damit U Normalteiler von H ist. (H heißt der *Normalisator* von U.)

e) Die Anzahl verschiedener Untergruppen U^g ist gleich dem Index von H.

Lösung: M sei die Menge aller Untergruppen U^g mit $g \in G$. Dann definiert die Vorschrift $(x, U^g) \mapsto (U^g)^x$ eine Operation von G auf M, denn für $x, y \in G$ ist nach der in der Lösung von *b)* durchgeführten Rechnung $(U^g)^{(xy)} = \left((U^g)^x\right)^y$. Der Stabilisator von $U = U^e$ ist nach Definition gleich H, und die Bahn von U ist nach Definition von M ganz M. Nach der Bahnbilanzgleichung ist die Elementanzahl von M daher der Quotient der Gruppenordnungen von G und H, also der Index von H in G.

f) U sei eine maximale Untergruppe von G, d.h. außer G selbst gibt es keine Untergruppe von G, die U echt enthält. Falls es ein $g \notin U$ gibt, für das $g^{-1}Ug = U$ ist, ist U ein Normalteiler von G.

Lösung: Da es ein $g \in G \setminus U$ mit $U^g = U$ gibt, ist die oben definierte Gruppe H echt größer als U. Da U maximal vorausgesetzt war, muß daher $H = G$ sein, und nach *d)* ist U ein Normalteiler von $H = G$.

Aufgabe 3: *(5 Punkte)*

a) Zeigen Sie, daß die Abbildung $\varphi\colon \mathbb{R}[X] \to \mathbb{R}$, die jedem Polynom $f \in \mathbb{R}[X]$ den Funktionswert $f(1)$ zuordnet, ein Homomorphismus ist, und bestimmen Sie Kern und Bild von φ!

Lösung: Polynome definieren Funktionen $f\colon \mathbb{R} \to \mathbb{R}$, und für zwei Funktionen f, g ist $(f \pm g)(x) = f(x) \pm g(x)$ und $(fg)(x) = f(x)g(x)$. Dies gilt insbesondere für $x = 1$, also ist φ ein Homomorphismus. Sein Bild ist natürlich ganz $\mathbb{R}$, denn für jedes $a \in \mathbb{R}$ hat das konstante Polynom a insbesondere auch an der Stelle eins den Wert a. Liegt $f \in \mathbb{R}[X]$ im Kern, so ist $f(1) = 0$, also ist f durch das Polynom $X - 1$ teilbar, und umgekehrt verschwindet auch jedes Vielfache von $X - 1$ an der Stelle eins. Daher ist der Kern von φ das von $X - 1$ erzeugte Ideal.

b) Zeigen Sie, daß die Abbildung $\psi\colon \mathbb{R}[X] \to \mathbb{C}$, die jedem Polynom $f \in \mathbb{R}[X]$ den Funktionswert $f(i)$ zuordnet, ein Homomorphismus ist, und bestimmen Sie Kern und Bild von ψ!

Lösung: Polynome mit reellen Koeffizienten definieren auch Abbildungen $\mathbb{C} \to \mathbb{C}$ mit den gleichen Eigenschaften wie in *a);* daher können wir für x auch i einsetzen und erhalten so die Homomorphieeigenschaft. Auch ψ ist surjektiv, denn die komplexe Zahl $a + bi$ mit $a, b \in \mathbb{R}$ ist das Bild von $bX + a$ unter ψ. Im Kern liegt insbesondere das Polynom $X^2 + 1$, denn $i^2 = -1$. Für ein beliebiges Polynom $f \in \mathbb{R}[X]$ aus dem Kern von ψ betrachten wir den ggT von f und $X^2 + 1$ in $\mathbb{R}[X]$. Diesen können wir nach dem EUKLIDischen Algorithmus berechnen, und da uns dieser nie aus dem verwendeten Grundkörper hinausführt, können wir ihn statt in $\mathbb{R}[X]$ auch in $\mathbb{C}[X]$ berechnen. Dort ist er wegen $f(i) = 0$ durch $X - i$ teilbar, also muß er auch in $\mathbb{R}[X]$ ein Polynom sein, das in $\mathbb{C}[X]$ durch $X - i$ teilbar ist; außerdem ist er natürlich ein Teiler von $X^2 + 1$. Da er ein reelles Polynom sein muß, ist er somit $X^2 - 1$, d.h. $X^2 - 1$ teilt f und $\operatorname{Kern} \psi = (X^2 - 1)$.

Aufgabe 4: *(5 Punkte)*

a) R und S seien Ringe. Die direkte Summe $R \oplus S$ von R und S ist die Menge $R \times S$ mit den beiden Rechenoperationen

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \quad \text{und} \quad (r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)\,.$$

Zeigen Sie, daß auch $R \oplus S$ ein Ring ist!

Lösung: Da Addition und Multiplikation komponentenweise definiert sind und die Ringaxiome in jeder Komponente gelten, ist $R \oplus S$ ein Ring mit $(0, 0)$ als Neutralelement der Addition und $(1, 1)$ als Neutralelement der Multiplikation. Das additive Inverse zu (r, s) ist $(-r, -s)$.

b) Nun seien R und S kommutative Ringe. Ist dann auch $R \oplus S$ ein kommutativer Ring?

Lösung: Ja, denn wenn die Multiplikation in jeder der beiden Komponenten das Kommutativgesetz erfüllt, gilt es auch für $R \oplus S$.

c) Nun seien R und S Integritätsbereiche. Ist dann auch $R \oplus S$ ein Integritätsbereich?

Lösung: *Nein,* denn beispielsweise ist $(0, 1) \cdot (1, 0) = (0, 0)$, obwohl weder $(0, 1)$ noch $(1, 0)$ das Neutralelement der Addition sind.

d) Zeigen Sie: $\mathbb{R}[X]/(X^2-1) \cong \mathbb{R}[X]/(X+1) \oplus \mathbb{R}[X]/(X-1)$!

Lösung: Da $(X^2-1) = (X+1)(X-1)$ ist, liegt (X^2-1) sowohl im Ideal $(X+1)$ als auch im Ideal $(X-1)$; daher sind die Abbildungen, die die Restklasse von f modulo (X^2-1) auf die modulo $(X+1)$ *bzw.* $(X-1)$ abbilden, beide wohldefiniert und geben zusammen einen Homomorphismus von $R[X]/(X^2-1)$ nach $R[X]/(X+1) \oplus R[X]/(X-1)$. Er ist injektiv, denn wenn f mod (X^2-1) auf das Nullelement abgebildet wird, liegt f sowohl in $(X+1)$ als auch in $(X-1)$, also in deren Durchschnitt $\big((X+1)(X-1)\big) = (X^2-1)$. Die Abbildung ist auch surjektiv, denn wie die Darstellung $1 = \frac{1}{2}(X+1) - \frac{1}{2}(X-1)$ zeigt, ist $\frac{1}{2}(X+1) \equiv 0 \bmod (X+1)$ und $\equiv 1 \bmod (X-1)$; entsprechend $-\frac{1}{2}(X-1) \equiv 1 \bmod (X+1)$ und $\equiv 0 \bmod (X-1)$. Für ein vorgegebenes Element $\big(g+(X+1), h+(X-1)\big) \in R[X]/(X+1) \oplus R[X]/(X-1)$ ist daher die Restklasse von $\frac{1}{2}(X+1)h - \frac{1}{2}(X-1)g$ modulo (X^2-1) ein Urbild.

Aufgabe 5: *(4 Punkte)*

a) Ist $\mathbb{R}[X,Y]$, der Ring aller reeller Polynome in zwei Variablen X, Y, ein Hauptidealring?

Lösung: Falls ja, gibt es ein $f \in \mathbb{R}[X,Y]$, so daß $(X,Y) = (f)$ ist. Insbesondere gibt es also Polynome $g, h \in \mathbb{R}[X]$ mit $fg = X$ und $fh = Y$. Da X und Y irreduzibel sind, muß entweder f eine Einheit sein oder g und h sind Einheiten. Für eine Einheit f ist (f) der ganze Ring $\mathbb{R}[X,Y]$, was nicht sein kann, da (X,Y) nur die Polynome ohne konstantes Glied enthält. Sind g und h Einheiten, so unterscheiden sich X und Y nur durch eine Einheit, d.h. $X/Y \in \mathbb{R}[X,Y]$, was auch nicht der Fall ist. Also kann $\mathbb{R}[X,Y]$ kein Hauptidealring sein.

b) R sei ein Hauptidealring. Kann es eine unendliche Kette von Idealen $I_1, I_2, \ldots$ geben derart, daß jedes Ideal I_{k+1} echt in I_k enthalten ist für alle $k \in \mathbb{N}$?

Lösung: Ja, natürlich. Im Hauptidealring $\mathbb{Z}$ können wir beispielsweise $I_k = (2^k)$ nehmen: Für alle k ist (2^{k+1}) echt in (2^k) enthalten.

Aufgabe 6: *(2 Punkte)*

Zeigen Sie: Ein Polynom $f = f(X) \in R[X]$ über einem Integritätsbereich R ist genau dann irreduzibel, wenn das Polynom $f(X+1)$ irreduzibel ist.

Lösung: Ist $f = g \cdot h$, so ist natürlich auch $f(X+1) = g(X+1)h(X+1)$. Da $p(X+1)$ für jedes Polynom $p \in \mathbb{R}[X]$ denselben Grad hat wie p (sogar die führenden Koeffizienten stimmen überein), folgt aus der Reduzibilität von f also auch die von $f(X+1)$.

Ist umgekehrt $f(X+1) = gh$ mit zwei Polynomen $g, h \in R[X]$ von positivem Grad, so ist $f = g(X-1)h(X-1)$, wobei $g(X-1)$ den gleichen Grad hat wie g und $h(X-1)$ den von h, d.h. auch f ist reduzibel.

Aufgabe 7: *(4 Punkte)*

a) Bestimmen Sie Kern und Bild des Homomorphismus $\begin{cases} k[X] \to \mathbb{C} \\ X \mapsto \sqrt[3]{2} \end{cases}$ für $k = \mathbb{Q}$ und für $k = \mathbb{R}$!

Lösung: Für $k = \mathbb{Q}$ ist das Bild gleich $\mathbb{Q} \oplus \mathbb{Q}\sqrt[3]{2} \oplus \mathbb{Q}\sqrt[3]{4}$, denn alle Potenzen von $\sqrt[3]{2}$ sind entweder $\sqrt[3]{2}$ oder $\sqrt[3]{4}$ oder eins, und als Koeffizienten haben die Polynome nur rationale Zahlen. $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ ist beispielsweise Bild des Polynoms $cX^2 + bX + a$.

Liegt $f \in \mathbb{Q}[X]$ im Kern, so ist der ggT von f und $X^3 - 2$ ein Polynom aus $\mathbb{Q}[X]$, das an der Stelle $\sqrt[3]{2}$ verschwindet, also positiven Grad hat, und das auch das irreduzible Polynom $X^3 - 2$ teilt. Also ist der ggT gleich $X^3 - 2$, d.h. f ist durch $X^3 - 2$ teilbar. Somit ist Kern $\varphi = (X^3 - 2)$.

Für $k = \mathbb{R}$ ist das Bild gleich $\mathbb{R}$, da ein reelles Polynom an der Stelle $\sqrt[3]{2}$ nur reelle Werte annehmen kann, und schon die konstanten Polynome ausreichen, um alle reellen Werte zu

realisieren. Der Kern ist das Ideal $(X - \sqrt[3]{2})$, denn jedes Polynom, das an der Stelle $\sqrt[3]{2}$ verschwindet, ist in $\mathbb{R}[X]$ durch $X - \sqrt[3]{2}$ teilbar.

b) Zeigen Sie, daß die Gleichung $x^3 = 2$ im Bild jeweils genau eine Lösung hat!

Lösung: In beiden Fällen liegt das Bild in $\mathbb{R}$, und dort hat die Gleichung $x^3 = 2$ nur eine Lösung.

Aufgabe 8: *(4 Punkte)*
k sei ein Körper, und $f = uf_1^{e_1} \cdots f_n^{e_n}$ sei die Zerlegung des Polynoms $f \in k[X]$ in irreduzible Bestandteile f_i und eine Einheit u. Zeigen Sie: Dann ist

$$k[X]/(f) \cong k[X]/(f_1^{e_1}) \oplus \cdots \oplus k[X]/(f_n^{e_n})\,.$$

Lösung: Beweis durch Induktion nach n. Für $n = 1$ gibt es nichts zu beweisen; für $n > 1$ beachten wir, daß $g = uf_1^{e_1} \cdots f_{n-1}^{e_{n-1}}$ und $h = f_n^{e_n}$ teilerfremd zueinander sind, da die f_i verschiedene irreduzible Polynome sind. Da der Polynomring $k[X]$ EUKLIDisch ist, gibt es daher Polynome $\alpha, \beta \in k[X]$, so daß $\alpha g + \beta h = 1$ ist. Die Abbildung

$$k[X]/(gh) \to k[X]/(g) \oplus k[X]/(h)\,,$$

die der Restklasse eines Polynoms P modulo $(f) = (gh)$ das Paar $\big(P+(g), P+(h)\big)$ zuordnet, ist wohldefiniert, da (gh) sowohl in (g) als auch in (h) liegt. Sie ist auch injektiv, denn $(g) \cap (h) = (gh) = (f)$. Schließlich ist sie surjektiv, da $\big(P_1 + (g), P_2 + (h)\big)$ die Restklasse von $\beta h P_1 + \alpha g P_2$ modulo (f) als Urbild hat. Nach Induktionsannahme ist

$$k[X]/(g) \cong k[X]/(f_1^{e_1}) \oplus \cdots \oplus k[X]/(f_{n-1}^{e_{n-1}})\,,$$

also $k[X]/(f) \cong k[X]/(g) \oplus k[X]/(h) \cong k[X]/(f_1^{e_1}) \oplus \cdots \oplus k[X]/(f_n^{e_n})$, wie behauptet.