$G = \langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$

$\varphi : \mathbb{Z}(+) \to G$ Gruppenhomomorphismus

$i \mapsto a^i$ Homomorphiesatz

$\mathbb{Z}/\ker\varphi \cong G$

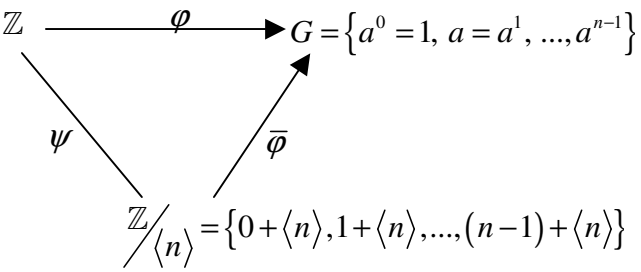
$\ker\varphi = \{i \in \mathbb{Z} \mid a^i = 1\}$ Untergruppe von $\mathbb{Z}(+)$

$n := \min(\ker\varphi)$

$\ker\varphi = \langle n \rangle$

$n = 0,\ \ker\varphi = \{0\}$

$n \geq 1$



Für $i, j \in \mathbb{Z}_n = \{0,1,...,n-1\}$

$$(i+\langle n \rangle)+(j+\langle n \rangle) = \underbrace{\rho_n(i+j)}_{i+_n j}+\langle n \rangle$$

$a^i a^j = a^{i+_n j}$ $\quad G \cong \mathbb{Z}_n(+)$

Sei G eine endliche Gruppe und $a \in G$, $\langle a \rangle$ Untergruppe von G.

Die kleinste Zahl $n \in \mathbb{N}$ mit $a^n - 1$ heißt die **Ordnung** von a $(= 0(a))$

$n := 0(a)$

4.13. a) $a^i = 1 \quad \Leftrightarrow \quad i \in \langle n \rangle$

b) $\langle a \rangle = \{1, a, a^2, ..., a^{n-1}\}$, insbesondere: $|\langle a \rangle| =$

c) Für $i, j \in \mathbb{Z}_n$ gilt $a^i a^j = a^{i+_n j}$

d) n ist Teiler von $|G|$ (Satz v. Lagrange (4.3.))

Beispiel:

$K = \mathbb{Z}_5,\ G = K^* = \{1,2,3,4\} \cong \mathbb{Z}_4$

$a = 2 \quad a^2 = 4 \quad a^3 = 3 \quad a^4 = 1 \quad 0(a) = 4$

$a = 3 \quad a^2 = 4 \quad a^3 = 2 \quad a^4 = 1 \quad 0(a) = 4$

4.14. Sei G eine endliche zyklische Gruppe und a Erzeuger von G (d.h. $G = \langle a \rangle$).

Dann ist: $0(a) = |G|$, ist $n := 0(a)$, so ist G isomorph zur Gruppe $\mathbb{Z}_n(+)$.

In 4.2. haben wir die Untergruppe von $\mathbb{Z}_n(+)$ schon bestimmt.

$\Rightarrow$

4.15. Sei $G=\langle a\rangle$ eine zyklische Gruppe der Ordnung n. Die Untergruppen U von G haben die Form $U=\langle a^m\rangle$, wobei m Teiler von $|G|$ ist.

Ist $k=\frac{n}{m}$ so ist U eine zyklische Gruppe der Ordnung k, insbesondere ist $0(a^m)=k$

4.16. Sei $G=\langle a\rangle$ zyklische Gruppe der Ordnung n.

Sei $0\neq m\in\mathbb{Z}$ und $g=\mathrm{ggT}(n,m)$

Dann ist $0(a^m)=0(a^g)=\frac{n}{g}$

Weiter ist $\langle a^m\rangle=\langle a^g\rangle$ Untergruppe der Ordnung $\frac{n}{g}$.

Beweis: $g/m \Rightarrow m=i\cdot g \Rightarrow a^m=(a^g)^i\in\langle a^g\rangle$

$\Leftrightarrow \langle a^m\rangle\subseteq\langle a^g\rangle$

$g=pm+qn$ (Bezout)

$a^g=a^{pm+qn}=a^{pm}\cdot a^{qn}=(a^m)^p:(a^n)^q$

$\langle a^g\rangle\subseteq\langle a^m\rangle$

$\Rightarrow$

4.17. Sei $G=\langle a\rangle$ eine zyklische Gruppe der Ordnung n.

Genau dann ist eine Potenz a^m Erzeuger von G, wenn $\mathrm{ggT}(n,m)=1$

4.18. Ist n eine Primzahl, so ist jedes Element $\neq 1$ aus $G=\langle a\rangle$ Erzeuger.

Im folgenden sei G eine abelsche, endliche Gruppe

„Primfaktorzerlegung in *G*“

„G ist direktes Produkt von Untergruppen $G_1,...,G_r$“

$G_1,...,G_r$ Untergruppen von G

$G_1\times G_2\times...\times G_r=\{(a_1,a_2,...,a_r)\,|\,a_i\in G_i\}$

Kartesisches Produkt $|G_1\times...\times G_r|=\prod_{i=1}^{r}|G_i|$

Ist die Abbildung $\beta: G_1\times...\times G_r\to G$ mit $(a_1,...,a_r)\mapsto a_1,...,a_r$ bijektiv, so heißt G das **direkte Produkt** von $G_1,...,G_r$, $(G=G_1\times...\times G_r)$

d.h.: Zu $a \in G$ existieren in eindeutiger Weise Elemente $a_i \in G_i$ mit $a = a_1 a_2 ... a_r$

Sei genauso $b = b_1, ..., b_r \in G,\ b_i \in G_i$

$a \cdot b = (a_1 .... a_r)(b_1 .. b_r) = (a_1 b_1)(a_2 b_2) ... (a_r b_r)$

Multiplikation ist komponentenweise

$m \in \mathbb{N} : G(m) := \{ a \in G \mid a^m \}$

$a \in G(m) \quad \Leftrightarrow \quad 0(a) \mid m \qquad (4.13.)$

4.19. a) $G(m)$ ist Untergruppe von G

b) $\exists$ ein $m \in \mathbb{N}$ mit $G = G(m)$

$[4.13.\ d)]\ 0(a)$ teilt $|G| =: m$

$a^m = 1$ [4.13. a)]

$m = \prod_{a \in G} 0(a) \quad \Rightarrow \quad G(m) = 1$

zu a) z.Z. $a^m = 1,\ b^m = 1$

$(ab^{-1}) = a^m (b^{-1})^m = a^m (b^m)^{-1} = 1$

$\Rightarrow \quad ab^{-1} \in G(m)$

4.20. Satz

Seien m_1, m_2 teilerfremde Zahlen aus $\mathbb{N}$, so dass $G = G(m_1, m_2)$

Setzen $G_1 := G(m_1),\ G_2 := G(m_2)$

a) $G = G_1 \times G_2$

b) Ist $a = a_1 a_2$ mit $a_i \in G_i$, so ist $0(a) = 0(a_1) 0(a_2)$

Beweis:

a) $a \in G_1$ bzw. $a \in G_2$: $\underbrace{(a^{m_1})^{m_2}}_{=1} = \underbrace{(a^{m_2})^{m_1}}_{=1} = 1$

$\Rightarrow G_1$ und G_2 Untergruppen von G

Sei $a \in G_1, G_2 \ \Rightarrow\ 0(a)$ ist Teiler von m_1 und m_2

(1) $G_1 \cap G_2 = 1$

Bezout $\quad 1 = i \cdot m_1 + j \cdot m_2 \quad i, j \in \mathbb{Z}$

$a \in G,\ a = a^1 = a^{i \cdot m_1 + j \cdot m_2} = \underbrace{a^{i \cdot m_1}}_{a_2} \cdot \underbrace{a^{j \cdot m_2}}_{a_1} = a_1 a_2$

$$a_1^{m_1} = a^{m_2 m_1 j} = \left(a^{m_2 m_1}\right)^j = 1 \quad a_1 \in G_1$$

$$a_2^{m_2} = \left(a^{m_2 m_1}\right)^i = 1 \qquad a_2 \in G_2$$

$$a = a_1 a_2 = b_1 b_2, \quad b_i \in G_i$$

$$\underbrace{b_1^{-1} a_1}_{=1} = b_2 a_2^{-1} \in G_1 \cap G_2$$

$$a_1 = b_1,\ b_2 = a_2$$

b) $k := 0(a),\ a = a_1 a_2$

$$1 = a^k = (a_1 a_2)^k = a_1^k a_2^k = 1$$

$$a_1^k = \left(a_2^k\right)^{-1} \in G_1 \cap G_2 = 1$$

(2) k ist Teiler von m_1, m_2

$0(a_1)$ und $0(a_2)$ sind Teiler von k

$0(a_1) \mid m_1,\ 0(a_2) \mid m_2$

$\text{ggT}(m_1, m_2) = 1 \Rightarrow\ 0(a_1), 0(a_2)$ Teiler von k

Sei $G = G(m)$

Sei $m = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$ Primfaktorzerlegung von m

$$G = G(m) = G\left(p_1^{e_1} \cdot \left(p_2^{e_2} \cdots p_r^{e_r}\right)\right) = G_{p_1^{e_1}} \times \underbrace{G\left(p_2^{e_2} \cdots p_r^{e_r}\right)}_{= G_{p_2^{e_2}} \times G\left(p_3^{e_3} \cdots p_r^{e_r}\right)}$$

$$= G\left(p_1^{e_1}\right) \times G\left(p_2^{e_2}\right) \times \ldots \times G\left(p_r^{e_r}\right)$$