Hauptsatz der elementaren Zahlentheorie

Sei $n \in \mathbb{Z}_{>1}$. Dann: $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ mit Primzahlen $p_1 < \ldots < p_r$ und $\nu_i \geq 1$. Z.B.:

$$60 = 2^2 \cdot 3 \cdot 5.$$

Definition Ein Int-Ring R heißt faktoriell, falls jedes $0_R \neq a \in R \setminus R^*$ zerlegbar als

$$a = p_1 \cdots p_r \quad \text{mit } p_1, \ldots, p_r \in R \text{ prim.}$$

Satz Jeder euklidische Ring ist faktoriell.

Beweis Sei R eukl. Ring mit Gradabb. $\delta: R \setminus \{0_R\} \to \mathbb{Z}_{\geq 0}$.

Wissen: R ist HIR. Somit für jedes $q \in R$:

$$q \text{ irreduzibel} \Rightarrow q \text{ prim.}$$

Also genügt es z.z.: Für jedes $0_R \neq a \in R$ gilt:

$$a \in R^* \text{ oder } a = q_1 \cdots q_r \text{ mit } q_i \in R \text{ irred.}$$

Induktion über $\delta(a)$. Falls $\delta(a) = 0$: Haben

$$1_R = ca + r, \quad \delta(r) < \delta(a) \text{ oder } r = 0_R.$$

Wegen $\delta(a) = 0$: $r = 0_R$. Somit $1_R = ca$, d.h., $a \in R^*$.

Sei $\delta(a) > 0$. Falls $a \in R^*$ oder a irred.: ✓

Noch zu behandeln: $a = bc$ mit $b, c \in R \setminus R^*$.

Zeigen: $\delta(b) < \delta(a)$. Haben

$$b = q \cdot \underbrace{(bc)}_{a} + r, \quad \delta(r) < \delta(bc) \text{ oder } r = 0_R.$$

Falls $r = 0_R$: $b = qbc \Rightarrow 1_R = qc \Rightarrow c \in R^*$ ↯

Somit $\delta(r) < \delta(bc)$. Weiter:

$$b(1_R - qc) = b - qbc = r$$

Damit

$$\delta(b) \leq \delta(b(1_R - qc)) = \delta(r) < \delta(bc) = \delta(a)$$

Analog: $\delta(c) < \delta(a)$. IV: b und c sind Produkte irred. EL. Also $a = bc$ auch. □

Folgerung $\mathbb{Z}$ und $\mathbb{Z}[I]$ sind faktoriell. Weiter ist $\mathbb{K}[T]$ faktoriell für jeden Körper $\mathbb{K}$.

Definition R Int-Ring. **Primsystem**: $P \subset R$ mit

* jedes $p \in P$ prim,
* $q \in R$ prim $\Rightarrow q \sim p$ für ein $p \in P$,
* $p, p' \in P$ mit $p \neq p' \Rightarrow p \not\sim p'$.

Bemerkung $P \subset R$ Primsystem $\Leftrightarrow P$ Repräsentantensystem für "$\sim$" auf der Menge aller Primel. von R.

Beispiel $\{2, 3, 5, 7, 11, \dots\}$ ist Primsystem in $\mathbb{Z}$.

Satz R faktorieller Ring, $P \subset R$ Primsystem. Dann hat jedes $a \in R \setminus \{0_R\}$ Primfaktorzerlegung:

$$(*)\quad a = c \prod_{p \in P} p^{\nu_p(a)}, \qquad c \in R^*,\ \nu_p(a) \in \mathbb{Z}_{\geq 0},\ \nu_p(a) \neq 0 \text{ für nur endl. viele } p \in P.$$

Dabei: c und die $\nu_p(a)$ eindeutig bestimmt.

Lemma R Int-Ring, $p, q_1, \dots, q_k \in R$ prim mit $p \mid q_1 \cdots q_k$. Dann: $p \sim q_i$ für ein $1 \leq i \leq k$.

Beweis Induktion über k. Zu $k = 1$:

$$p \mid q_1 \Rightarrow q_1 = cp.$$

Wegen q_1 irred. und $p \notin R^*$: $c \in R^*$. Also $q_1 \sim p$.

Induktionsschritt:

$$p \mid q_1 \cdots q_k \xRightarrow{p \text{ prim}} p \mid q_1 \text{ oder } p \mid q_2 \cdots q_k \xRightarrow{IV} p \sim q_i \text{ für ein } i. \qquad \square$$

Beweis Satz Sei $0_R \neq a \in R$. Falls $a \in R^*$: ✓

Sei $a \in R \setminus R^*$. Wegen R faktoriell:

$$a = q_1 \cdots q_r \text{ mit } q_i \in R \text{ prim}.$$

Wegen $P \subset R$ Primsystem:

$$q_i = c_i p_i \text{ mit } c_i \in R^*,\ p_i \in P.$$

Damit: Existenz von (*). Zur Eindeutigkeit:

Betrachte

$$c \prod_{p \in P} p^{\nu_p} = c' \prod_{p \in P} p^{\mu_p}.$$

Zeigen $\nu_p = \mu_p$ für alle $p \in P$. Andernfalls:

Etwa $\nu_p > \mu_p$. kürzen mit p^{μ_p} liefert

$$p \mid \prod_{q \in P \setminus \{p\}} q^{\mu_q}$$

Lemma: $p \sim q$ für ein $q \in P \setminus \{p\}$ ↯.

Folglich $\nu_p = \mu_p$ f. alle $p \in P$. Somit $c = c'$. $\square$

Beispiel Primzahlen bilden Primsystem in $\mathbb{Z}$:

$$P = \{2, 3, 5, 7, 11, \dots\}.$$

Primfaktorzerlegung von -360 bez. P:

$$-360 = -1 \cdot 2^3 \cdot 3^2 \cdot 5.$$

Weiter: Jedes $n \in \mathbb{Z}_{>1}$ hat eindeutige Darst.

$$n = p_1^{\nu_1} \cdots p_r^{\nu_r}, \quad p_i \in P, \quad \nu_i \in \mathbb{Z}_{\geq 1}, \quad p_1 < \dots < p_r.$$

Satz R faktorieller Ring, $P \subset R$ Primsystem. Weiter $a_1, \dots, a_n \in R$ mit Primfaktorzerlegung

$$a_i = c_i \prod_{p \in P} p^{\nu_p(a_i)}.$$

Dann:

$$a_i \mid a_j \iff \nu_p(a_i) \leq \nu_p(a_j) \text{ für alle } p \in P.$$

Weiter:

$$\prod_{p \in P} p^{\min(\nu_p(a_i))} \in ggT(a_1, \dots, a_n),$$

$$\prod_{p \in P} p^{\max(\nu_p(a_i))} \in kgV(a_1, \dots, a_n).$$

Beweis Falls $a_i \mid a_j$:

$$c_j \prod_{p \in P} p^{\nu_p(a_j)} = a_j = b a_i$$

$$= c \prod_{p \in P} p^{\nu_p(b)} \cdot c_i \prod_{p \in P} p^{\nu_p(a_i)}$$

$$= c c_i \prod_{p \in P} p^{\nu_p(b) + \nu_p(a_i)}.$$

Eindeutigkeit der Primfaktorzerlegung:

$$c_j = c c_i, \quad \nu_p(a_j) = \nu_p(b) + \nu_p(a_i) \geq \nu_p(a_i).$$

Klar: $\nu_p(a_i) \leq \nu_p(a_j) \Rightarrow a_i \mid a_j$. Ebenso klar: Aussagen zu ggT, kgV. □

Beispiel Betrachte 12 und 18 in $\mathbb{Z}$:

$$12 = 2^2 \cdot 3, \quad 18 = 2 \cdot 3^2$$

Damit

$$ggT(12, 18) = \{\pm 2 \cdot 3\} = \{\pm 6\},$$

$$kgV(12, 18) = \{\pm 2^2 \cdot 3^2\} = \{\pm 36\}.$$

Satz R euklidischer Ring, $a = c p_1^{\nu_1} \cdots p_n^{\nu_n} \in R$, wobei $c \in R^*$, $p_i \in R$ prim mit $p_i \not\sim p_j$ für $i \neq j$. Dann hat man Iso. von kl-Ringen:

$$R/\langle a \rangle \cong R/\langle p_1^{\nu_1} \rangle \times \cdots \times R/\langle p_n^{\nu_n} \rangle.$$

Beweis Sei $P \subset R$ Primsystem. Wir dürfen annehmen:

* $p_1, \ldots, p_n \in P$,
* $c = 1$.

Voriger Satz über PFZ und Teilbarkeit: Für $i \neq j$ hat man

$$1_R \in ggT(p_i^{\nu_i}, p_j^{\nu_j}).$$

Satz über ggT in HIR:

$$\langle p_i^{\nu_i} \rangle + \langle p_j^{\nu_j} \rangle = \langle p_i^{\nu_i}, p_j^{\nu_j} \rangle = \langle 1_R \rangle = R.$$

Chinesischer Restsatz:

$$R/\bigcap_{i=1}^{n} \langle p_i^{\nu_i} \rangle \cong R/\langle p_1^{\nu_1} \rangle \times \cdots \times R/\langle p_n^{\nu_n} \rangle.$$

Nur noch zu zeigen:

$$\langle a \rangle = \langle p_1^{\nu_1} \rangle \cap \cdots \cap \langle p_n^{\nu_n} \rangle.$$

Klar: "$\subseteq$". "$\supseteq$": Betrachte

$$b \in \langle p_1^{\nu_1} \rangle \cap \cdots \cap \langle p_n^{\nu_n} \rangle.$$

Dann: $p_i^{\nu_i} \mid b$ für $i = 1, \ldots, n$. Satz über PFZ und Teilbarkeit:

$$b \in \langle p_1^{\nu_1} \cdots p_n^{\nu_n} \rangle = \langle a \rangle. \quad \square$$

Bemerkung Sei $n \in \mathbb{Z}_{\geq 1}$ mit PFZ $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$. Dann hat man Iso. von kl-Ringen:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\nu_r}\mathbb{Z}.$$

Weiter hat man Iso. von ab. Grp.:

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{\nu_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_r^{\nu_r}\mathbb{Z})^*.$$

Satz In $\mathbb{C}[T]$ hat man das Primsystem

$$\{T-a;\ a\in\mathbb{C}\}\subset\mathbb{C}[T].$$

Insbesondere hat jedes nichtkonstante $f\in\mathbb{C}[T]$ eindeutige Darstellung

$$f = c\prod_{a\in\mathbb{C}}(T-a)^{\nu_a(f)}$$

mit $c\in\mathbb{C}^*$ und der Nullstellenordnung $\nu_a(f)$ von f in $a\in\mathbb{C}$.

Beweis Wissen: $T-a$ irreduzibel in $\mathbb{C}[T]$.

Wegen $\mathbb{C}[T]$ HIR: $T-a$ prim.

Weiter haben wir in $\mathbb{C}[T]$:

$$\begin{aligned} T-a\sim T-b &\iff (T-b)=c(T-a) \\ &\quad \text{mit } c\in\mathbb{C}^* \\ &\iff T-b = cT-ca \\ &\iff T-b = T-a. \end{aligned}$$

Also: $\{T-a;\ a\in\mathbb{C}\}$ ist Menge paarweise nicht assoz. Primel. in $\mathbb{C}[T]$.

Noch zu zeigen: Jedes Primelement $f\in\mathbb{C}[T]$ ist assoziiert zu einem $T-a$.

Fundamentalsatz der Algebra liefert:

$$f = c\cdot(T-a_1)\cdots(T-a_r)$$

mit $c\in\mathbb{C}^*$ und $a_i\in\mathbb{C}$. Wegen f irreduzibel:

$$f = c\cdot(T-a_1)$$

Somit $f\sim T-a_1$. □

Satz In $\mathbb{R}[T]$ hat man das Primsystem

$$\{T-a;\ a\in\mathbb{R}\}\cup\{T^2+bT+c;\ b,c\in\mathbb{R},\ b^2<4c\}.$$

Beweisidee klar: Obige $T-a$, T^2+bT+c sind pw. nichtassoz. prim.

Falls $f\in\mathbb{R}[T]$ prim, $f\neq T-a$: Zerlege f in $\mathbb{C}[T]$:

$$f = c(T-a_1)(T-\bar{a}_1)\cdots(T-a_r)(T-\bar{a}_r).$$

Damit $f\sim T^2-(a_1+\bar{a}_1)T+a_1\bar{a}_1$. □