Fachbereich Mathematik
Prof. Dr. Nils Scheithauer
Walter Reußwig

TECHNISCHE UNIVERSITÄT DARMSTADT

WS 08/09 25. November 2008

Algebra

7. Übung mit Lösungshinweisen

Aufgabe 31 Sei R ein Integritätsbereich, $R[X]$ der Polynomring über R und $\iota_x : R[X] \to R$ die Punktauswertung in $x \in R$.

(a) Zeige, daß der Kern der Punktauswertung ι_x ein Primideal ist.

(b) Zeige, daß folgende Aussagen äquivalent sind.

(1) Der Ring $R[X]$ ist ein Hauptidealring.

(2) Der Ring R ist ein Körper

Lösung: (a) Es sei $x \in R$ beliebig, $f, g \in R[X]$ und $f \cdot g \in P := \ker \iota_x$. Dann erhalten wir

$$0 = (f \cdot g)(x) = f(x) \cdot g(x).$$

Da R ein Integritätsbereich war, gilt entweder $f(x) = 0$ oder $g(x) = 0$, also $f \in P$ oder $g \in P$. Somit ist P ein Primideal.

(b) (1) $\Rightarrow$ (2) Es sei ι_0 der Auswertungshomomorphismus

$$\iota_0 : R[X] \to R, \quad \iota_0(f) := f(0)$$

und sei $M := \ker(\iota_0)$. Da M ein Primideal ist, für das $(0) \neq M$ gilt, ist M ein maximales Ideal. Weiter ist die Punktauswertung surjektiv, also folgt nach dem ersten Isomorphiesatz

$$R = \mathrm{im}(\iota_0) \cong R[X]/\ker(\iota_0) = R[X]/M.$$

Da M ein maximales Ideal ist, ist somit R als Quotient ein Körper.
(2) $\Rightarrow$ (1) In diesem Fall wissen wir, daß $R[X]$ ein euklidischer Ring, also insbesondere ein Hauptidealring, ist.

Aufgabe 32 Betrachte den Polynomring $\mathbb{R}[X]$.

(a) Zeige, daß das Polynom $X^2 + 1$ in $\mathbb{R}[X]$ irreduzibel ist.

(b) Zeige, daß der Quotientenring $\mathbb{R}[X]/(X^2 + 1)$ isomorph zu $\mathbb{C}$ ist, indem Du

(i) die Restklassen des Quotientenringes analysierst,

(ii) eine geeignete Auswertungsabbildung $\iota_\lambda : \mathbb{R}[X] \to \mathbb{C}$ betrachtest.

Lösung: (a) Angenommen $X^2 + 1$ wäre als echtes Produkt irreduzibler Polynome ausdrückbar. Dieses Produkt hätte notwendigerweise 2 Faktoren von Grad 1 und hätte damit eine Nullstelle x_0. Mit $0 \leq x_0^2 = -1$ folgte aber ein Widerspruch, also ist $X^2 + 1$ ein irreduzibles Polynom.

(b) *(ii)* Es bezeichne $\mathbb{K} := \mathbb{R}[X]/(X^2+1)$ den Quotientenring. Da X^2+1 irreduzibel ist, ist X^2+1 prim, also (X^2+1) ein nichttriviales Primideal und damit maximal. Der Ring $\mathbb{K}$ ist somit ein Körper.
Es sei $[f] \in \mathbb{K}$ eine Restklasse mit Repräsentant f. Mit Hilfe des euklidischen Algorithmus erhalten wir eine Darstellung

$$f = g \cdot (X^2+1) + r,$$

wobei $g, r \in \mathbb{R}[X]$ Polynome sind mit $r = 0$ oder $\deg(r) < 2$. Damit ist r ebenfalls ein Repräsentant von $[f]$, also wird jedes Element von $\mathbb{K}$ durch ein Polynom vom Grad kleiner 2 repräsentiert.
Wir zeigen, daß die Menge $\{1, X\}$ in $\mathbb{K}$ linear unabhängig über $\mathbb{R}$ ist. Angenommmen

$$\begin{aligned}
& [\lambda \cdot X + \mu] = [0] \\
\Leftrightarrow\ & \lambda \cdot X + \mu \in (X^2+1) \\
\Leftrightarrow\ & \lambda \cdot X + \mu = g \cdot (X^2+1) \text{ für ein geeignetes } g \in \mathbb{R}[X] \\
\Leftrightarrow\ & \deg(\lambda \cdot X + \mu) = \deg(g) \cdot \deg(X^2+1) \\
\Leftrightarrow\ & \lambda \cdot X + \mu = 0 \text{ oder } 1 = \deg(g) \cdot \deg(X^2+1) \geq 2.
\end{aligned}$$

Somit muß die Menge linear unabhängig sein, also ist $\mathbb{K}$ ein zweidimensionaler $\mathbb{R}$-Vektorraum. Die Multiplikation in $\mathbb{K}$ funktioniert wie folgt

$$\begin{aligned}
[f] \cdot [g] &= [a \cdot X + b][c \cdot X + d] \\
&= [(a \cdot X + b)(c \cdot X + d)] \\
&= [ac \cdot X^2 + (ad + bc) \cdot X + bd] \\
&= [ac \cdot (X^2 + 1 - 1) + (ad + bc) \cdot X + bd] \\
&= [(ad + bc) \cdot X + bd - ac].
\end{aligned}$$

Somit erhalten wir einen Körperisomorphismus

$$[a \cdot X + b] \to a \cdot i + b \in \mathbb{C}.$$

(iii) Mit der Auswertungsabbildung

$$\iota_i : \mathbb{R}[X] \to \mathbb{C}, \quad \iota_i(f) := f(i)$$

erhalten wir einen Ringhomomorphismus. Dieser ist surjektiv, da der zweidimensionale Teilraum aller Polynome vom Grad kleiner 2 auf ganz $\mathbb{C}$ abgebildet wird. Somit ist der Kern von ι_i ein maximales Ideal. Weiter liegt X^2+1 im Kern, also $(X^2+1) \subseteq \ker(\iota_i)$. Da aber auch (X^2+1) ein maximales Ideal ist, folgt $\ker(\iota_i) = (X^2+1)$ und damit

$$\mathbb{C} = \operatorname{im}(\iota_i) \cong \mathbb{R}[X]/\ker(\iota_i) = \mathbb{R}[X]/(X^2+1).$$

Aufgabe 33 Sei $R = M_2(\mathbb{C})$ der Ring komplexer 2×2-Matrizen.

(a) Zeige, daß für jedes $A \in R$ im Polynomring $R[X]$ gilt:

$$(X - A) \cdot (X + A) = X^2 - A^2.$$

(b) Finde Matrizen A, B mit

$$(B - A) \cdot (B + A) \neq B^2 - A^2.$$

(c) Wo liegt der scheinbare Widerspruch?

LÖSUNG: (a) Nach der Definition des Polynomrings gilt

$$\begin{aligned}(X-A)(X+A) &\mathrel{\hat{=}} (-A,1,0,0,0,...)\cdot(A,1,0,0,0,...)\\ &= (-A^2, A-A, 1, 0, 0, ...)\\ &= (-A^2, 0, 1, 0, 0, ...)\\ &\mathrel{\hat{=}} X^2 - A^2.\end{aligned}$$

(b) Mit der Wahl der partiellen Isometrien

$$A := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad \text{und} \quad B := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

erhalten wir geeignete Matrizen, denn

$$\begin{aligned}A^2 &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},\\ B^2 &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},\\ (B-A)(B+A) &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1. \end{pmatrix}\end{aligned}$$

(c) Für jeden Ring R vertauscht im Polynomring $R[X]$ das Element X mit jedem $r \in R$. Ausgewertet ist dies in nichtkommutativen Ringen in der Regel jedoch falsch. Somit ist der Polynomring in gewissem Sinn „kommutativer als es die Auswertung verträgt".

Aufgabe 34 Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad $n \in \mathbb{N}$. Zeige, daß dann f, aufgefaßt als komplexes Polynom, n verschiedene Nullstellen besitzt. Gilt auch die Umkehrung?

LÖSUNG: Ist f in $\mathbb{Q}[X]$ irreduzibel, so sind f und f' teilerfremd in $\mathbb{Q}[X]$. Damit existieren Polynome $g_1, g_2 \in \mathbb{Q}[X]$ mit

$$1 = g_1 \cdot f + g_2 \cdot f'.$$

Wäre nun ein $x \in \mathbb{C}$ mehrfache Nullstelle von f, so wäre x eine Nullstelle von f' und wir erhielten

$$1 = 1(x) = g_1(x)\cdot f(x) + g_2(x)\cdot f'(x) = 0 + 0 = 0,$$

ein Widerspruch.
Die Umkehrung gilt natürlich nicht, denn

$$(X^2+1)\cdot(X^2-2)$$

ist nicht irreduzibel in $\mathbb{Q}[X]$, hat keine doppelte Nullstelle in $\mathbb{C}$ und keine Nullstelle in $\mathbb{Q}$.

Aufgabe 35 Es sei $\mathbb{K}$ ein endlicher Körper mit $q := |\mathbb{K}|$ Elementen.

(a) Mache Dir klar, daß

$$f(X) := \prod_{k \in \mathbb{K}} (X - k)$$

ein Polynom von Grad q mit führendem Koeffizienten 1 ist, welches jedes Körperelement als Nullstelle hat.

(b) Folgere aus einem geeigneten Satz der Gruppentheorie, daß es für ein geeignetes $m \in \mathbb{N}$ paarweise verschiedene Primzahlen $p_1, ..., p_m$ und eine Zerlegung

$$\mathbb{K}^\times \cong G_{p_1} \oplus G_{p_2} \oplus ... \oplus G_{p_m}$$

gibt, so daß jeder direkte Summand G_{p_k} eine p_k-Gruppe ist.
Erinnerung: *Eine Gruppe G heißt p-Gruppe für eine Primzahl p, falls jedes Element $g \in G$ als Gruppenordnung eine Potenz von p besitzt.*

(c) Zeige, daß jede Untergruppe von $\mathbb{K}^\times$ zyklisch ist.
Hinweis: *Wie viele Nullstellen kann das Polynom $(X^d - 1)$ für $d \in \mathbb{N}$ höchstens haben?*

(d) Zeige, daß jedes $k \in \mathbb{K}$ Nullstelle des Polynoms

$$X^q - X$$

ist und folgere

$$f(X) = X^q - X.$$

Lösung: (a) Offensichtlich ist jedes Element aus $\mathbb{K}$ Nullstelle, offensichtlich ist $\deg(f) = q$ und offensichtlich hat f führenden Koeffizienten $a_q = 0$.

(b) Dieses Resultat findet sich z. B. in [Jan, p. 52 f.]. Wir gehen vom Struktursatz endlich erzeugter abelscher Gruppen aus. Dieser liefert uns einen Isomorphismus

$$\mathbb{K}^\times \cong \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus ... \oplus \mathbb{Z}_{d_n},$$

wobei folgende Teilerrelation gilt:

$$d_1 | d_2 | ... | d_n.$$

Es bezeichne $\{p_1, ..., p_m\}$ die Primteiler von d_n und es sei

$$d_j = \left(p_1^{\epsilon_{j,1}}\right) \cdot \left(p_2^{\epsilon_{j,2}}\right) \cdot ... \cdot \left(p_m^{\epsilon_{j,m}}\right)$$

die Primfaktorzerlegung von d_j. Aus der Teilerrelation erhalten wir, daß die Zahlen $0 \leq \epsilon_{j,k}$ in j monoton wachsen. Weiter wissen wir aus der Gruppentheorie, daß es einen Isomorphismus

$$\mathbb{Z}_{d_j} \cong \mathbb{Z}_{\left(p_1^{\epsilon_{j,1}}\right)} \oplus \mathbb{Z}_{\left(p_2^{\epsilon_{j,2}}\right)} \oplus ... \oplus \mathbb{Z}_{\left(p_m^{\epsilon_{j,m}}\right)}$$

gibt. Somit können wir umsortieren

$$\begin{aligned}
\mathbb{K}^\times &\cong \bigoplus_{i=1}^{n} \mathbb{Z}_{d_i} \\
&\cong \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m} \mathbb{Z}_{\left(p_j^{\epsilon_{j,i}}\right)} \\
&\cong \bigoplus_{j=1}^{m} \bigoplus_{i=1}^{n} \mathbb{Z}_{\left(p_j^{\epsilon_{j,i}}\right)}.
\end{aligned}$$

Mit der Definition

$$G_{p_j} := \bigoplus_{i=1}^{n} \mathbb{Z}_{\left(p_j^{\epsilon_{j,i}}\right)}$$

erhalten wir die gewünschte Zerlegung in p_j-Gruppen.

(c) Wir zeigen, daß jeder direkte Summand G_{p_j} eine zyklische Gruppe ist. Dabei bezeichne $q_j := |G_{p_j}|$ die Anzahl der Elemente von G_{p_j}.
Gibt es ein Element mit Ordnung q_j, so generiert dieses Element G_{p_j}, also ist G_{p_j} zyklisch.
Gibt es kein Element der Ordnung q_j, so existiert eine Potenz $t := p_j^r < q_j$ mit $g^t = 1$ für alle $g \in G_{p_j}$, da die Ordnung eines Elementes die Gruppenordnung teilen muß. Somit hätte das Polynom $X^t - 1$ mehr Nullstellen als es Grad hat, ein Widerspruch, denn $\mathbb{K}$ als Körper ist Integritätsbereich. Somit kann dieser Fall nicht vorkommen.
Da jeder direkte p_j-Summand zyklisch ist und verschiedene Summanden paarweise teilerfremde Ordnung haben, ist auch die direkte Summe zyklisch, also ist $\mathbb{K}^\times$ zyklisch und damit auch jede Untergruppe von $\mathbb{K}^\times$.

(d) Wir unterscheiden zwei Fälle.
Ist $x = 0$, so folgt $\iota_o(X^q - X) = 0^q - 0 = 0$, also ist 0 eine Nullstelle.
Ist $x \neq 0$, so gilt $x \in \mathbb{K}^\times$, also gilt, da $|K^\times| = q - 1$, $x^{q-1} = 1$, also $x^q = x$, also $x^q - x = 0$, also $\iota_x(X^p - X) = 0$ und die erste Behauptung ist gezeigt.
Wir erhalten

$$f(X) = X^q - X,$$

denn beide Polynome haben die gleichen Nullstellen und gleichen führenden Koeffizienten.

Hausübungen

Aufgabe H13 Sei $\mathbb{K}$ ein Körper, $f \in \mathbb{K}[X]$ und $\deg(f) > 1$.

(a) Zeige folgende Abschätzung:

$$\deg(f') \leq \deg(f) - 1.$$

(b) Wann gilt $\deg(f') = \deg(f) - 1$?

(c) Es gelte zusätzlich $\operatorname{char}(\mathbb{K}) = p$ für p prim. Zeige, daß folgende Bedingungen äquivalent sind.

(1) Es gilt $f' = 0$.

(2) Es existiert ein $g \in \mathbb{K}[X]$ mit $f(X) = g(X^p)$.

Lösung: (a) Ist $f = \sum_{k=1}^{n} a_n \cdot X^n$, dann ist $f' = \sum_{k=0}^{n-1} (k+1) \cdot a_{k+1} \cdot X^k$ und der Grad dieses Polynoms ist offensichtlich nicht größer als $n - 1$.

(b) Ist $n \cdot a_n \neq 0$, dann ist der $(n-1)$-te Koeffizient von f' nicht 0, also gilt Gleichheit. Dieses ist genau dann gegeben, wenn n nicht von der Charakteristik von $\mathbb{K}$ geteilt wird.

(c) (1) $\Rightarrow$ (2) Es sei $f' = 0$, so folgt aus

$$f(X) = \sum_{k=0}^{n} a_k \cdot X^k, \quad f'(X) = \sum_{k=0}^{n-1} (k+1) \cdot a_{k+1} \cdot X^k = 0,$$

daß $(k+1) \cdot a_{k+1} = 0$ ist für alle $0 \leq k \leq n-1$. Dies ist nur möglich, wenn bereits einer der Faktoren 0 ist, somit verschwindet entweder a_{k+1} oder $(k+1)$.
Sind alle $a_{k+1} = 0$, dann ist nichts zu zeigen, denn

$$f = a_0 = a_0 \cdot (X^p)^0.$$

Ist ein $a_{k+1} \neq 0$, so folgt $(k+1) \in p{\cdot}\mathbb{Z}$, also $(k+1) = m{\cdot}p$. Damit ist f aber Linearkombination von Monomen mit durch p teilbaren Exponenten, also

$$f = \sum_{j=0}^{\frac{n}{p}} a_{p\cdot j} X^{p\cdot j} = \sum_{j=0}^{\frac{n}{p}} a_{p\cdot j} (X^p)^j.$$

Alle anderen Koeffizienten, für die die verwendete Notation keinen Sinn macht, verschwinden zum Glück. (2) $\Rightarrow$ (1) Es gilt auf Grund der Derivationseigenschaft der Ableitung für ein Polynom $g \in \mathbb{K}[X]$ und eine natürliche Zahl $m > 0$:

$$(g^m)' = \sum_{i=1}^{m} g' \cdot g^{m-1} = m \cdot g' \cdot g^{m-1}.$$

Damit erhalten wir für beliebige Polynome $g, h \in \mathbb{K}[X]$ mit $h(X) = \sum_{k=0}^{n} a_k \cdot X^k$ folgende Rechenregel:

$$\begin{aligned}
[h(g(X))]' &:= \left[\sum_{k=0}^{n} a_k \cdot (g(X))^k\right]' \\
&= \sum_{k=0}^{n} a_k \cdot \left[(g(X))^k\right]' \\
&= \sum_{k=1}^{n} a_k \cdot k \cdot g' \cdot (g(X))^{k-1} \\
&= g' \cdot \left(\sum_{k=1}^{n} a_k \cdot k \cdot (g(X))^{k-1}\right) \\
&= g' \cdot h'(g(X)).
\end{aligned}$$

Mit dieser Version der Kettenregel folgt nun sofort die Behauptung, da $\mathbb{K}$ Charakteristik p hat und alle Koeffizienten von $f(g(X))'$ von p geteilt werden mit der Wahl $g(X) = X^p$.

Aufgabe H14

(a) Charakterisiere alle rationalen Zahlen, die als Nullstellen des Polynoms

$$f(X) = X^3 + \frac{5}{3}X^2 - 9X + 15$$

bzw. alle rationalen Zahlen, die als Nullstellen des Polynoms

$$g(X) = X^3 - \frac{17}{19}X^2 - 121X + \frac{2057}{19}$$

in Frage kommen.

(b) Finde alle rationalen Nullstellen des Polynoms

$$h(X) = X^7 - 2X^6 + X^5 - 2X^4 + X^3 - 2X^2 + X - 2.$$

Lösung: Wir verwenden in dieser Aufgabe ausschließlich, daß eine rationale Nullstelle eines Polynoms aus $\mathbb{Z}[X]$ folgende Bedingungen erfüllen muß: Der Zähler der Nullstelle teilt den letzten Koeffizienten des Polynoms und der Nenner der Nullstelle teilt den führenden Koeffizienten des Polynoms.

(a) Wir skalieren das Polynom, so daß die Koeffizienten ganzzahlig und teilerfremd sind. Dabei bleiben rationale Nullstellen offensichtlich erhalten und das skalierte Polynom ist primitiv.

$$0 = x^3 + \frac{5}{3}x^2 - 9x + 15 \Leftrightarrow 0 = 3x^3 + 5x^2 - 27x + 45.$$

Somit kommen nur die rationalen Zahlen $\frac{a}{b}$ in Frage, mit

$$a \in \text{Teiler}(45) = \{\pm 1, \pm 3, \pm 5, \pm 9, \pm 15, \pm 45\},$$

$$b \in \text{Teiler}(3) = \{\pm 1, \pm 3\}.$$

Der Nenner b kann dabei oBdA positiv gewählt werden und der Bruch gekürzt, somit erhalten wir 16 mögliche Lösungen.
Analog zu f betrachten wir

$$0 = 19X^3 - 17X^2 - 19 \cdot 121X + 2057.$$

Somit kommen nur rationale Zahlen $\frac{a}{b}$ in Frage mit

$$a \in \text{Teiler}(2057) = \{\pm 1, \pm 11, \pm 17, \pm 121, \pm 187, \pm 2057\},$$

$$b \in \{1, 19\}.$$

Da 19 und 2057 teilerfremd sind, erhalten wir 24 mögliche Lösungen.

(b) Analog zu oben sind nur $1, -1, 2, -2$ mögliche Nullstellen. Ausprobieren liefert, daß nur 2 eine Nullstelle obigen Polynoms ist, welches die einzige rationale Nullstelle sein muß.