Skript: Algebra

Prof. Dr. Vladimir Lazić

(nach dem Mitschrieb von Marian Dietz im Wintersemester 2018/19)

Inhaltsverzeichnis

1 Ideale, Hauptidealringe, faktorielle Ringe, noethersche Ringe

Integritätsringe

Wir erinnern uns zuerst, dass wir in LA1 Ringe eingeführt haben. In diesem Kurs ist (falls nichts anderes explizit gesagt wird) jeder Ring *kommutativ mit* 1, d.h. es existiert das neutrale Element 1 bezüglich der Multiplikation. Insbesondere, wenn $R \neq \{0\}$ ein kommutativer Ring mit 1 ist, so hat R mindestens zwei verschiedene Elemente: 0 und 1. Wir bezeichnen die Operationen in allen Ringen mit $+$ und $\cdot$; wenn wir mit mehreren Ringen arbeiten, dann soll es klar sein, welche Operation (in welchem Ring) angewendet wird.

In diesem Kapitel untersuchen wir Ringe mit zusätzlichen Eigenschaften.

Definition 1.1. Sei R ein Ring. Ein Element $a \in R$ ist eine *Einheit*, falls a invertierbar bezüglich der Multiplikation ist, d.h. wenn es ein Element $b \in R$ gibt, sodass $ab = 1$. Wir bezeichnen

$$R^* := \{a \in R \mid a \text{ ist eine Einheit}\}.$$

Ein Element $a \in R \setminus R^*$ heißt *Nichteinheit*. Zwei Elemente $a, b \in R$ sind zueinander *assoziiert*, wenn es eine Einheit $c \in R$ gibt, sodass $a = bc$. Assoziiertheit ist offensichtlich eine Äquivalenzrelation auf R.

Lemma 1.2.

(a) Sei $(R, +, \cdot)$ ein Ring. Dann ist $(R^*, \cdot)$ eine Gruppe.

(b) Seien $(R_i, +, \cdot)$ Ringe für $i = 1, \ldots, n$. Wir definieren das ringtheoretische Produkt *der Ringe $R_1, \ldots, R_n$ als die Menge $R_1 \times \cdots \times R_n$ mit komponentenweisen Operation, d.h. für alle $a_i, b_i \in R_i$ setze*

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) := (a_1 + b_1, \ldots, a_n + b_n),$$
$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) := (a_1 b_1, \ldots, a_n b_n).$$

Das Element $(1, \ldots, 1)$ ist die Eins in $R_1 \times \cdots \times R_n$.

Dann ist die Gruppe $R_1^* \times \cdots \times R_n^*$ kanonisch isomorph zur Gruppe $(R_1 \times \cdots \times R_n)^*$.

Beweis. Es ist offensichtlich, dass $1 \in R^*$. Für $a, b \in R^*$ gilt $(ab^{-1})(ba^{-1}) = 1$ und damit $ab^{-1} \in R^*$. Dies zeigt (a).

Zu (b): Es ist offensichtlich, dass die Abbildung

$$R_1^* \times \cdots \times R_n^* \to (R_1 \times \cdots \times R_n)^*, \quad (a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_n)$$

ein wohldefinierter Gruppenisomorphismus ist. □

Ein nicht-kommutativer Ring R ist ein *Schiefkörper*, falls $R^* = R \setminus \{0\}$. Wenn R kommutativ ist, dann ist R ein *Körper*, wie schon in LA1 eingeführt.

Beispiel 1.3. Sei $(\mathbb{H}, +)$ ein 4-dimensionaler $\mathbb{R}$-Vektorraum mit einer Basis $\{e, i, j, k\}$ (normalerweise schreibt man 1 anstatt e), wobei die Multiplikation durch die folgenden Formeln gegeben ist:

$$\begin{aligned} &e^2 = e, \quad i^2 = j^2 = k^2 = -e, \\ &ei = ie = i, \quad ej = je = j, \quad ke = ek = k, \\ &ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j. \end{aligned}$$

Man checkt einfach, dass dann $(\mathbb{H}, +, \cdot)$ ein Schiefkörper ist. Man nennt $\mathbb{H}$ den Schiefkörper der *hamiltonischen Quaternionen*.

Definition 1.4. Ein Element a eines Ringes R heißt *Nullteiler*, falls $a \neq 0$ und es existiert ein $b \in R \setminus \{0\}$ mit $ab = 0$. Ein Ring R heißt *Integritätsring* oder *nullteilerfreier Ring*, falls $R \neq \{0\}$ und R keine Nullteiler besitzt.

Bemerkung 1.5. In anderen Worten, ein Ring R ist Integritätsring genau dann, wenn Folgendes gilt:

$$\text{wenn } ab = 0 \text{ für } a, b \in R, \text{ dann } a = 0 \text{ oder } b = 0.$$

Äquivalent zu dieser Bedingung ist die *Kürzungsregel*:

$$\text{wenn } ab = ac \text{ für } a, b, c \in R, \text{ dann } a = 0 \text{ oder } b = c.$$

Beispiel 1.6.

(a) Jeder Körper ist ein Integritätsring. Der Ring $\mathbb{Z}$ ist ein Integritätsring.

(b) Betrachte die Menge

$$\mathbb{Z}[i\sqrt{5}] := \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}.$$

Man checkt einfach, dass die Menge ein Ring ist. Dies ist ein Integritätsring: Und zwar, seien $a, b, c, d \in \mathbb{Z}$ mit

$$(a + bi\sqrt{5})(c + di\sqrt{5}) = 0.$$

Diese Gleichung ist äquivalent zu

$$(ac - 5bd) + i\sqrt{5}(ad + bc) = 0,$$

welches nur dann möglich ist, wenn

$$ac - 5bd = 0 \quad \text{und} \quad ad + bc = 0. \tag{1}$$

Wenn $a = 0$, so folgt $bd = bc = 0$, und damit $b = 0$ (und so $a + bi\sqrt{5} = 0$) oder $c = d = 0$ (und so $c + di\sqrt{5} = 0$). Auf ähnliche Weise behandelt man den Fall $c = 0$. Wir dürfen also annehmen, dass a und c von Null verschieden sind.

Wenn $a \neq 0$, dann folgt aus der zweiten Gleichung in (1), dass $d = -bc/a$, und wenn man dies in die erste Gleichung einsetzt, bekommt man $a^2 + 5b^2 = 0$. Dies gilt genau dann, wenn $a = b = 0$, ein Widerspruch.

Definition 1.7. Sei R ein Ring und seien $a, b \in R$. Wir sagen, dass *das Element b das Element a teilt*, oder dass b *ein Teiler von a ist*, und schreiben $b \mid a$, wenn ein Element $c \in R$ existiert, sodass $a = bc$.

Definition 1.8. Sei R ein Integritätsring und seien $x_1, \ldots, x_n \in R$.

Wir nennen ein Element $d \in R$ den *größten gemeinsamen Teiler von* $x_1, \ldots, x_n$, und schreiben $d = \mathrm{ggT}(x_1, \ldots, x_n)$, falls:

(a) $d \mid x_i$ für alle $i = 1, \ldots, n$, und

(b) wenn es ein $c \in R$ gibt, sodass $c \mid x_i$ für alle $i = 1, \ldots, n$, so gilt $c \mid d$.

Dieses Element ist eindeutig bis auf Assoziiertheit. Wenn es eine Einheit ist, dann sagen wir, dass $x_1, \ldots, x_n$ *koprim* sind.

Wir nennen ein Element $b \in R$ *kleinstes gemeinsames Vielfaches von* $x_1, \ldots, x_n$, und schreiben $b = \mathrm{kgV}(x_1, \ldots, x_n)$, falls:

(1) $x_i \mid b$ für alle $i = 1, \ldots, n$, und

(2) wenn es ein $c \in R$ gibt, sodass $x_i \mid c$ für alle $i = 1, \ldots, n$, so gilt $b \mid c$.

Dieses Element ist eindeutig bis auf Assoziiertheit.

Definition 1.9. Sei R ein Integritätsring. Die *Charakteristik* von R ist die kleinste positive natürliche Zahl n, sodass

$$n \cdot 1 = \underbrace{1 + \cdots + 1}_{n\text{-mal}} = 0.$$

(Hier ist $n \cdot 1_R$ nur die Notation.) Wir schreiben $\mathrm{char}\, R = n$. Falls es keine solche Zahl gibt, dann ist per Definition die Charakteristik von R gleich Null, $\mathrm{char}\, R = 0$.

Wenn $R \subseteq R'$ zwei Integritätsringe sind, so ist es offensichtlich, dass $\operatorname{char} R = \operatorname{char} R'$.

Analog wie wir es für Körper in LA1 gemacht haben, so beweisen wir:

Lemma 1.10. *Die Charakteristik eines Integritätsringes ist eine Primzahl oder* 0.

Bemerkung 1.11. Sei p eine Primzahl und sei R ein Integritätsring mit $\operatorname{char} R = p$. Dann gilt für alle $a, b \in R$ und $r \in \mathbb{N}$:

$$(a+b)^{p^r} = a^{p^r} + b^{p^r}.$$

Und zwar: Per Induktion nach r genügt es die Aussage für $r = 1$ zu zeigen. Nach der binomischen Formel gilt

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

Per Definition gilt

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$$

Da p prim ist, so ist $k!$ nicht durch p teilbar für $0 < k < p$. Die Zahl $p(p-1)\cdots(p-k+1)$ ist aber offensichtlich durch p teilbar, sodass

$$p \text{ teilt } \binom{p}{k} \quad \text{für } k = 1, \ldots, p-1.$$

Insbesondere ist $\binom{p}{k} a^k b^{p-k} = 0$ für $k = 1, \ldots, p-1$, und die Aussage folgt.

Definition 1.12. Sei K ein Körper der Charakteristik $p > 0$. Dann ist die Abbildung $F\colon K \to K$, $a \mapsto a^p$ ein Körperhomomorphismus nach Bemerkung 1.11. Dieser Homomorphismus heißt *Frobenius-Homomorphismus von* K.

Das nächste Lemma zeigt, wie man neue Integritätsringe bilden kann.

Lemma 1.13. *Sei R ein Integritätsring. Dann ist $R[x]$ auch ein Integritätsring und für jede zwei Polynome $p, q \in R[x]$ gilt*

$$\deg(pq) = \deg p + \deg q.$$

Beweis. Seien

$$p = \sum_{i=0}^{n} p_i x^i \quad \text{und} \quad q = \sum_{i=0}^{m} q_i x^i$$

zwei Polynome in $R[x]$, sodass $p_n \neq 0$ und $q_m \neq 0$. Dann gilt

$$pq = p_n q_m x^{n+m} + \text{Terme der niedrigeren Graden.}$$

Falls $pq = 0$, dann $p_n q_m = 0$, und damit $p_n = 0$ oder $q_m = 0$, da R ein Integritätsring ist, ein Widerspruch. Damit ist $R[x]$ auch Integritätsring und $\deg(pq) = n + m = \deg p + \deg q$. □

Korollar 1.14. *Sei R ein Integritätsring. Dann ist $R[x_1, \ldots, x_n]$ auch ein Integritätsring.*

Beweis. Wir wissen, dass $R[x_1, \ldots, x_n] = \big(R[x_1, \ldots, x_{n-1}]\big)[x_n]$ für jedes $n \in \mathbb{N}$. Damit folgt das Korollar aus dem vorigen Lemma per Induktion nach n. □

Nun konstruieren wir einen minimalen Körper, der einen Integritätsring enthält.

Konstruktion 1.15. Sei R ein Integritätsring. Wir definieren eine Relation auf der Menge $R \times (R \setminus \{0\})$ wie folgt:

$$(a, b) \sim (a', b') \quad \Longleftrightarrow \quad ab' = a'b.$$

Diese Relation ist offensichtlich reflexiv und symmetrisch. Sie ist auch transitiv: Und zwar, sei $(a, b) \sim (a', b')$ und $(a', b') \sim (a'', b'')$. Dann gilt

$$ab' = a'b \quad \text{und} \quad a'b'' = a''b', \tag{2}$$

und somit:

$$a'(ab'') = a(a'b'') = a(a''b') = a''(ab') = a''(a'b) = a'(a''b).$$

Nach der Kürzungsregel gilt $a' = 0$ oder $ab'' = a''b$. Im zweiten Falle folgt sofort, dass $(a, b) \sim (a'', b'')$. Wenn $a' = 0$, so folgt aus (2), dass $ab' = 0$ und $a''b' = 0$, und damit $a = 0$ und $a'' = 0$, da $b' \neq 0$. Insbesondere ist wieder $(a, b) \sim (a'', b'')$. Also, $\sim$ ist auch transitiv, und damit eine Äquivalenzrelation.

Wir definieren

$$Q(R) := \big(R \times (R \setminus \{0\})\big) / \sim .$$

Wir bezeichnen die Äquivalenzklasse von (a, b) als $\frac{a}{b}$ oder a/b. Wir definieren auf $Q(R)$ zwei Operationen: Für alle $a, a' \in R$ und $b, b' \in R \setminus \{0\}$ setzen wir

$$\frac{a}{b} + \frac{a'}{b'} := \frac{ab' + a'b}{bb'} \quad \text{und} \quad \frac{a}{b} \cdot \frac{a'}{b'} := \frac{aa'}{bb'}.$$

Man zeigt einfach, dass $(Q(R), +, \cdot)$ ein Körper ist, der *Quotientenkörper von* R. Wir haben die Injektion

$$R \to Q(R), \quad a \mapsto \frac{a}{1},$$

und damit identifizieren wir R mit dem Bild von R unter dieser Abbildung.

Beispiel 1.16.

(a) Es gilt $Q(\mathbb{Z}) = \mathbb{Q}$.

(b) Sei R ein Integritätsring. Der Quotientenkörper $Q\big(R[X_1, \ldots, X_n]\big)$ wird mit $R(X_1, \ldots, X_n)$ bezeichnet, und heißt der *Körper der rationalen Funktionen in n Unbestimmten über R.*

Ideale und Hauptidealringe

Definition 1.17. Sei $(R, +, \cdot)$ ein Ring. Eine Menge $I \subseteq R$ heißt *Ideal*, wenn:

(a) $(I, +)$ eine Untergruppe von $(R, +)$ ist, und

(b) für alle $r \in R$, $a \in I$ gilt: $ra \in I$.

Beispiel 1.18.

(i) In jedem Ring R sind R und $\{0\}$ Ideale in R. Sie heißen *triviale Ideale* in R.

(ii) Seien I und J zwei Ideale in einem Ring R. Wir definieren:

$$\begin{aligned} I + J &:= \{a + b \mid a \in I, b \in J\}, \\ IJ &:= \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; n \in \mathbb{N}, a_i \in I, b_i \in J \right\}, \\ I \cap J &:= \{a \mid a \in I \text{ und } a \in J\}. \end{aligned}$$

Alle drei sind wieder Ideale in R und es gilt $IJ \subseteq I \cap J$. (Übung)

(iii) Sei $\mathcal{A}$ eine Familie von Idealen in einem Ring R. Definiere

$$\sum_{I_i \in \mathcal{A}} I_i := \left\{ \sum a_i \;\middle|\; a_i \in I_i \text{ für jedes } i;\ a_i \neq 0 \text{ für nur endlich viele } i \right\}.$$

Dies ist ein Ideal in R.

(iv) Sei $I_1 \subseteq I_2 \subseteq \dots$ eine aufsteigende Kette von Idealen in R. Dann ist die Menge $I = \bigcup_{j \in \mathbb{N}} I_j$ ein Ideal in R. Und zwar: seien $a, b \in I$ und $r \in R$. Dann existieren $i_1, i_2 \in \mathbb{N}_{>0}$, sodass $a \in I_{i_1}, b \in I_{i_2}$. Setze $j_0 := \max\{i_1, i_2\}$. Dann gilt $a, b \in I_{j_0}$, und damit gilt

$$a - b \in I_{j_0} \subseteq I \quad \text{und} \quad ra \in I_{j_0} \subseteq I,$$

da I_{j_0} ein Ideal ist. Dies impliziert, dass I ein Ideal ist.

(v) Sei R ein Ring. Für jedes $a \in R$ definiere

$$(a) := \{ra \mid r \in R\}.$$

Dies ist ein Ideal in R; wir bezeichnen es auch mit aR. Zum Beispiel: für $R = \mathbb{Z}$ und $a = 2$ ist das Ideal $(2) = 2\mathbb{Z}$ das Ideal aller geraden Zahlen in $\mathbb{Z}$.

(vi) Ein Ideal $I \subseteq R$ heißt *Hauptideal*, falls es ein Element $a \in R$ gibt, sodass $I = (a)$. Dann sagen wir auch, dass I vom Element a erzeugt wird.

(vii) Seien $a_1, \dots, a_n$ Elemente in einem Ring R. Dann ist

$$(a_1, \dots, a_n) := a_1R + \dots + a_nR = \left\{ \sum_{i=1}^{n} a_i r_i \;\middle|\; r_i \in R \right\}$$

ein *von $a_1, \dots, a_n$ erzeugtes Ideal in R*.

(viii) Für jede Untermenge $\{a_i \mid i \in \mathcal{A}\}$ eines Ringes R können wir das *von $\{a_i \mid i \in \mathcal{A}\}$ erzeugte Ideal* betrachten:

$$(a_i)_{i \in \mathcal{A}} := \sum_{i \in \mathcal{A}} a_i R.$$

Sei I ein Ideal in R. Eine Familie $\{a_i \mid i \in \mathcal{A}\} \subseteq I$ heißt *Erzeugendensystem von I*, wenn $I = (a_i)_{i \in \mathcal{A}}$. Man nennt I *endlich erzeugt*, wenn I ein endliches Erzeugendensystem besitzt.

Definition 1.19. Ein Ring R heißt *Hauptidealring*, wenn R ein Integritätsring ist und jedes Ideal in R ist ein Hauptideal.

Beispiel 1.20.

(a) Jeder Körper K ist ein Hauptidealring, da K nur triviale Ideale besitzt. Und zwar: Sei $I \subseteq K$ ein Ideal. Ohne Beschränkung der Allgemeinheit dürfen wir annehmen, dass $I \neq \{0\}$. Wähle ein Element $a \in I \setminus \{0\}$. Dann ist offensichtlich $(a) \subseteq I$. Aber $(a) = K$, da für jedes $r \in K$ gilt

$$r = r \cdot 1 = ra^{-1}a \in (a).$$

Folglich gilt $I = K$.

(b) Der Ring $\mathbb{Z}$ ist ein Hauptidealring. Und zwar: Sei $I \subseteq \mathbb{Z}$ ein Ideal; Ohne Beschränkung der Allgemeinheit dürfen wir annehmen, dass $I \neq \{0\}$. Sei m die kleinste positive Zahl in I und sei $a \in I$ ein beliebiges Element. Nach dem Satz über Division mit Rest existieren $q, r \in \mathbb{Z}$ mit $0 \leq r < m$, sodass $a = mq + r$. Aber dann gilt $r = a - mq \in I$, und somit ist $r = 0$ per Definition von m. Dies zeigt, dass $a = mq \in (m)$, und damit ist $I = (m)$ ein Hauptideal in R.

(c) Der Ring $\mathbb{Z}[x]$ ist kein Hauptidealring. Und zwar, betrachte das Ideal $(2, x) \subseteq \mathbb{Z}[x]$. Es ist einfach zu sehen, dass

$$(2, x) = \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; a_0 \text{ ist eine gerade Zahl} \right\}.$$

Insbesondere gilt $2 \in (2, x)$. Wäre $(2, x)$ ein Hauptideal, z.B. $(2, x) = (a)$ für ein $a \in \mathbb{Z}[x]$, so wäre $2 \in (a)$, und damit gäbe es ein Polynom $b \in \mathbb{Z}[x]$ mit $ab = 2$. Aber dann wäre $a \in \{\pm 1, \pm 2\}$, und damit entweder

$$(a) = (1) = \mathbb{Z}[x]$$

oder

$$(a) = (2) = \left\{ \sum a_i x^i \mid a_i \text{ ist eine gerade Zahl für alle } i \right\}.$$

In beiden Fällen bekämen wir einen Widerspruch.

Lemma 1.21. *Seien (a) und (b) zwei Hauptideale in einem Integritätsring R. Dann gilt $(a) = (b)$ genau dann, a und b assoziiert sind.*

Beweis.

$\Longleftarrow$: Diese Richtung ist klar; vergleiche mit Beispiel 1.20(a).

$\Longrightarrow$: Ohne Beschränkung der Allgemeinheit dürfen wir annehmen, dass (a) und (b) von $\{0\}$ verschieden sind. Wenn $(a) = (b)$, so ist insbesondere $a \in (b)$, und damit existiert $c \in R$ mit $a = bc$. Auf ähnliche Weise existiert $c^* \in R$ mit $b = ac^*$. Aus dieser zwei Gleichungen folgt $b = (bc)c^* = b(cc^*)$, und die Kürzungsregel ergibt $cc^* = 1$. Damit ist c eine Einheit. □

In LA1 haben wir Ringhomomorphismen eingeführt. Ein injektiver Ringhomomorphismus heißt *Monomorphismus*; ein surjektiver Ringhomomorphismus heißt *Epimorphismus*; ein bijektiver Ringhomomorphismus heißt *Isomorphismus*. Wir bezeichnen zwei isomorphe ringe R und R' mit $R \cong R'$. Wenn R ein Ring ist, so heißt ein Isomorphismus $R \to R$ *Automorphismus von* R. Wir bezeichnen

$$\mathrm{Aut}(R) := \{\sigma \colon R \to R \mid \sigma \text{ ist ein Automorphismus}\};$$

ähnliche Definition gilt für Automorphismen einer Gruppe.

Lemma 1.22. *Sei* $\varphi \colon (R, +, \cdot) \to (R', +, \cdot)$ *ein Ringhomomorphismus. Dann gilt:*

(1) $\ker \varphi$ *ist ein Ideal in* R*,*

(2) $\mathrm{Im}\, \varphi$ *ist ein Unterring von* R'*,*

(3) φ *induziert den Gruppenhomomorphismus* $\varphi|_{R^*} \colon (R^*, \cdot) \to \big((R')^*, \cdot\big)$.

Beweis.

(1) Wir wissen aus LA1, dass $(\ker \varphi, +)$ eine Untergruppe von $(R, +)$ ist. Sei nun $a \in \ker \varphi$ und $r \in R$. Dann gilt:

$$\varphi(ra) = \varphi(r) \underbrace{\varphi(a)}_{=0} = 0,$$

und somit gilt $ra \in \ker \varphi$. Also, $\ker \varphi$ ist ein Ideal in R.

(2) ist einfach.

(3) Sei $r \in R^*$. Dann existiert $q \in R^*$ mit $rq = 1$, und somit

$$\varphi(r)\varphi(q) = \varphi(rq) = \varphi(1) = 1,$$

sodass $\varphi(r) \in (R')^*$. Wir bekommen also die Abbildung $\varphi|_{R^*} \colon R^* \to (R')^*$. Es ist einfach zu zeigen, dass diese Abbildung ein Gruppenhomomorphismus ist.

Dies zeigt das Lemma. □

Lemma 1.23. *Sei K ein Körper und $R \neq \{0\}$ ein Ring. Dann ist jeder Homomorphismus $\varphi\colon K \to R$ injektiv. Insbesondere ist jeder Homomorphismus zwischen zwei Körpern injektiv.*

Beweis. Nach Lemma 1.22(a) ist $\ker\varphi$ ein Ideal in K. Aber nach Beispiel 1.20(a) hat K genau zwei Ideale: $\{0\}$ und K. Wenn $\ker\varphi = \{0\}$, so ist φ injektiv. Wenn $\ker\varphi = K$, so gilt $\operatorname{Im}\varphi = \{0\}$, welches der Gleichung $\varphi(1) = 1$ widerspricht. □

Beispiel 1.24. Zu jedem Ring R gibt es genau einen Ringhomomorphismus $\varphi\colon \mathbb{Z} \to R$. Und zwar, da $\varphi(1) = 1_R$, so gilt für jedes $n \in \mathbb{N}$:

$$\varphi(n) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{n\text{-mal}} = n \cdot 1_R$$

und

$$\varphi(-n) = -\varphi(n) =: -n \cdot 1_R.$$

Also der Homomorphismus φ ist eindeutig bestimmt.

Homomorphiesatz

Konstruktion 1.25. Sei R ein Ring und sei $I \subseteq R$ ein Ideal. Definiere R/I als Gruppe bezüglich der Operation $+$. Zur Erinnerung, die Addition in R/I ist definiert durch die Formel

$$(x + I) + (y + I) := (x + y) + I \quad \text{für alle } x, y \in R.$$

Nun definieren wir die Multiplikation in R/I durch die Formel

$$(x + I) \cdot (y + I) := x \cdot y + I \quad \text{für alle } x, y \in R.$$

Diese Operation ist wohldefiniert: Und zwar, wir müssen zeigen, dass sie von der Wahl von x und y unabhängig ist. Seien $x', y' \in R$ mit der Eigenschaft, dass

$$x + I = x' + I \quad \text{und} \quad y + I = y' + I.$$

Wie wir aus LA1 wissen, diese Gleichungen sind äquivalent zu $x - x' \in I$ und $y - y' \in I$, und damit existieren $z, w \in I$, sodass

$$x' = x + z \quad \text{und} \quad y' = y + w.$$

Deswegen gilt:

$$\begin{aligned}(x'+I)(y'+I) &:= x'y'+I = (x+z)(y+w)+I \\ &= xy + \underbrace{xw}_{\in I} + \underbrace{zy}_{\in I} + \underbrace{zw}_{\in I} + I \\ &= xy + I =: (x+I)(y+I).\end{aligned}$$

Damit ist die Multiplikation wohldefiniert und diese Addition und Multiplikation geben der Menge R/I die Struktur eines kommutativen Ringes. Die Eins in R/I ist das Element $1+I$. Der Ring R/I ist der *Faktorring R modulo I*. Die *kanonische Projektion* ist die Abbildung

$$\pi\colon R \to R/I, \quad r \mapsto r+I.$$

Notation 1.26. Sei R ein Ring und sei I ein Ideal in R. Dann bezeichnen wir die Klasse eines Elementes $a \in R$ im Ring R/I mit $[a]$. In dieser Notation gilt: $[a+b] = [a]+[b]$ und $[ab] = [a][b]$ für $a, b \in R$. Es gilt $[a] = [b]$ genau dann, wenn $a - b \in I$, und in diesem Falle schreiben wir auch

$$a \equiv b \pmod{I},$$

und sagen, dass *a und b kongruent modulo I sind*. Insbesondere, wenn $R = \mathbb{Z}$, so ist jedes Ideal $I \subseteq \mathbb{Z}$ ein Hauptideal, und es gibt $m \in \mathbb{Z}$ mit $I = (m)$. Dann schreiben wir $a \equiv b \pmod{m}$, wenn $m \mid (a-b)$, welches mit der Notation oben konsistent ist.

Satz 1.27 (Homomorphiesatz)**.** *Sei $\varphi\colon R \to R'$ ein Ringhomomorphismus und sei $I \subseteq R$ ein Ideal mit $I \subseteq \ker\varphi$. Sei $\pi\colon R \to R/I$ die kanonische Projektion. Dann gibt es einen eindeutig bestimmten Homomorphismus*

$$\overline{\varphi}\colon R/I \to R',$$

sodass das Diagramm

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & R' \\ & \searrow^{\pi} & \uparrow{\scriptstyle \overline{\varphi}} \\ & & R/I \end{array}$$

kommutiert. Ferner gilt:

(1) $\operatorname{Im}\varphi = \operatorname{Im}\overline{\varphi}$,

(2) $\ker\overline{\varphi} = \pi(\ker\varphi)$,

(3) $\ker\varphi = \pi^{-1}(\ker\overline{\varphi})$.

Insbesondere ist $\overline{\varphi}$ genau dann injektiv, wenn $I = \ker\varphi$. In diesem Falle gibt es den Ringisomorphismus

$$R/\ker\varphi \cong \operatorname{Im}\varphi.$$

Beweis. Für jedes $x \in R$ definieren wir $\overline{\varphi}\colon R/I \to R'$ durch die Formel $\overline{\varphi}\big([x]\big) := \varphi(x)$. Dies ist wohldefiniert: wenn $[x] = [x']$ für $x, x' \in R$, dann $x - x' \in I \subseteq \ker\varphi$, sodass $\varphi(x - x') = 0$ und somit $\varphi(x) = \varphi(x')$.

Das Diagramm oben ist offensichtlich per Konstruktion kommutativ und (1) ist auch klar.

Zu (2): Sei $x \in R$. Dann ist $[x] \in \ker\overline{\varphi}$ äquivalent zu $0 = \overline{\varphi}\big([x]\big) = \varphi(x)$, d.h. zu $x \in \ker\varphi$. Daraus folgen (2) und (3) und der Rest des Satzes. □

Beispiel 1.28. Für jede natürliche Zahl m ist die Gruppe $\mathbb{Z}/m\mathbb{Z}$, die wir in LA1 eingeführt haben, ein Ring: Für alle $k, \ell \in \mathbb{Z}$ sind die Operationen durch die Formel

$$[k] + [\ell] := [k + \ell], \quad [k][\ell] := [k\ell]$$

gegeben. Dies ist nach dem Homomorphiesatz wohldefiniert. Wir merken hier, dass $m\mathbb{Z}$ das Hauptideal (m) in $\mathbb{Z}$ ist, also $\mathbb{Z}/m\mathbb{Z}$ ist der Faktorring $\mathbb{Z}/(m)$.

Nun untersuchen wir, wann der Ring $\mathbb{Z}/m\mathbb{Z}$ ein Körper ist:

Satz 1.29. *Sei $m \in \mathbb{N}_{>0}$. Dann sind äquivalent:*

(1) m ist eine Primzahl,

(2) $\mathbb{Z}/m\mathbb{Z}$ ist ein Integritätsring,

(3) $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper.

Beweis.

(1) $\Longrightarrow$ (2): Angenommen, m ist eine Primzahl. Seien $[a], [b] \in \mathbb{Z}/m\mathbb{Z}$, sodass $[ab] = [a][b] = [0]$. Dann gilt $m \mid ab$, und damit $m \mid a$ oder $m \mid b$. Somit ist $[a] = [0]$ oder $[b] = [0]$. Dies zeigt, dass $\mathbb{Z}/m\mathbb{Z}$ ein Integritätsring ist.

(2) $\Longrightarrow$ (3): Sei $\alpha \in \mathbb{Z}/m\mathbb{Z} \setminus \{[0]\}$ und betrachte die Multiplikationsabbildung

$$\theta_\alpha\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \quad \beta \mapsto \alpha\beta.$$

Wir zeigen zuerst, dass θ_α injektiv ist. Sei $\beta \in \ker \theta_\alpha$. Dann gilt $\alpha\beta = \theta_\alpha(\beta) = [0]$. Da $\mathbb{Z}/m\mathbb{Z}$ ein Integritätsring ist, so folgt $\beta = [0]$.

Da die Menge $\mathbb{Z}/m\mathbb{Z}$ endlich ist und θ_α injektiv ist, so folgt, dass θ_α surjektiv ist, und somit existiert $\gamma \in \mathbb{Z}/m\mathbb{Z}$, sodass $\theta_\alpha(\gamma) = [1]$. Dies ist äquivalent zu $\alpha\gamma = [1]$, welches zeigt, dass α invertierbar ist. Da dies gilt für jedes beliebige Element $\alpha \in \mathbb{Z}/m\mathbb{Z} \setminus \{[0]\}$, so ist $\mathbb{Z}/m\mathbb{Z}$ ein Körper.

(3) $\Longrightarrow$ (1): Angenommen, $\mathbb{Z}/m\mathbb{Z}$ ein Körper. Wäre m keine Primzahl, so gäbe es natürliche Zahlen $1 < k, \ell < m$, sodass $k\ell = m$. Dann wäre

$$[0] = [m] = [k\ell] = \underbrace{[k]}_{\neq [0]} \underbrace{[\ell]}_{\neq [0]},$$

ein Widerspruch. Damit ist m eine Primzahl. □

Wenn $p \in \mathbb{N}$ eine Primzahl ist, so bezeichnen wir den Körper $\mathbb{Z}/p\mathbb{Z}$ mit $\mathbb{F}_p$. Es ist einfach zu sehen, dass $\operatorname{char} \mathbb{F}_p = p$.

Definition 1.30. Sei K ein Körper. Der kleinste Körper $P \subseteq K$ heißt *Primkörper* von K. Äquivalent: Der Primkörper ist der Durchschnitt aller Körper, die in K enthalten sind.

Es ist einfach zu sehen, dass der Primkörper von $\mathbb{F}_p$ er selbst ist, und dass der Primkörper von $\mathbb{Q}$ er selbst ist: dies folgt aus der Tatsache, dass der Primkörper zwangsweise alle Brüche der Form $m \cdot 1/n \cdot 1$ enthalten muss, wobei $n \cdot 1 \neq 0$.

Satz 1.31. *Sei K ein Körper und sei $P \subseteq K$ der Primkörper von K. Dann gilt:*

(i) $\operatorname{char} K = p > 0 \quad \Longleftrightarrow \quad P \cong \mathbb{F}_p$,

(ii) $\operatorname{char} K = 0 \quad \Longleftrightarrow \quad P \cong \mathbb{Q}$.

Beweis. Die Implikationen „$\Longleftarrow$“ in (i) und (ii) sind trivial.

Nun zeigen wir die umgekehrten Implikationen. Betrachte den kanonischen Homomorphismus

$$\varphi \colon \mathbb{Z} \to K, \quad n \mapsto n \cdot 1.$$

Dann ist $\ker \varphi \subseteq \mathbb{Z}$ ein Hauptideal, sodass $\ker \varphi = p\mathbb{Z}$ für $p \in \mathbb{N}$. Der Ring $\operatorname{Im} \varphi \subseteq K$ ist ein Integritätsring, da K ein Integritätsring ist. Nach dem Homomorphiesatz gilt $\operatorname{Im} \varphi \cong \mathbb{Z}/p\mathbb{Z}$, und somit ist, nach Satz 1.29, p entweder eine Primzahl und $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper, oder $p = 0$.

Wenn $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, dann $P \subseteq \operatorname{Im} \varphi \cong \mathbb{F}_p$, und somit $P \cong \mathbb{F}_p$.

Wenn $p = 0$, so ist $\ker \varphi = (0)$ und damit ist φ injektiv. Somit gilt $\varphi(\mathbb{Z}) \cong \mathbb{Z}$ und $Q\big(\varphi(\mathbb{Z})\big) \cong Q(\mathbb{Z}) = \mathbb{Q}$. Da $P \subseteq Q\big(\varphi(\mathbb{Z})\big)$, so folgt $P \cong \mathbb{Q}$. □

Primideale

Satz 1.29 besagt, dass m ein Primzahl ist genau dann, wenn der Faktorring $\mathbb{Z}/(m)$ ein Integritätsring, bzw. ein Körper ist. Dies motiviert die folgende Definition.

Definition 1.32. Sei R ein Ring.

(i) Ein Ideal $I \subseteq R$ heißt *prim* oder *Primideal*, wenn $I \neq R$ und für alle $a, b \in R$ gilt:

$$ab \in I \quad \Longrightarrow \quad a \in I \text{ oder } b \in I.$$

(ii) Ein Ideal $I \subseteq R$ heißt *maximal*, wenn $I \neq R$ und wenn gilt: Ist $J \subseteq R$ ein Ideal mit $I \subseteq J \subseteq R$, dann entweder $I = J$ oder $J = R$.

Satz 1.33. *Sei R ein Ring.*

(i) Ein Ideal $I \subseteq R$ ist genau dann ein Primideal, wenn R/I ein Integritätsring ist.

(ii) Ein Ideal $I \subseteq R$ ist genau dann maximal, wenn R/I ein Körper ist. Insbesondere ist jedes maximale Ideal auch prim.

Beweis. Wir zeigen zuerst (i). Angenommen, I ist ein Primideal. Seien $a, b \in R$, sodass $[ab] = [a][b] = I$. Dann gilt $ab \in I$, und damit $a \in I$ oder $b \in I$. Somit ist $[a] = [0]$ oder $[b] = [0]$, welches zeigt, dass R/I ein Integritätsring ist.

Nun nehmen wir an, dass R/I ein Integritätsring ist. Wäre I kein Primideal, so gäbe es $a, b \in R$, sodass $ab \in I$, aber $a, b \notin I$. Dann wäre

$$[0] = [ab] = \underbrace{[a]}_{\neq [0]} \underbrace{[b]}_{\neq [0]},$$

ein Widerspruch. Damit ist I ein Primideal.

Nun zeigen wir (ii). Sei I maximal und sei $a \in R$, sodass $[a] \neq [0]$ in R/I, d.h. $a \in R \setminus I$. Dann gilt $I \subsetneq I + aR$, und somit $I + aR = R$. Insbesondere, es existieren $r \in R$ und $m \in I$, sodass $m + ar = 1$. Dann gilt:

$$[1] = [m + ar] = [ar] = [a][r].$$

Damit ist $[a]$ eine Einheit in R/I und so ist R/I ein Körper.

Nun nehmen wir an, dass R/I ein Körper ist, aber I ist nicht maximal. Dann gibt es ein Ideal $M \subsetneq R$ mit $I \subsetneq M$. Wähle $a \in M \setminus I$. Dann ist

$[a] \neq [0]$ in R/I, und somit ist $[a]$ invertierbar in R/I, d.h. es gibt ein $r \in R$, sodass

$$[ar] = [a][r] = [1].$$

Dies impliziert, dass $ar - 1 \in I$, und so gibt es $m \in I$ mit $m + ar = 1$. Aber dann gilt:

$$R = (1) = (m + ar) \subseteq (m) + aR \subseteq I + aR \subseteq M \subseteq R,$$

und damit $M = R$, Widerspruch. Dies zeigt (ii). □

Definition 1.34. Sei R ein Ring. Zwei Ideale I und J in R heißen *koprim*, falls $I + J = R$. D.h. es gibt $i \in I$ und $j \in J$ mit $i + j = 1$.

Satz 1.35 (Chinesischer Restsatz)**.** *Sei R ein Ring und seien $I_1, \dots, I_n \subseteq R$ paarweise koprime Ideale in R. Seien $\pi_i \colon R \to R/I_i$ die kanonischen Projektionen für alle $i = 1, \dots, n$. Dann ist der Homomorphismus*

$$\varphi \colon R \to R/I_1 \times \cdots \times R/I_n, \quad x \mapsto \big(\pi_1(x), \dots, \pi_n(x)\big)$$

surjektiv und es gilt $\ker \varphi = \bigcap_{i=1}^{n} I_i$*. Nach dem Homomorphiesatz induziert damit φ den Isomorphismus*

$$\overline{\varphi} \colon R \Big/ \bigcap_{i=1}^{n} I_i \cong R/I_1 \times \cdots \times R/I_n.$$

Beweis. Fixiere ein i. Da die Ideale I_i und I_j für $j \neq i$ koprim sind, so gibt es für alle $j \neq i$ Elemente $a_j \in I_i$ und $a'_j \in I_j$ mit $a_j + a'_j = 1$. Wenn man das Produkt $\prod_{j \neq i} (a_j + a'_j)$ ausmultipliziert, so erhalten alle Summanden mindestens ein a_j (und damit gehören zu I_i), bis auf den Summand $a'_1 \dots a'_{i-1} a'_{i+1} \dots a'_n \in \bigcap_{j \neq i} I_j$. So gilt

$$1 = \prod_{j \neq i} (a_j + a'_j) \in I_i + \bigcap_{j \neq i} I_j,$$

und damit $R = (1) \subseteq I_i + \bigcap_{j \neq i} I_j \subseteq R$. Dies zeigt, dass $I_i + \bigcap_{j \neq i} I_j = R$, und deswegen sind für alle $i = 1, \dots, n$ die Ideale I_i und $\bigcap_{j \neq i} I_j$ koprim.

Insbesondere, für alle $i = 1, \ldots, n$ gibt es $d_i \in I_i$ und $e_i \in \bigcap_{j \neq i} I_i$, sodass $d_i + e_i = 1$. Da $e_i \in I_j$ für $j \neq i$, so gilt

$$\pi_j(e_i) = 0 \quad \text{für } j \neq i. \tag{3}$$

Ferner:

$$1 = \pi_i(1) = \pi_i(d_i + e_i) = \underbrace{\pi_i(d_i)}_{=0, \text{ da } d_i \in I_i} + \pi_i(e_i) = \pi_i(e_i)$$

also

$$\pi_i(e_i) = 1. \tag{4}$$

Sei nun $(r_1, \ldots, r_n) \in R/I_1 \times \cdots \times R/I_n$, und wähle $s_i \in R$ mit $s_i + I_i = r_i$, d.h. die Klasse von s_i in R/I_i ist r_i. Insbesondere, $\pi_i(s_i) = r_i$. Dann gilt für jedes i:

$$\begin{aligned}\varphi(s_i e_i) &= \big(\pi_1(s_i e_i), \ldots, \pi_n(s_i e_i)\big) = \big(\pi_1(s_i)\pi_1(e_i), \ldots, \pi_n(s_i)\pi_n(e_i)\big) \\ &= \big(0, \ldots, 0, \pi_i(s_i), 0, \ldots, 0\big) = (0, \ldots, 0, r_i, 0, \ldots, 0),\end{aligned}$$

wobei wir (3) und (4) benutzt haben. Dies impliziert:

$$\varphi\left(\sum_{i=1}^{n} s_i e_i\right) = \sum_{i=1}^{n} \varphi(s_i e_i) = \sum_{i=1}^{n} (0, \ldots, 0, r_i, 0, \ldots, 0) = (r_1, \ldots, r_n),$$

und damit ist φ surjektiv.

Schließlich, $x \in \ker \varphi$ genau dann, wenn $\pi_i(x) = 0$ für alle $i = 1, \ldots, n$, oder äquivalent, wenn $x \in \bigcap_{i=1}^{n} \ker \pi_i = \bigcap_{i=1}^{n} I_i$. Damit ist $\ker \varphi = \bigcap_{i=1}^{n} I_i$. □

Wir werden später eine passende Formulierung des Chinesischen Restsatzes im Ring $\mathbb{Z}$ finden.

Euklidische Ringe

Definition 1.36. Sei R ein Integritätsring. Angenommen, es existiert eine Abbildung $\delta\colon R \setminus \{0\} \to \mathbb{N}$ mit der folgenden Eigenschaft: Für alle $f \in R$ und $g \in R \setminus \{0\}$ gibt es $q, r \in R$, sodass

$$f = gq + r \quad \text{und} \quad \delta(r) < \delta(g) \text{ oder } r = 0;$$

dies bezeichnen wir als *Division von f durch g mit Rest r*. Dann heißt R *euklidischer Ring* und δ *Gradabbildung*. Der Wert $\delta(a)$ heißt *Grad von a*, für jedes $a \in R \setminus \{0\}$.

Beispiel 1.37.

(a) Der Ring $\mathbb{Z}$ ist ein euklidischer Ring mit der Gradabbildung $\delta\colon \mathbb{Z} \setminus \{0\} \to \mathbb{N},\ r \mapsto |r|$.

(b) Sei K ein Körper. Dann ist der Polynomring $K[x]$ ein euklidischer Ring mit der Gradabbildung $\delta\colon K[x] \setminus \{0\} \to \mathbb{N},\ f \mapsto \deg f$.

(c) Betrachte den *Ring der ganzen Gaußschen Zahlen*:

$$\mathbb{Z}[i] := \{x + iy \mid x, y \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

Dies ist ein euklidischer Ring: Und zwar, definiere die Gradabbildung

$$\delta\colon \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}, \quad x + iy \mapsto x^2 + y^2 = |x + iy|^2.$$

Seien $f \in \mathbb{Z}[i]$ und $g \in \mathbb{Z}[i]\setminus\{0\}$. Dann ist $f/g \in \mathbb{C}$, und es gibt $x, y \in \mathbb{Z}$ mit

$$\left|\frac{f}{g} - (x + iy)\right| \leq \frac{\sqrt{2}}{2};$$

d.h. $x + yi$ ist eine der komplexen Zahlen mit ganzen reellen und imaginären Teilen, die der Zahl f/g am nächsten ist. Setze $q := x + iy$ und $r := f - qg$. Dann gilt $r = 0$ oder

$$\delta(r) = |r|^2 = |f - qg|^2 = |g|^2 \left|\frac{f}{g} - q\right|^2 < |g|^2 = \delta(g),$$

welches die Aussage zeigt.

Satz 1.38. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Sei R ein euklidischer Ring mit der Gradabbildung δ und sei $I \subseteq R$ ein Ideal. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass $I \neq 0$. Wähle $b \in I \setminus \{0\}$ mit dem kleinsten Grad.

Sei $a \in I$. Dann gibt es $q, r \in R$, sodass $a = bq + r$ und $\delta(r) < \delta(b)$ oder $r = 0$. Aber dann gilt

$$r = \underbrace{a}_{\in I} - \underbrace{bq}_{\in I} \in I,$$

und somit $r = 0$ per Wahl von b. Deswegen gilt $a = bq \in (b)$, welches die Inklusion $I \subseteq (b)$ zeigt. Da trivialerweise $(b) \subseteq I$, so gilt $I = (b)$, und damit ist jedes Ideal in R ein Hauptideal. □

Korollar 1.39. *Sei K ein Körper. Dann ist der Polynomring $K[x]$ ein Hauptidealring.*

Beweis. Folgt aus Beispiel 1.6(b) und Satz 1.38. □

Nun werden wir sehen, wie man in einem euklidischen Ring größte gemeinsame Teiler berechnen kann.

Konstruktion 1.40 (Euklidischer Algorithmus)**.**

Sei R ein euklidischer Ring. Für zwei Elemente $x, y \in R \setminus \{0\}$ betrachten wir die Folge $(z_n)_{n\in\mathbb{N}}$ von Elementen in R, die wir induktiv definieren wie folgt: Setze

$$z_0 := x \quad \text{und} \quad z_1 := y.$$

Seien z_i schon definiert für $i \leq n$. Dann setze

$$z_{n+1} := \begin{cases} \text{der Rest in der Division von } z_{n-1} \text{ durch } z_n, & \text{falls } z_n \neq 0, \\ 0, & \text{sonst.} \end{cases}$$

In anderen Worten, für alle $n \in \mathbb{N}_{>0}$ mit $z_n \neq 0$, existiert ein $q_{n+1} \in R$, sodass

$$z_{n-1} = z_n q_{n+1} + z_{n+1} \quad \text{und } \delta(z_{n+1}) < \delta(z_n) \text{ oder } z_{n+1} = 0. \qquad (*_{n+1})$$

Dieser Prozess muss irgendwann aufhören, da die Zielmenge der Abbildung δ die Menge $\mathbb{N}$ ist, die das kleinste Element besitzt. In anderen Worten, es existiert die kleinste natürliche Zahl $m \in \mathbb{N}$ mit der Eigenschaft, dass $z_{m+1} = 0$.

Wir behaupten, dass

$$z_m = \mathrm{ggT}(x, y). \tag{5}$$

Und zwar, aus $(*)_{m+1}$ folgt, dass $z_{m-1} = z_m q_{m+1}$, und damit

$$z_m \mid z_{m-1}. \tag{6}$$

Aus $(*)_m$ folgt dann, dass $z_{m-2} = z_{m-1}q_m + z_m$, und da $z_m \mid z_{m-1}q_m + z_m$ nach (6), so folgt

$$z_m \mid z_{m-2}.$$

Wir setzen induktiv fort und zeigen, dass $z_m \mid x$ und $z_m \mid y$. Dies zeigt, dass z_m ein Teiler von x und y ist.

Sei c ein Teiler von x und y. Aus $(*)_2$ folgt, dass $x = yq_2 + z_2$, und da $c \mid x - yq_2$, so folgt

$$c \mid z_2. \tag{7}$$

Aus $(*)_3$ folgt dann, dass $y = z_2q_3 + z_3$, und da $c \mid y - z_2q_3$ nach (7), so folgt

$$c \mid z_3.$$

Wir setzen induktiv fort und zeigen, dass $c \mid z_m$. Dies zeigt (5).

Diese Konstruktion gibt mehr:

Lemma 1.41. *Sei R ein euklidischer Ring und seien $x, y \in R$. Wenn $d = \mathrm{ggT}(x, y)$, dann gibt es $a, b \in R$, sodass*

$$ax + by = d.$$

Beweis. Die Aussage ist einfach, wenn $x = 0$ oder $y = 0$. Wir dürfen also annehmen, dass $x, y \in R \setminus \{0\}$. Wir benutzen die Notation aus Konstruktion 1.40.

Aus $(*)_m$ folgt, dass z_m eine lineare Kombination von z_{m-2} und z_{m-1} ist. Aus $(*)_{m-1}$ folgt, dass z_{m-1} eine lineare Kombination von z_{m-3} und z_{m-2} ist, und damit ist z_m eine lineare Kombination von z_{m-3} und z_{m-2}. Wir setzen induktiv fort und zeigen, dass z_m eine lineare Kombination von x und y ist. Da $d = z_m$, so folgt das Lemma. □

Primelemente und irreduzible Elemente

Definition 1.42. Sei R ein Ring und sei $p \in R \setminus \{0\}$ eine Nichteinheit.

(1) p heißt *irreduzibel*, wenn für alle $x, y \in R$ mit $p = xy$ gilt $x \in R^*$ oder $y \in R^*$. Ansonsten heißt p *reduzibel*.

(2) p heißt *prim*, wenn für alle $x, y \in R$ mit $p \mid xy$ gilt $p \mid x$ oder $p \mid y$.

Beispiel 1.43.

(i) Sei R ein Integritätsring und sei $p \in R \setminus \{0\}$ eine Nichteinheit. Dann ist p prim genau dann, wenn (p) ein Primideal ist.

(ii) In einem Körper K gibt es keine Primelemente und keine irreduziblen Elemente.

(iii) In $\mathbb{Z}$ sind die Primelemente Elemente der Menge

$$\{\pm p \mid p \text{ ist eine Primzahl}\}.$$

Dies ist auch die Menge aller irreduziblen Elemente.

(iv) In $\mathbb{C}[x]$ sind die Primelemente und irreduziblen Elemente gleich: diese sind – nach dem Fundamentalsatz der Algebra – genau die linearen Polynome $x - \alpha$, wobei $\alpha \in \mathbb{C}$.

(v) Im Ring $\mathbb{Z} \times \mathbb{Z}$ ist $(1, 0)$ ein Primelement. Da $(1, 0) = (1, 0) \cdot (1, 0)$, so ist $(1, 0)$ nicht irreduzibel.

(vi) Im Integritätsring $\mathbb{Z}[i\sqrt{5}]$ (siehe Beispiel 1.6(b)) kann man zeigen, dass die Zahl 2 irreduzibel ist. Sie ist aber nicht prim: Und zwar, es gilt $2 \mid 6 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$, aber keiner der Faktoren ist durch 2 teilbar.

Lemma 1.44. *Sei R ein Integritätsring und sei $p \in R\backslash\{0\}$ eine Nichteinheit.*

(i) Ist (p) ein maximales Ideal, so ist p prim.

(ii) Ist p prim, so ist p irreduzibel.

Beweis.
(i) Sei (p) maximal. Nach Satz 1.33(ii) ist (p) prim, d.h. p ist prim.
(ii) Sei p prim. Angenommen, p ist reduzibel, d.h. es gibt $x, y \notin R^*$ mit $p = xy$. Dann folgt (ohne Beschränkung der Allgemeinheit), dass $p \mid x$ und insbesondere $(x) \subseteq (p)$. Da $x \mid p$, so gilt auch $(p) \subseteq (x)$, und damit $(x) = (p)$. Aus Lemma 1.21 folgt, dass p und x assoziiert sind: es gibt eine Einheit c mit $x = pc$. Daraus folgt: $p = pcy$, somit $cy = 1$, ein Widerspruch, da y keine Einheit ist. □

In Hauptidealringen sind prim und irreduziblen Elemente gleich:

Satz 1.45. *Sei R ein Hauptidealring und sei $p \in R \setminus \{0\}$ eine Nichteinheit. Dann sind äquivalent:*

(i) p ist irreduzibel,

(ii) p ist prim,

(iii) (p) ist ein maximales Ideal in R.

Beweis. Die Implikationen (iii) $\Longrightarrow$ (ii) $\Longrightarrow$ (i) folgen aus Lemma 1.44.
Es bleibt zu zeigen, dass (i) $\Longrightarrow$ (iii). Sei p irreduzibel und sei $I \subseteq R$ ein Ideal mit $(p) \subseteq I$. Da R ein Hauptidealring ist, so gibt es $a \in R$ mit $I = (a)$, woraus folgt, dass $(p) \subseteq (a)$. Insbesondere gilt $p \in (a)$, sodass ein $x \in R$ existiert mit $p = ax$. Da p irreduzibel ist, so gilt $a \in R^*$ (und damit $I = R$) oder $x \in R^*$ (und damit $I = (p)$). Dies zeigt, dass (p) maximal ist. □

Unser nächstes Ziel ist es zu zeigen, dass man jedes Element eines Hauptidealringes als Produkt von Primelementen schreiben kann. Dafür brauchen wir die folgende Definition.

Definition 1.46. Ein Ring R heißt *noethersch*, falls jede aufsteigende Kette von Idealen

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

stationär wird, d.h. es existiert $n \in \mathbb{N}_{>0}$, sodass $I_n = I_m$ für alle $m \geq n$.

Der Begriff eines noetherschen Ringes ist fundamental im Gebiet der kommutativen Algebra. Die Bedingung „noethersch“ spielt in vielen Beweisen die Rolle des Auswahlaxioms.

Lemma 1.47. *Jeder Hauptidealring ist noethersch.*

Beweis. Sei $I_1 \subseteq I_2 \subseteq \dots$ eine Kette von Idealen in R. Dann ist $I = \bigcup_{j \in \mathbb{N}_{>0}} I_j$ nach Beispiel 1.18(iv) ein Ideal in R. Da R ein Hauptidealring ist, so gibt es $a \in R$ mit $I = (a)$. Insbesondere gilt $a \in I = \bigcup_{j \in \mathbb{N}_{>0}} I_j$, und so existiert $k \in \mathbb{N}_{>0}$ mit $a \in I_k$. Somit:

$$I = (a) \subseteq I_k \subseteq I,$$

und damit $I_k = I$. Insbesondere gilt $I_\ell = I$ für alle $\ell \geq k$. □

Satz 1.48. *Sei R ein Hauptidealring und sei $p \in R \setminus \{0\}$ eine Nichteinheit. Dann lässt sich p als endliches Produkt von Primelementen in R schreiben.*

Beweis. Sei

$$\mathcal{S} := \big\{ x \in R \setminus (R^* \cup \{0\}) \mid x \text{ ist kein endliches Produkt von Primelementen} \big\}$$

und sei

$$\mathcal{H} = \big\{ (x) \mid x \in \mathcal{S} \big\}.$$

Unser Ziel ist es zu zeigen, dass $\mathcal{S} = \emptyset$. Es genügt zu zeigen, dass $\mathcal{H} = \emptyset$.

Angenommen, $\mathcal{H} \neq \emptyset$. Wir merken, dass $(\mathcal{H}, \subseteq)$ eine partiell geordnete Menge ist. Wir behaupten, dass $\mathcal{H}$ ein maximales Element hat. Und zwar, wir nehmen an, dass es kein maximales Element in $\mathcal{H}$ gibt und sei $I_1 \in \mathcal{H}$ ein beliebiges Ideal. Dann ist I_1 nicht maximal in $\mathcal{H}$, es gibt also ein Ideal $I_2 \in \mathcal{S}$ mit $I_1 \subsetneq I_2$. Dann ist I_2 nicht maximal in $\mathcal{H}$, es gibt also ein Ideal $I_3 \in \mathcal{S}$ mit $I_2 \subsetneq I_3$. Wir konstruieren induktiv eine aufsteigende Kette

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots.$$

Das widerspricht dem Lemma 1.47.

Sei nun $M \in \mathcal{H}$ ein maximales Element. Dann gibt es $x \in \mathcal{S}$ mit $M = (x)$. Das Element x ist reduzibel: Und zwar, wäre x irreduzibel, so wäre x prim nach Satz 1.45. Folglich wäre x nicht in $\mathcal{S}$, ein Widerspruch.

Es existieren also $x_1, x_2 \in R \setminus R^*$ mit $x = x_1 x_2$. Da x, x_1 bzw. x, x_2 nicht assoziiert sind, so gilt nach Lemma 1.21:

$$M = (x) \subsetneq (x_1) \quad \text{und} \quad M = (x) \subsetneq (x_2).$$

Da M ein maximales Element in $\mathcal{H}$ ist, so gilt $(x_1) \notin \mathcal{H}$ und $(x_2) \notin \mathcal{H}$. Es folgt, dass $x_1, x_2 \notin \mathcal{S}$, und damit sind – per Definition von $\mathcal{S}$ – x_1 und x_2 endliche Produkte von Primelementen in R. Aber dann ist auch $x = x_1 x_2$ ein endliches Produkt von Primelementen in R. Damit ist $x \notin \mathcal{S}$, ein Widerspruch. Dies zeigt, dass $\mathcal{H} = \emptyset$ und damit, dass $\mathcal{S} = \emptyset$. □

Faktorielle Ringe

Satz 1.49. *Sei R ein Integritätsring. Betrachte die folgenden Aussagen:*

(a) Jede Nichteinheit $a \in R \setminus \{0\}$ lässt sich eindeutig (bis auf Assoziiertheit und Reihenfolge) als Produkt von irreduziblen Elementen schreiben.

(b) Jede Nichteinheit $a \in R \setminus \{0\}$ lässt sich als Produkt von Primelementen schreiben.

Dann gilt:

(i) Wenn (a) gilt, so ist jedes irreduzible Element von R prim.

(ii) Wenn (b) gilt, so lässt sich jede Nichteinheit $a \in R \setminus \{0\}$ eindeutig (bis auf Assoziiertheit und Reihenfolge) als Produkt von Primelementen schreiben.

(iii) Die Aussagen (a) und (b) sind äquivalent.

Beweis.

(i) Sei $a \in R$ irreduzibel und seien $x, y \in R$ mit $a \mid xy$. Dann gibt es $r \in R$ mir $ar = xy$. Wäre x eine Einheit, so wäre $y = arx^{-1}$, also $a \mid y$; wir argumentieren analog im Falle, wo y eine Einheit wäre.

Wir dürfen also annehmen, dass x und y keine Einheiten sind. Nach Voraussetzung gibt es irreduzible Elemente $x_1, \ldots, x_t$, $y_1, \ldots, y_s$ und $r_1, \ldots, r_q$, sodass $x = x_1 \ldots x_t$, $y = y_1 \ldots y_s$ und $r = r_1 \ldots r_q$ (wenn r eine Einheit ist, so schreiben wir einfach $r = r_1$). Dann folgt

$$ar_1 \ldots r_q = x_1 \ldots x_t y_1 \ldots y_s.$$

Die Eindeutigkeit in (a) ergibt, dass das irreduzible Element a zu einem x_i oder einem y_j assoziiert ist. Wir haben also $a \mid x$ oder $a \mid y$. Damit ist a ein Primelement.

(ii) folgt aus (iii).

(iii) Die Implikation (a) $\Longrightarrow$ (b) folgt aus (i).

Nun zeigen wir die Implikation (b) $\Longrightarrow$ (a). Sei $a \in R \setminus \{0\}$ eine Nichteinheit und seien $x_1, \ldots, x_t$ Primelemente mit $a = x_1 \ldots x_t$. Jedes Primelement ist nach Lemma 1.44 irreduzibel, sodass wir deswegen nur die Eindeutigkeit in der Aussage zeigen müssen. Angenommen, es gibt weitere irreduzible Elemente $y_1, \ldots, y_s$, sodass $a = y_1 \ldots y_s$. Da x_t prim ist, so folgt aus

$$x_1 \ldots x_t = y_1 \ldots y_s, \tag{8}$$

dass es ein y_i gibt, sodass $x_t \mid y_i$; ohne Beschränkung der Allgemeinheit dürfen wir annehmen, dass $i = s$. Es existiert dann $c \in R$ mit $y_s = cx_t$. Da y_s irreduzibel ist, so folgt $c \in R^*$, und (8) wird zu

$$x_1 \ldots x_{t-1} x_t = y_1 \ldots y_{s-1} c x_t,$$

und damit zu

$$x_1 \ldots x_{t-1} = (cy_1) \ldots y_{s-1}.$$

Wir setzen den Prozess induktiv fort. Am Ende bekommen wir, dass $t = s$ und dass (ohne Beschränkung der Allgemeinheit) x_i zu y_i assoziiert ist, für alle $i = 1, \ldots, t$. □

Definition 1.50. Ein Integritätsring R, der eine der zwei äquivalenten Bedingungen (a) und (b) in Satz 1.49 erfüllt, heißt *faktoriell*. In diesem Falle sagen wir, dass jedes $a \in R$ eine *Primfaktorzerlegung* hat, die bis auf die Reihenfolge und Assoziiertheit eindeutig ist.

Bemerkung 1.51. Nach Lemma 1.44 und Satz 1.49 ist in einem faktoriellen Ring ein Element genau dann irreduzibel, wenn es prim ist.

Aus Sätzen 1.38, 1.48 und 1.49 folgt sofort:

Korollar 1.52. *Jeder Hauptidealring ist faktoriell. Jeder euklidische Ring ist faktoriell.*

Damit haben wir die folgende Inklusion von Strukturen:

Körper $\subseteq$ euklidische Ringe $\subseteq$ Hauptidealringe
$\subseteq$ faktorielle Ringe $\subseteq$ Integritätsringe

Beispiel 1.53.

(a) Die Ringe $\mathbb{Z}$ und $K[x]$ (wobei K ein Körper ist) sind faktoriell, da sie euklidische Ringe sind.

(b) Der Ring der ganzen Gaußschen Zahlen $\mathbb{Z}[i]$ ist nach Beispiel 1.37(c) ein euklidischer Ring und damit faktoriell.

(c) Sei R ein faktorieller Ring. Wir werden später zeigen, dass dann $R[x]$ auch faktoriell ist.

Notation 1.54. Es ist üblich, Primfaktorzerlegungen in faktoriellen Ringen R durch Zusammenfassen assoziierter Primelemente zu Potenzen in der Form

$$a = \varepsilon p_1^{\nu_1} \dots p_r^{\nu_r}$$

zu schreiben, wobei $\varepsilon \in R^*$ und p_i sind paarweise verschiedene Primelemente. Hier setzen wir $p^0 = 1$ für $p \in R \setminus \{0\}$. Jedes Element $a \in R \setminus \{0\}$ besitzt eine solche *Primfaktorzerlegung*.

Um die Primfaktorzerlegung weiter zu standardisieren, kann man in R ein *Vertretersystem $\mathcal{P}$ der Primelemente* auswählen, d.h. eine Teilmenge $\mathcal{P}$ bestehend aus Primelementen, sodass $\mathcal{P}$ aus jeder Klasse zueinander assoziierter Primelemente genau eines enthält. Dann kann man für jedes $a \in R\setminus\{0\}$ seine Primfaktorzerlegung in R in der Form

$$a = \varepsilon \prod_{p \in \mathcal{P}} p^{\nu_p(a)}$$

schreiben, wobei nunmehr $\varepsilon \in R^*$ und die Zahlen $\nu_p(a) \in \mathbb{N}$ eindeutig bestimmt sind. Es gilt nach Satz 1.49 $\nu_p(a) = 0$ für fast alle $p \in \mathcal{P}$, sodass dieses Produkt in Wahrheit endlich ist.

Betrachten wir die folgenden Beispiele:

(a) im Ring $\mathbb{Z}$ können wir für $\mathcal{P}$ die Menge der positiven Primzahlen wählen;

(b) wenn K ein Körper ist, so können wir im Ring $K[x]$ für $\mathcal{P}$ die Menge aller monischen irreduziblen Polynome wählen.

Da jedes Element in $Q(R)$ ein Bruch zweier Elemente in R ist, wobei R ein faktorieller Ring ist, so kann man wie in $\mathbb{Q}$ das folgende Lemma beweisen:

Lemma 1.55. *Sei R ein faktorieller Ring und sei $\mathcal{P}$ ein Vertretersystem der Primelemente in R. Dann besitzt jedes $a \in Q(R)^*$ eine eindeutige Darstellung*

$$a = \varepsilon \prod_{p \in \mathcal{P}} p^{\nu_p(a)},$$

wobei $\varepsilon \in R^*$, $\nu_p(a) \in \mathbb{Z}$ für $p \in \mathcal{P}$, und es gilt $\nu_p(a) = 0$ für fast alle p. Setze $\nu_p(0) = \infty$. Damit ist die Abbildung

$$\nu_p \colon Q(R) \to \mathbb{Z} \cup \{\infty\}, \quad a \mapsto \nu_p(a)$$

wohldefiniert und es gilt

$$\nu_p(xy) = \nu_p(x) + \nu_p(y) \quad \text{für alle } p \in \mathcal{P} \text{ und } x, y \in Q(R).$$

Es gilt $a \in R$ genau dann, wenn $\nu_p(a) \geq 0$ für alle $p \in \mathcal{P}$.

Der folgende Satz ist einfach:

Satz 1.56. *Sei R ein faktorieller Ring und seien $x_1, \ldots, x_n \in R \setminus \{0\}$. Ist $\mathcal{P}$ ein Vertretersystem der Primelemente in R und sind*

$$x_i = \varepsilon_i \prod_{p \in \mathcal{P}} p^{\nu_p(x_i)} \quad \text{für } i = 1, \ldots, n$$

die entsprechenden Primfaktorzerlegungen, so gilt (bis auf Assoziiertheit):

$$\mathrm{ggT}(x_1, \ldots, x_n) = \prod_{p \in \mathcal{P}} p^{\min\left\{\nu_p(x_1), \ldots, \nu_p(x_n)\right\}}$$

und

$$\mathrm{kgV}(x_1, \ldots, x_n) = \prod_{p \in \mathcal{P}} p^{\max\left\{\nu_p(x_1), \ldots, \nu_p(x_n)\right\}}.$$

In Hauptidealringen lassen sich der ggT und das kgV idealtheoretisch charakterisieren:

Satz 1.57. *Sei R ein Integritätsring und seien $x_1, \ldots, x_n$ Elemente von R.*

(i) Falls $(x_1, \ldots, x_n)$ ein Hauptideal ist, also von einem Element $d \in R$ erzeugt wird, so gilt $d = \mathrm{ggT}(x_1, \ldots, x_n)$.

(ii) Falls $(x_1) \cap \cdots \cap (x_n)$ ein Hauptideal ist, also von einem Element $v \in R$ erzeugt wird, so gilt $v = \mathrm{kgV}(x_1, \ldots, x_n)$.

Beweis.

(i) Angenommen, $(x_1, \ldots, x_n) = (d)$. Dann folgt $x_i \in (d)$ und somit $d \mid x_i$ für alle $i = 1, \ldots, n$. Andererseits, aus $d \in (x_1, \ldots, x_n)$ folgt, dass $d = \sum_{i=1}^{n} a_i x_i$ mit $a_i \in R$. Somit ist jeder gemeinsame Teiler der x_i auch ein Teiler von d. Dies beweist (i).

(ii) Angenommen, $(x_1) \cap \cdots \cap (x_n) = (v)$. Dann folgt $v \in (x_i)$ für alle i und somit ist v ein gemeinsames Vielfaches von $x_1, \ldots, x_n$. Andererseits, sei u ein weiteres gemeinsames Vielfaches von $x_1, \ldots, x_n$. Dann gilt $u \in (x_i)$ für alle i, also $u \in (x_1) \cap \cdots \cap (x_n) = (v)$ und somit $v \mid u$. Dies beweist (ii). □

Dann können wir den Chinesischen Restsatz in Hauptidealringen so umformulieren:

Korollar 1.58 (Chinesischer Restsatz in Hauptidealringen)**.** *Sei R ein Hauptidealring und sei*

$$a = \varepsilon p_1^{\nu_1} \ldots p_r^{\nu_r}$$

eine Primfaktorzerlegung in R, wobei ε eine Einheit ist und $p_1, \ldots, p_r$ sind Primelemente, die paarweise nicht assoziiert sind. Dann sind die Ideale

$$(p_1^{\nu_1}), \ldots, (p_r^{\nu_r})$$

paarweise koprim in R und es gilt

$$a = \mathrm{kgV}(p_1^{\nu_1}, \ldots, p_r^{\nu_r}) \quad \textit{und} \quad (a) = \bigcap_{i=1}^{r} (p_i^{\nu_i}).$$

Insbesondere existiert ein kanonischer Isomorphismus

$$R/(a) \cong R/(p_1^{\nu_1}) \times \cdots \times R/(p_r^{\nu_r}).$$

Mit Hilfe von Lemma 1.41 können wir den Chinesischen Restsatz in $\mathbb{Z}$ so umformulieren; der Beweis ist eine einfache Übung.

Satz 1.59 (Chinesischer Restsatz in $\mathbb{Z}$)**.** *Seien $a_1, \ldots, a_n \in \mathbb{Z}$ paarweise teilerfremd und seien $x_1, \ldots, x_n \in \mathbb{Z}$. Betrachte das System von Kongruenzen:*

$$\begin{aligned} x &\equiv x_1 \pmod{a_1} \\ &\vdots \\ x &\equiv x_n \pmod{a_n} \end{aligned}$$

Dann ist dieses System immer lösbar. Ist x eine Lösung, so liegt jede andere Lösung in der Menge $x + (a_1 \cdots a_n)\mathbb{Z}$.

Wir können nun die invertierbaren Elemente in Gruppen $\mathbb{Z}/n\mathbb{Z}$ genauer untersuchen.

Definition 1.60. Sei $n \in \mathbb{N}_{>0}$ und setze

$$\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*|,$$

also die Anzahl der Elemente in $\mathbb{Z}/n\mathbb{Z}$, die Einheiten sind. Die Abbildung

$$\varphi\colon \mathbb{N}_{>0} \to \mathbb{N}_{>0}, \quad n \mapsto \varphi(n)$$

heißt die *Eulersche φ-Funktion.*

Lemma 1.61. *Sei φ die Eulersche φ-Funktion.*

(a) Für $n \in \mathbb{N}_{>0}$ gilt

$$(\mathbb{Z}/n\mathbb{Z})^* = \big\{[a] \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(a,n) = 1\big\}$$

und damit

$$\varphi(n) = \big|\{a \in \mathbb{Z} \mid 0 \le a \le n-1 \text{ und } \mathrm{ggT}(a,n) = 1\}\big|.$$

(b) Die Funktion φ ist multiplikativ *im folgenden Sinne: Es gilt*

$$\varphi(mn) = \varphi(m)\varphi(n) \quad \text{wenn } m,n \in \mathbb{N}_{>0} \text{ koprim sind.}$$

(c) Sei $n = \prod_{i=1}^{k} p_i^{\nu_i}$ die Primfaktorzerlegung von n mit $\nu_i > 0$ für jedes i. Dann gilt

$$\varphi(n) = \prod_{i=1}^{k} p_i^{\nu_i - 1}(p_i - 1).$$

Beweis.

(a) Sei $a \in \mathbb{Z}$. Dann ist $\mathrm{ggT}(a,n) = 1$ äquivalent zur Existenz von $e, f \in \mathbb{Z}$ mit $ae + nf = 1$ nach Lemma 1.41. Dies ist äquivalent zu $[a][e] = [ae] = [1]$ in $\mathbb{Z}/n\mathbb{Z}$, und damit äquivalent zur Bedingung, dass $[a]$ in $\mathbb{Z}/n\mathbb{Z}$ invertierbar ist.

(b) Wenn $m, n \in \mathbb{N}_{>0}$ koprim sind, so gilt $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ nach Korollar 1.58, und dann folgt nach Lemma 1.2, dass $(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$. Damit gilt $\varphi(mn) = \varphi(m)\varphi(n)$.

(c) Nach (b) genügt es zu zeigen, dass $\varphi(p^\nu) = p^{\nu-1}(p-1)$ für jede Primzahl p und jedes $\nu \in \mathbb{N}_{>0}$. Wir berechnen mit Hilfe von (a):

$$\begin{aligned}\big|(\mathbb{Z}/p^\nu\mathbb{Z}) \setminus (\mathbb{Z}/p^\nu\mathbb{Z})^*\big| &= \big|\{a \in \mathbb{Z} \mid 0 \le a \le p^\nu - 1 \text{ und } \operatorname{ggT}(a, p^\nu) \neq 1\}\big| \\ &= \big|\{a \in \mathbb{Z} \mid 0 \le a \le p^\nu - 1 \text{ und } p \mid a\}\big| \\ &= \big|\{0, p, 2p, \ldots, (p^{\nu-1}-1)p\}\big| = p^{\nu-1}.\end{aligned}$$

Daraus folgt, dass $\varphi(p^\nu) = p^\nu - p^{\nu-1} = p^{\nu-1}(p-1)$. □