

Lösungen zu Zettel 6

Jendrik Stelzner

4. Dezember 2016

Aufgabe 1

Es seien \mathcal{P} ein Repräsentantensystem der Assoziiertheitsklassen der Primelemente von R .

Lemma 1. 1. Für alle $x, y \in R$ und $p \in \mathcal{P}$ gilt $\nu_p(xy) = \nu_p(x) + \nu_p(y)$.

2. Für alle $x, y \in R$ gilt genau dann $x \mid y$, wenn $\nu_p(x) \leq \nu_p(y)$ für alle $p \in \mathcal{P}$.

Beweis. Wir fixieren ein $p \in \mathcal{P}$.

1. Es gibt Primfaktorzerlegungen $x = u_1 \prod_{p \in \mathcal{P}} p^{\nu_p(x)}$ und $y = u_2 \prod_{p \in \mathcal{P}} p^{\nu_p(y)}$. Hieraus ergibt sich für das Produkt xy eine Primfaktorzerlegung

$$xy = u_1 \prod_{p \in \mathcal{P}} p^{\nu_p(x)} \cdot u_2 \prod_{p \in \mathcal{P}} p^{\nu_p(y)} = (u_1 u_2) \prod_{p \in \mathcal{P}} p^{\nu_p(x) + \nu_p(y)},$$

weshalb $\nu_p(xy) = \nu_p(x) + \nu_p(y)$.

2. Gilt $x \mid y$, so gibt es $z \in R$ mit $y = xz$, weshalb

$$\nu_p(y) = \nu_p(xz) = \nu_p(x) + \nu_p(z) \geq \nu_p(x).$$

Gilt andererseits $\nu_p(x) \leq \nu_p(y)$ für alle $p \in \mathcal{P}$, so betrachte man für die existierenden Primfaktorzerlegungen $x = u_1 \prod_{p \in \mathcal{P}} p^{\nu_p(x)}$ und $y = u_2 \prod_{p \in \mathcal{P}} p^{\nu_p(y)}$ mit $u_1, u_2 \in R^\times$ das Element $z := u_1^{-1} u_2 \prod_{p \in \mathcal{P}} p^{\nu_p(y) - \nu_p(x)} \in R$. Für dieses gilt

$$xz = \left(u_1 \prod_{p \in \mathcal{P}} p^{\nu_p(x)} \right) \left(u_1^{-1} u_2 \prod_{p \in \mathcal{P}} p^{\nu_p(y) - \nu_p(x)} \right) = u_2 \prod_{p \in \mathcal{P}} p^{\nu_p(y)} = y,$$

weshalb $x \mid y$. □

Für das Element $z := \prod_{p \in \mathcal{P}} p^{\min(\nu_p(x), \nu_p(y))} \in R$ gilt $\nu_p(z) = \min(\nu_p(x), \nu_p(y))$ für alle $p \in \mathcal{P}$. Deshalb ist z ein größter gemeinsamer Teiler von x und y , denn für jedes $z' \in R$ gilt

$$\begin{aligned} z' \mid x, y &\iff \nu_p(z') \leq \nu_p(x), \nu_p(y) \text{ für alle } p \in \mathcal{P} \\ &\iff \nu_p(z') \leq \min(\nu_p(x), \nu_p(y)) \text{ für alle } p \in \mathcal{P} \\ &\iff \nu_p(z') \leq \nu_p(z) \text{ für alle } p \in \mathcal{P} \\ &\iff z' \mid z. \end{aligned}$$

Aufgabe 2

Für $k, n \in \mathbb{Z}$ schreiben wir im Folgenden $[k]_n$ für die Restklasse von k in $\mathbb{Z}/n\mathbb{Z}$. Das Gleichungssystem

$$\begin{cases} 4x \equiv 5 \pmod{9}, \\ 3x \equiv 10 \pmod{11}, \end{cases}$$

für $x \in \mathbb{Z}$ ist also äquivalent zum Gleichungssystem

$$\begin{cases} [4]_9[x]_9 = [5]_9 \\ [3]_{11}[x]_{11} = [10]_{11} \end{cases}$$

Da 4 und 9 teilerfremd sind, ist $[4]_9 \in \mathbb{Z}/9\mathbb{Z}$ eine Einheit (siehe Übungszettel 4), und es ergibt sich, dass $[4]_9^{-1} = [7]_9$. Für alle $x \in \mathbb{Z}$ ist deshalb

$$[4]_9[x]_9 = [5]_9 \iff [7]_9[4]_9[x]_9 = [7]_9[5]_9 \iff [x]_9 = [8]_9.$$

Analog ergibt sich, dass $[3]_{11} \in \mathbb{Z}/11\mathbb{Z}$ eine Einheit ist, und mit $[3]_{11}^{-1} = [4]_{11}$ ergibt sich für alle $x \in \mathbb{Z}$, dass

$$[3]_{11}[x]_{11} = [10]_{11} \iff [x]_{11} = [7]_{11}.$$

Es gilt also die Lösungen $x \in \mathbb{Z}$ des Gleichungssystems

$$\begin{cases} [x]_9 = [8]_9, \\ [x]_{11} = [7]_{11}, \end{cases}$$

zu finden, also die Urbilder von $([8]_9, [7]_{11}) \in (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z})$ unter dem Ringhomomorphismus

$$\mathbb{Z} \rightarrow (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z}), \quad x \mapsto ([x]_9, [x]_{11}).$$

Da 9 und 11 teilerfremd sind, gibt es nach dem chinesischen Restklassensatz einen Ringisomorphismus

$$\varphi: \mathbb{Z}/99\mathbb{Z} \rightarrow (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z}), \quad [x]_{99} \mapsto ([x]_9, [x]_{11}),$$

und da $5 \cdot 9 + (-4) \cdot 11 = 1$ ist φ^{-1} durch

$$\begin{aligned} \varphi^{-1}: (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z}) &\rightarrow \mathbb{Z}/99\mathbb{Z}, \\ ([x]_9, [y]_{11}) &\mapsto [5 \cdot 9 \cdot y + (-4) \cdot 11 \cdot x]_{99} = [55x + 45y]_{99} \end{aligned}$$

gegeben (man vergleiche dies mit dem Beweis des chinesischen Restklassensatzes aus der Vorlesung). Dieser Isomorphismus bringt das folgende Diagramm zum kommutieren:

$$\begin{array}{ccc} & \mathbb{Z} & \\ \pi_{99} \swarrow & & \searrow (\pi_9, \pi_{11}) \\ \mathbb{Z}/99\mathbb{Z} & \xrightarrow{\varphi} & (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z}) \end{array} \quad (1)$$

Dabei bezeichnet $\pi_n: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, $x \mapsto [x]_n$ für alle $n \in \mathbb{Z}$ die kanonische Projektion. Zusammen mit $\varphi^{-1}([8]_9, [7]_{11}) = [755]_{99} = [62]_{99}$ erhalten wir, dass

$$(\pi_9, \pi_{11})^{-1}([8]_9, [7]_{11}) = \pi_{99}^{-1}(\varphi^{-1}([8]_9, [7]_{11})) = \pi_{99}^{-1}([62]_{99}) = 62 + 99\mathbb{Z}.$$

Dies ist die Lösungsmenge des gegebenen Gleichungssystems.

Bemerkung 2. Aus der Kommutativität der Diagrams (1) ergibt bereits, dass die gesuchte Lösungsmenge von der Form $x_0 + 99\mathbb{Z}$ ist, wobei x_0 eine spezielle Lösung ist. Um eine solche spezielle Lösung zu finden, haben wir die konkrete Berechnung von φ^{-1} genutzt, um $\varphi^{-1}([8]_9, [7]_{11}) = [62]_{99}$ zu bestimmen.

In dem konkreten Beispiel dieser Aufgabe ist es allerdings einfacher, eine spezielle Lösung zu bruteforcen, als φ^{-1} zu berechnen: Möglichen Lösungen der Gleichung $[x]_9 = [8]_9$ sind nämlich

$$8, 17, 26, 35, 44, 53, 62, 71, 80, 89, 98, \dots,$$

und mögliche Lösungen der Gleichung $[x]_{11} = [7]_{11}$ sind

$$7, 18, 29, 40, 51, 62, 73, 84, 95, \dots,$$

woraus sich durch direkten Vergleich die gemeinsame Lösung 62 ergibt.

Aufgabe 6

Wir erinnern an das folgende Resultat aus der Vorlesung:

Lemma 3. Es sei $0 \rightarrow M \xrightarrow{f} P \xrightarrow{g} N \rightarrow 0$ eine kurze exakte Sequenz von R -Moduln. Sind M und N endlich erzeugt, so ist auch P endlich erzeugt.

Es sei $0 \rightarrow M \xrightarrow{f} P \xrightarrow{g} N \rightarrow 0$ eine kurze exakte Sequenz von R -Moduln.

M und N sind noethersch $\implies P$ ist noethersch

Wir fixieren einen Untermoduln $P' \subseteq P$. Es seien $M' := f^{-1}(P')$ und $N' := g(P')$, sowie $f' := f|_{M'}: M' \rightarrow P', m \mapsto f(m)$ und $g' := g|_{P'}: P' \rightarrow N', p \mapsto g(p)$. Die Sequenz

$$0 \rightarrow M' \xrightarrow{f'} P' \xrightarrow{g'} N' \rightarrow 0 \tag{2}$$

ist exakt: Die Injektivität von f' folgt aus der von f , denn Restriktionen von Injektionen sind ebenfalls injektiv. Die Surjektivität von g' ergibt sich aus $\text{im } g' = g'(P') = g(P') = N'$. Die Exaktheit der Sequenz (2) an P' ergibt sich aus

$$\ker g' = P' \cap \ker g = P' \cap \text{im } f = f(f^{-1}(P')) = f(N') = f'(N') = \text{im } f'.$$

Die Untermoduln $M' \subseteq M$ und $N' \subseteq N$ sind endlich erzeugt, da M und N noethersch sind. Zusammen mit der Exaktheit der Sequenz (2) ergibt sich nach Lemma 3, dass auch P' endlich erzeugt ist.