Einführung in die Algebra
Übung 1

Beispiel 1.8 (1). Wir zeigen zuerst, dass $p_n \leq p_1 \cdot \ldots \cdot p_{n-1} + 1$. Sei $q := p_1 \cdot \ldots \cdot p_{n-1} + 1$, dann gilt $p_i \nmid q$ für $i \in \{1, \ldots, n-1\}$. Angenommen $p_n > q$, dann ist q prim, da jede Primzahl die kleiner als q ist, q nicht teilt, also ist q die n-te Primzahl. Ein Widerspruch. Also ist $p_n \leq q = p_1 \cdot \ldots \cdot p_{n-1} + 1$.

Wir zeigen $p_n \leq 2^{2^{n-1}}$ mittels Induktion.

$\underline{n=1}$: $\quad p_1 = 2 \leq 2^{2^0} = 2$ ✓

$\underline{n-1 \to n}$: $\quad p_n \leq p_1 \cdot \ldots \cdot p_{n-1} + 1 \leq \prod_{k=1}^{n-1} 2^{2^{k-1}} + 1 = 2^{\sum 2^{k-1}} + 1 = 2^{2^{n-1}-1} + 1 \leq 2^{2^{n-1}}$

Beispiel 1.8 (4). Sei $(I_\alpha)_{\alpha \in A}$ eine Familie von Idealen in $\mathbb{Z}$. Wir zeigen, dass $J = \cap I_\alpha$ ein Ideal ist.

1. $0 \in J$
2. Sei $a, b \in J$, dann ist natürlich $a, b \in I_\alpha$ für alle $\alpha \in A$, also gilt $a - b \in I_\alpha$ für alle $\alpha \in A$, daher $a - b \in \cap I_\alpha = J$
3. Sei $r \in \mathbb{Z}$ und $a \in J$, dann gilt analog $ra \in I_\alpha$ für alle $\alpha \in A$, folglich $ra \in J$

Beispiel 1.12 (2). $a, b \in \mathbb{Z}$, $y \in \mathbb{Z}$: $a \mid y$, $b \mid y$, $\mathrm{ggT}(a, b) = 1$

Wir zeigen $ab \mid y$. Mit Definition der Teilbarkeit und der Eigenschaft, dass der ggT zweier Zahlen als Linearkombination dargestellt werden kann, erhalten wir

$$\exists \alpha \in \mathbb{Z} : a \cdot \alpha = y$$
$$\exists \beta \in \mathbb{Z} : b \cdot \beta = y$$
$$\exists u, v \in \mathbb{Z} : u \cdot a + v \cdot b = 1$$

Multiplizieren wir die letzte Gleichung mit y und ersetzen dann auf der linken Seite y durch $b\beta$ bzw. $a\alpha$ so erhalten wir

$$\begin{aligned} uay + vby &= y \\ uab\beta + vba\alpha &= y \\ ab(u\beta + v\alpha) &= y \end{aligned}$$

Das heißt $ab \mid y$

Beispiel 1.12 (5).

$$G_1(a_1) := a_1,\ G_1(a_1,\dots,a_n) := \mathrm{ggT}(G_1(a_1,\dots,a_{n-1}),a_n))$$
$$G_2(a_1,\dots,a_n) := \max\{z\in\mathbb{N} : z \mid a_i \text{ für alle } i\in\{1,\dots,n\}\}$$
$$G_3(a_1,\dots,a_n) := \min\{z\in\mathbb{N} : \exists\lambda_1,\dots,\lambda_n\in\mathbb{Z} \text{ sodass } z=\sum\lambda_i a_i\}$$

$\underline{\boldsymbol{G_1 = G_2}}$**:**

Wir zeigen mittels Induktion, dass $G_1 \mid a_i$ für $i\in\{1,\dots,n\}$.

$\underline{n=1}$: $G_1(a_1) = a_1$ also $G_1(a_1) \mid a_1$ ✓

$\underline{n-1\to n}$: $G_1(a_1,\dots,a_n) = \mathrm{ggT}(G_1(a_1,\dots,a_{n-1}),a_n)$
Nach Definition des ggT gilt $G_1(a_1,\dots,a_n) \mid a_n$ und $G_1(a_1,\dots,a_n) \mid G_1(a_1,\dots,a_{n-1})$, weiters gilt nach Induktionsvoraussetzung $G_1(a_1,\dots,a_{n-1}) \mid a_i$ für $i\in\{1,\dots,n-1\}$ so folgt $G_1(a_1,\dots,a_n) \mid a_i$ für $i\in\{1,\dots,n\}$

Sei t ein Teiler von a_i für $i\in\{1,\dots,n\}$, dann gilt $t \mid G_1(a_1,\dots,a_n)$. Beweis mittels Induktion:

$\underline{n=1}$: $t \mid a_1$ und $G_1(a_1) = a_1$ ✓

$\underline{n-1\to n}$: Für alle $i\le n$ gilt $t\mid a_i$, nach Induktionsvoraussetzung gilt $t \mid G_1(a_1,\dots,a_{n-1})$, da $G_1(a_1,\dots,a_n) = \mathrm{ggT}(G_1(a_1,\dots,a_{n-1}),a_n)$ und t beide Zahlen teilt, so folgt $t \mid G_1(a_1,\dots,a_n)$.

$t = G_2(a_1,\dots,a_n)$ erfüllt die Voraussetzungen, also $G_2(a_1,\dots,a_n) \mid G_1(a_1,\dots,a_n)$.

Da G_1 alle a_i teilt, $G_2 \mid G_1$ und G_2 die größte natürliche Zahl ist die alle a_i teilt, so folgern wir, dass $G_2 = G_1$.

$\underline{\boldsymbol{G_2 = G_3}}$**:**

Da sich G_3 als Linearkombination der a_i schreiben lässt und G_2 alle a_i teilt so folgt $G_2 \mid G_3$.

Nachdem alle a_i natürliche Zahen sind, so gilt $G_3 \le a_i$ für $i\in\{1,\dots,n\}$, wähle dazu $\lambda_j = 0$ falls $j\ne i$ und $\lambda_j = 1$ falls $j = i$, dann gilt $a_i = \sum\lambda_j a_j$, nach Definition von G_3 ist dann $G_3 \le a_i$.

Sei $G_3 := G_3(a_1,\dots,a_n) = \sum_{j=1}^n \lambda_j a_j$, da die a_i kleiner gleich G_3 sind, so erhält man nach Division mit Rest: $a_i = \alpha_i G_3 + \beta_i$ mit $0\le\beta_i < G_3$. Dann gilt $\beta_i = a_i - \alpha_i G_3 = a_i(1-\alpha_i\lambda_i) - \sum_{j\ne i}\alpha_i\lambda_j a_j$, da G_3 die kleinste natürliche Zahl ist, die sich als Linearkombination der a_i schreiben lässt, so folgt $\beta_i = 0$ und somit $G_3 \mid a_i$ für $i\in\{1,\dots,n\}$.

Also folgt mit der selben Argumentation wie für G_1, dass $G_2 = G_3$ und somit $G_1 = G_2 = G_3$.

Beispiel 1.12 (6). $a = \prod p_i^{\alpha_i}, b = \prod p_i^{\beta_i}, \gamma_i = \min\{\alpha_i, \beta_i\}$

Wir zeigen $\mathrm{ggT}(a,b) = \prod p_i^{\gamma_i}$

$$\mathrm{ggT}(a,b) \overset{\exists u,v}{=} u \cdot a + v \cdot b = u \prod p_i^{\alpha_i} + v \prod p_i^{\beta_i} = \prod p_i^{\gamma_i} \left(u \prod p_i^{\alpha_i - \gamma_i} + v \prod p_i^{\beta_i - \gamma_i} \right)$$

Also $\prod p_i^{\gamma_i} \mid \mathrm{ggT}(a,b)$

Sei q prim, sodass $q \mid \mathrm{ggT}(a,b)$, dann gilt nach Definition, dass $q \mid a$ und $q \mid b$, also $q \mid \prod p_i^{\alpha_i}$. Deshalb erhalten wir induktiv mit dem Fundamentallemma, dass $q \mid p_j$ für ein j mit $\alpha_j > 0$, da q und p_j prim sind, so ist $q = p_j$. Analog gilt für b, dass für dasselbe j gilt $q = p_j$ und $\beta_j > 0$, also $q \mid p_j^{\min\{\alpha_j, \beta_j\}}$ und somit $q \mid \prod p_i^{\gamma_i}$. Also kommt jeder Primfaktor von $\mathrm{ggT}(a,b)$ auch in $\prod p_i^{\gamma_i}$ vor, die Vielfachheit jedes Primfaktors ist in $\prod p_i^{\gamma_i}$ jedoch maximal gewählt, bezüglich der Eigenschaft $p_i^{\gamma_i} \mid a$ und $p_i^{\gamma_i} \mid b$, daher folgern wir, dass $\mathrm{ggT}(a,b) = \prod p_i^{\gamma_i}$, da $\prod p_i^{\gamma_i} \mid \mathrm{ggT}(a,b)$.