Einfürung in die Algebra Hausaufgaben Blatt Nr. 11

Jun Wei Tan*

Julius-Maximilians-Universität Würzburg

(Dated: February 1, 2024)

Problem 1. Sei $R := K^{n\times n}$ der Ring der $n \times n$-Matrizen über einem Körper K. Zeigen Sie, dass $\{0\}$ und R die einzigen Ideale von R sind, vgl. Bemerkung 3.13.

Proof. Sei $I \neq \{0\}$ ein Ideal von R. Wir nehmen an, dass $m \in I$ gibt mit m invertierbar. Dann ist $m^{-1} \in R$ und $1 = mm^{-1} \in I$. Sei jetzt $m \in R$ beliebig. Da $1 \in I$, ist $1m = m \in I$, also $I = R$.

Deswegen nehmen wir an, dass I nur nichtinvertierbare Elemente enthält.Sei $m \in I$. Aus dem Spektralsatz bzw. Jordannormalform haben wir eine Zerlegung $m = m_d + m_n$ mit $[m_d, m_n] = 0$, m_d diagonalisierbar und m_n nilpotent. Da $m^n = m_d + m_n \in I$ für alle $n \in \mathbb{N}^*$, enthält I ein diagonalisierbares Element.

Wir diagonalisieren das Element, also I enthält ein diagonales Element, z.B. $\operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n) \in I$. Wir wissen, dass Zeilenumformungen durch Matrixmulplikationen dargestellt werden kann. Durch diese Zeilenumformungen erhalten wir für jedes Diagonalelement zumindest ein Element, das keine Nullstelle in diesem Eintrag besitzt.

Wir additieren alle solche Elemente und erhalten daher eine diagonale Matrix, mit alle diagonale Elemente ungleich Null. Dies ist invertierbar, und die Behauptung folgt. □

Problem 2. Seien R ein kommutativer Ring und $g \in R[x]$ ein normiertes Polynom vom Grad $n \in \mathbb{N}^*$. Sei $I := gR \trianglelefteq R[X]$ das von g erzeugte Ideal von $R[X]$. Zeigen Sie:

(a) Jedes Element des Faktorrings $R[X]/I$ lässt sich in der Form

$$r_0 + r_1X + \ldots, +r_{n-1}X^{n-1} + I \qquad \text{mit gewissen } r_i \in R$$

darstellen. Es gilt also $R[X]/I = \{r_0 + r_1X + \cdots + r_{n-1}X^{n-1} | r_0, \ldots, r_{n-1} \in R\}$.

* jun-wei.tan@stud-mail.uni-wuerzburg.de

(b) Die Elemente $\sum_{i=0}^{n-1} r_i X^i + I$ aus der Menge in Teil (a) sind paarweise verschieden, d.h. für beliebige $r_0, \ldots, r_{n-1}, s_0, \ldots, s_{n-1}$ gilt

$$(r_0, \ldots, r_{n-1}) \neq (s_0, \ldots, s_{n-1}) \implies \sum_{i=0}^{n-1} r_i X^i + I \neq \sum_{i=0}^{n-1} s_i X^i + I.$$

Proof. (a) Per Definition können wir die Elemente als $p + I, p \in R[X]$. Es ist einfach zu zeigen, dass wir oBdA $\text{grad}(p) < n$. Wir betrachten $p + I$ mit grad $p \geq n$. Dann führen wir Division mit Rest durch und erhalten

$$p = gq + r,\ g, r \in R[x], \text{grad } r < n.$$

Es gilt deswegen

$$p + I = (gq + r) + I.$$

Weil $gq \in I$ per Definition, ist $gq + I = I$ und

$$p + I = r + I,$$

also wir dürfen oBdA annehmen, dass grad $p < n$.

(b) Sei die Polynome $r = (r_0, \ldots, r_{n-1}$ und $s = (s_0, \ldots, s_{n-1})$. Falls $r + I = s + I$, wäre $r - s \in I$. Da grad$r$ und grad$(s) < n$ sind, ist grad$(r - s) < n$. $r - s \in I$ liefert dann $r - s = gq$. Aber g ist vom Grad n und gq ist daher vom Grad $\geq n$, ein Widerspruch. □

Problem 3. Zur Abkürzung schreiben wir $\mathbb{Z}_n$ für den Ring $\mathbb{Z}/n\mathbb{Z}$. Zeigen Sie, dass die vier Ringe

$$R_1 := \mathbb{Z}_4,\ R_2 := \mathbb{Z}_2 \times \mathbb{Z}_2,\ R_3 := \mathbb{Z}_2[X]/X^2\mathbb{Z}_2[X],\ R_4 := \mathbb{Z}_2[X]/(X^2 + X + 1)\mathbb{Z}_2[X]$$

paarweise nicht isomorph sind.

Proof. Die Elemente sind

$$\begin{aligned}
\mathbb{Z}_4 :& \overline{0}, \overline{1}, \overline{2}, \overline{3} \\
\mathbb{Z}_2 \times \mathbb{Z}_2 :& (\overline{0}, \overline{0}), (\overline{0}, \overline{1}) \\
& (\overline{1}, \overline{0}), (\overline{1}, \overline{1})
\end{aligned}$$

$$
\begin{aligned}
\mathbb{Z}_2[X]/X^2 :& 0 + X^2, 1 + X^2 \\
& X + X^2, X + 1 + X^2 \\
\mathbb{Z}_2[X]/(X^2+X+1) :& 0 + (X^2+X+1), \\
& 1 + (X^2+X+1), \\
& X + (X^2+X+1), \\
& X + 1 + (X^2+X+1)
\end{aligned}
$$

Es gilt $\overline{1} + \overline{1} = \overline{2} \neq \overline{0}$ in $\mathbb{Z}_4$, aber das additive Neutrale hat immer die Ordnung 2 in die letzte drei. □

Problem 4. Sei R ein kommutativer Ring. Ein Element $a \in R$ heißt *nilpotent*, falls $a^n = 0$ für ein $n \geq 1$ gilt.

(a) Begründen Sie, warum Null in einem Körper das einzige nilpotente Element ist.

(b) Zeigen Sie, dass das *Nullradikal* $N := \{a \in R | a \text{ ist nilpotent}\}$ ein Ideal ist.

(c) Zeigen Sie, dass das Nilradikal in jedem Primideal P von R enthalten ist.

Proof. (a) Sei K ein Körper mit $K \ni a \neq 0$. Da $K \backslash \{0\}$ multiplikativ abgeschlossen sein sollte, wäre $a^k \in K \backslash \{0\}$, also $a^k \neq 0$ für alle $k \in \mathbb{N}^*$

(b) N ist eine additive Untergruppe:

(i) 0 ist nilpotent (siehe oben)

(ii) Sei a nilpotent mit $a^n = 0$. Es gilt dann $(-a)^n = (-1)^n a^n = (-1)^n 0 = 0$.

(iii) Sei a, b nilpotent mit $a^n = b^m = 0$. Da R kommutativ ist, dürfen wir den Binomialsatz verwenden. Wir betrachten

$$(a+b)^{n+m} = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+m-k}.$$

Falls $k \geq n$ wäre, gälte dann $a^k = 0$ und $a^k b^{n+m-k} = 0$. Falls $k \leq n$ wäre, gälte $n + m - k \geq m$ und $b^{n+m-k} = 0$, daher $a^k b^{n+m-k} = 0$. Dann ist $(a+b)^{n+m} = 0$, und $a + b$ ist nilpotent.

Sei jetzt $a \in N, b \in R$ mit $a^n = 0$. Es gilt $(ab)^n = a^n b^n = 0 b^n = 0$.

(c) Sei P ein Ideal von R mit $N \not\subseteq P$. Wir zeigen, dass $P + N \supseteq P \cup N$ ein Ideal ist, also P ist nicht maximal.

Die additive Eigenschaften folgen, da sowohl P als auch N Untergruppen sind. Da die additive Gruppe abelsch ist, ist $P + N = N + P$, also $P + N$ ist eine abelsche Untergruppe der additive Gruppe.

Sei jetzt $p \in P, a \in N, r \in R$, also $p + a \in P + N$. Da sowohl P als auch N Ideale sind, ist

$$r(p + a) = \underbrace{rp}_{\in P} + \underbrace{ra}_{\in N} \in P + N.$$

$P + N$ ist also ein Ideal. Da $N \not\subseteq P$, ist $P \subsetneq P + N$, also P ist nicht maximal. $\square$