$$A = \prod_{P \in \mathcal{P}} P^{a_p}, \quad a_p \geq 0$$

$$P^0 := 1$$

$$A \cdot B = \prod_{P \in \mathcal{P}} P^{a_p + b_p}$$

$$\mathrm{ggT}(A,B) = \prod_{P \in \mathcal{P}} P^{\min(a_p, b_p)}$$

$$\mathrm{kgV}(A,B) = \prod_{P \in \mathcal{P}} P^{\max(a_p, b_p)}$$

Ausblick: Ring R heißt **faktoriell**, wenn gilt:

- R ist kommutativ und nullteilerfrei
- Es gilt der Satz von der eindeutigen Primfaktorzerlegungen (Primelement = unzerlegbar, $p \setminus a \cdot b \Rightarrow p \setminus a$ oder $p \setminus b$)

1) R faktoriell $\Rightarrow R[X]$ faktoriell

$$\Rightarrow (K[X])[Y] = K[X,Y] \text{ faktoriell}$$

2) R **Hauptideal** $\Rightarrow R$ faktoriell
(I Ideal von R)

$$\Rightarrow I = \langle r \rangle$$

Der euklidische Algorithmus berechnet $\mathrm{ggT}(A,B)$

Teile A durch B:

$A = PB + R$ grad $R <$ grad B

$R = 0 \quad \Rightarrow \quad \mathrm{ggT}(A,B) = B$

$R \neq 0 \quad \Rightarrow \quad \mathrm{ggT}(A,B) = \mathrm{ggT}(B,R)$

$DIV(A,B) =$ Rest

$EA(A,B)$

WHILE $B \neq 0$ *DO*

$R := DIV(A,B)$

$A :=$

WEND

$a = 633,\ b = 270,\ g = \mathrm{ggT}(a,b)$

$633 = 2 \cdot 270 + 93$

$270 = 2 \cdot 93 + 84$

$93 = 1 \cdot 84 + 9$

$84 = 9 \cdot 9 + 3$

$9 = 3 \cdot 3$

$g = 3$

3. Gruppen

$\mathbb{Z}_n = \{0,1,...,n-1\}$

1) Nachtrag zu Kapitel 1

Wir haben die Untergruppen von $\mathbb{Z}_n(+)$ $\quad (i+j = \rho_n(i+j))$

Sei $m \in \mathbb{Z}_n$ und m Teiler von n etwa $n = m \cdot R$

$$\langle m \rangle_n = \{0, m, 2m, ..., (R-1)m\}$$
$$= \{i \cdot m \,|\, i \in \mathbb{Z}_R = \{0,1,...,R-1\}\}$$

ist Untergruppe von $\mathbb{Z}_n(+)$

$i, j \in \mathbb{Z}_k$

$i + j = q \cdot R + r, \quad r = \rho_R(i+j)$

$i \cdot m + j \cdot m = (i+j) \cdot m = qR \cdot m + rm$

$\rho_n(...)... = \rho_n(r \cdot m)$

3.1. $(i \cdot m +_n j \cdot m) = (i +_R j) \cdot m$

3.2. Satz

Sei $U \neq \{0\}$ Untergruppe von $\mathbb{Z}_n(+)$ und sei m die kleinste Zahl in $U, m \neq 0$

Dann ist m Teiler von n: $n = m \cdot k$ und $U = \langle m \rangle n$

Beweis:

$\hat{U} = \{i \in \mathbb{Z} \,|\, \rho_n(i) \in U\}$

$(+) \quad U = \hat{U} \cap \mathbb{Z}_n \qquad (1.3\,\text{a})$

- $\hat{U}$ ist Untergruppe von $\mathbb{Z}(+)$, denn
  $\rho_n(i-j) = \rho_n(i) -_n \rho_n(j) \in U$
  $\Rightarrow i - j \in \hat{U}$
- $1.2. \Rightarrow \hat{U} = \langle m \rangle$, $m = \min \hat{U}$
  $(+) \Rightarrow U = \hat{U} \cap \mathbb{Z}_n = \{0, m, 2m, ...\} = \langle m \rangle_n$

$N = N_1 N_2$

$\rho_{N_1}(\rho_N(A)) = \rho_{N_1}(A)$

$\rho_{N_1}(\rho_N(AB)) = \rho_{N_1}(AB)$

$\rho_{N_1}(A \cdot_N B) = A \cdot_{N_1} B$

Beispiel:

$\mathbb{Z}_6 = k$

$U = \{0, k, k +_6 k, k +_6 k +_6 k, ...\} = \{0, k, 2, 0, ...\}$

$\Rightarrow m = 2$

$\Rightarrow U = \langle 2 \rangle_6 = \{0, 2, k\}$

ist Untergruppe, also $\langle 2 \rangle_6 = \langle k \rangle_6$

Definitionen und Bemerkungen

1) $G = \{a, b, c, ...\}$ sei multiplikativ geschriebene Gruppe $(a, b \in G \Rightarrow a \cdot b \in G)$

G1 $a(bc) = (ab)c$ Assoziativität

G2 Es existiert ein neutrales Element: $1 = 1_G$: $1 \cdot a = a \cdot 1 = a$

G3 Zu a existiert ein inverses Element: $a^{-1} \in G$: $a \cdot a^{-1} = a^{-1} \cdot a = 1$

$\Rightarrow a^{-1}$ ist eindeutig

G2 und G3 $\Leftrightarrow a \cdot x = b$ bzw. $x \cdot a = b$

haben genau eine Lösung: $x = a^{-1} \cdot b$ bzw. $x = b \cdot a^{-1}$,

weil $a(a^{-1} \cdot b) = (a \cdot a^{-1}) \cdot b = 1 \cdot b = b$

2) $U \subseteq G$ heißt Untergruppe, wenn U bzgl. der in G erklärten Verknüpfung (Mult.) wieder Gruppe ist.

Es genügt:

$a, b \in U \quad \Rightarrow \quad a \cdot b^{-1} \in U$

$b = (b^{-1})^{-1}$

3) Sei $G(\cdot)$, $H(\cdot)$ zwei Gruppen

$\varphi : G \to H$ ist Homomorphismus

$$\varphi(\underset{\uparrow}{a \cdot b}) = \varphi(a) \underset{\uparrow}{\cdot} \varphi(b)$$
$$G(\cdot) \qquad H(\cdot)$$

Seien R, S Ringe

$\psi : R \to S$ ist Ringhomomorphismus

$\psi(a + b) = \psi(a) + \psi(b)$ Gruppenhomomorphismus

& $\psi(a \cdot b) = \psi(a) \cdot \psi(b)$ Gruppenhomomorphismus

Beispiele:

$G = \mathbb{Z}(+), \quad H = \mathbb{Z}_n(+_n)$

$\varphi = \rho_n$

$\rho_n(a+b) = \rho_n(a) +_n \rho_n(b)$

$\Rightarrow$ ρ_n ist Homomorphismus

Aber: G ist auch Ring und zusätzlich $\rho_n(a \cdot b) = \rho_n(a) \cdot_n \rho_n(b)$

$\Rightarrow$ ρ_n ist Ringhomomorphismus

1) $\varphi(1_G) = 1_H$ $\quad (\varphi(\sigma_R) = \sigma_S)$

2) $\varphi(a^{-1}) = \varphi(a)^{-1}$

3) U Untergruppe $G \Rightarrow \varphi(U)$ Untergruppe von H

$\hat{U}$ Untergruppe von $H \Rightarrow \hat{U} = \{a \in G \mid \varphi(a) \in U\} = \varphi^{-1}(U)$

Untergruppe von G