G endlich, abelsch

$G(m) = \{a \in G \mid a^m = 1\}$

Untergruppe von G $\quad o(a) \mid m$

4.21. $G = G(m) \qquad (m = |G|)$

$m = m_1 \cdot m_2, \ \text{ggT}(m_1, m_2) = 1$

a) $G = G(m_1) \times G(m_2)$

b) $a = a_1 \cdot a_2$

$o(a) = o(a_1) \cdot o(a_2)$

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

a) (1) $G_1 \cap G_2 = \{1\}$

$1 = i \cdot m_1 + j \cdot m_2$

$a = a^1 = a^{i \cdot m_1 + j \cdot m_2} = a^{i \cdot m_1} \cdot a^{j \cdot m_2}$

(2) $\underbrace{a_1 := a^{j \cdot m_2}}_{\in G_1}, \ \underbrace{a_2 := a^{i \cdot m_1}}_{\in G_2}$

$a_1^{m_1} = \left(a^{j \cdot m_2}\right)^{m_1} = \left(a^{m_1 \cdot m_2}\right)^j = \left(a^m\right)^j = 1$

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

$\underset{\in G_1}{b_1^{-1} a_1} = \underset{\in G_2}{b_2 a_2^{-1}} \quad \Rightarrow \quad b_1^{-1} a_1 = b_2 a_2^{-1} = 1$

$a \in G$

$k := o(a), \ k_1 = o(a_1), \ k_2 = o(a_2)$

$a^{k_1 k_2} = (a_1 a_2)^{k_1 k_2} = \left(a_1^{k_1}\right)^{k_2} \left(a_2^{k_2}\right)^{k_1} = 1$

$\Rightarrow \underset{\uparrow \text{ Teiler von } \uparrow}{k \mid k_1 k_2}$

Gegenbeispiel :

$12 \mid 24$

$6 \mid 24$

$\Rightarrow 12 \cdot 6 \neq 24$

$(2) \Rightarrow \quad k_1$ Teiler von $0(a) = k$

k_2 Teiler von $o(a) = k$

$k_1 \mid m_1, \ k_2 \mid m_2, \ m_1, \ m_2$ teilerfremd

$k_1, \ k_2$ teilerfremd $\quad \Rightarrow \quad k_1 k_2$ Teiler von k

$m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ Primfaktorzerlegung

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

4.22. Sei $G = G(m)$, $(\text{z.B. } m = |G|)$

$$G = \underbrace{G\left(p_1^{e_1}\right)}_{z_1} \times \underbrace{G\left(p_2^{e_2}\right)}_{z_2} \times \ldots \times \underbrace{G\left(p_r^{e_r}\right)}_{z_r}$$

$$a = a_1 \cdot a_2 \cdots a_r$$

$$o(a) = o(a_1) \cdot o(a_2) \cdots o(a_r)$$

$G\left(p_i^{e_i}\right)$ **Primärkomponenten** (**Sylowgruppe**)

4.23. Satz

Sei $z \in G$ ein Element von maximaler Ordnung in G und sei $m := o(z)$

Dann gilt $a^m = 1$ für alle $a \in G \quad (m = \exp G)$

4.24. Korollar

Sei K Körper und G eine endliche Untergruppe der multiplikativen Gruppe K^*.
Dann ist G eine zyklische Gruppe.

4.23. $\Rightarrow$ 4.24.

Wir zeigen $G = \langle z \rangle$, $a^m = 1$, $a^m - 1 = 0$

a ist Nullstelle von $X^m - 1$

$X^m - 1$ besitzt höchstens m Nullstellen $\Rightarrow |G| \le m$

$\langle z \rangle$ ist Untergruppe der Ordnung m

Beweis von 4.23.

Sei z_i aus $G\left(p_i^{e_i}\right)$ von maximaler Ordnung $\qquad i = 1, \ldots, r$

$o(z_i) = p_i^{m_i}$

Sei $a_i \in G\left(p_i^{e_i}\right)$ und $o(a_i) = p^t$

$$p_i^{\,t} \le p_i^{m_i} \Rightarrow p_i^{\,t} \mid p_i^{m_i}$$

$\Rightarrow o(a_i)$ teilt $a(z_i)$ für alle $a_i \in G\left(p_i^{e_i}\right)$

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

$$z = z_1 \cdot z_2 \cdots z_3$$

$$z := z_1 \cdot z_2 \cdots z_r$$

$$o(z) = o(z_1) \cdots o(z_r) = m$$

$$o(a) = \underbrace{o(a_1)}_{\text{teilt } o(z_1)} \cdot \underbrace{o(a_2)}_{\text{teilt } o(z_2)} \cdots \underbrace{o(a_r)}_{\text{teilt } o(z_r)} \text{ teilt } o(z) = m$$

G beliebige Gruppe
Ein Homomorphismus
$\alpha: G \to G$
$\big(\alpha(ab) = \alpha(a)\alpha(b)\big)$
heißt **Automorphismus**, wenn α bijektiv ist.

Auf G ist die Menge der Automorphismen von G
$\alpha, \beta \in \operatorname{Aut} G$
$\alpha \circ \beta: \; a \mapsto \alpha\big(\beta(a)\big)$ Komposition

4.25. Bezüglich dieser Verknüpfung ist $\operatorname{Aut} G$ eine Gruppe

1) $\overbrace{(\alpha \circ \beta)}^{\in \operatorname{Aut} G}(ab) = \alpha\big(\beta(ab)\big) = \alpha\big(\beta(a)\beta(b)\big)$
$= \alpha\big(\beta(a)\big)\alpha\big(\beta(b)\big) = \ldots = (\alpha \circ \beta)(a)(\alpha \circ \beta)(b)$
$\Rightarrow$ Homomorphismus

2) Assoziativgesetz: $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$

3) id_G ist neutrales Element

4) α^{-1} ist die Umkehrabbildung
$\alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = \mathrm{id}$ (Inverse)

z.Z. Umkehrabbildung ist Homomorphismus
$\Rightarrow \; \alpha^{-1}(ab) = \alpha^{-1}(a)\alpha^{-1}(b)$
$\alpha^{-1}(ab) = c \quad \Leftrightarrow \quad \alpha(c) = ab$
$\alpha^{-1}(a) = c_1 \quad \Leftrightarrow \quad \alpha(c_1) = a$
$\alpha^{-1}(b) = c_2 \quad \Leftrightarrow \quad \alpha(c_2) = b$
$\alpha(c_1 c_2) = \alpha(c_1)\alpha(c_2) \overset{\text{Hom.}}{=} ab$
$\alpha^{-1}(ab) = c_1 c_2 = \alpha^{-1}(a)\alpha^{-1}(b)$

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

Für $j \in \mathbb{Z}$ definiert $\alpha_j: G \to G$ mit $a^i \mapsto \big(a^i\big)^j = a^{ij} = \big(a^j\big)^i$

α_j ist Homomorphismus $\quad a^i a^k = a^{i+k} \overset{\alpha_j}{\mapsto} a^{(i+k)j} = a^{ij}a^{kj} = \alpha_j\big(a^i\big)\alpha_j\big(a^k\big)$

- $\operatorname{im} \alpha_j = \langle \alpha^j \rangle$
- $\alpha_{j_1} \circ \alpha_{j_2}: G \to G$ mit $a^i \mapsto \Big(\big(a^i\big)^{j_2}\Big)^{j_1} = \big(a^i\big)^{j_1 j_2}$
$\alpha_{j_1} \circ \alpha_{j_2} = \alpha_{j_1 j_2}$

Beispiele (additiv):

1) $G = \mathbb{Z}(+) \quad (= \langle 1 \rangle)$

$\alpha_j(i) = j \cdot i$ (injektiv für $j \neq 0$)

$\operatorname{im} \alpha_j = \langle j \rangle$

α_j Automorphismus $\Leftrightarrow \quad j = \pm 1$

$\operatorname{Aut}(\mathbb{Z}(+)) = \underset{\text{"Einheitsgruppe"}}{\mathrm{E}(\mathbb{Z})} = \{-1, +1\}$

2) $G = \mathbb{Z}_n(+) = \langle 1 \rangle_n$

$\alpha_j \in \operatorname{Aut} G \quad \Leftrightarrow \quad \langle j \rangle_n = \mathbb{Z}_n(+)$

$\Leftrightarrow \quad j$ teilerfremd zu n

Ergebnis $\operatorname{Aut} G \triangleq \mathrm{E}_n(\mathbb{Z}_n)$

5. Die Interpolation

K Körper, $\xi_1, ..., \xi_n$ seien verschiedene Elemente von K

$A = a_0 + a_1 X + ... + a_n X^n \in K[X]$

Definierte Abbildung von $K[X] \to K^n$ ist $A \mapsto \underbrace{\left(\overset{=v_1}{A(\xi_1)}, \overset{=v_2}{A(\xi_2)}, ..., \overset{v_n}{A(\xi_n)} \right)}_{=\operatorname{val} A}$

Einsetzungsregel $\Rightarrow$ val ist eine Lineare Abbildung

$v(\lambda A + \mu B) = \lambda(\operatorname{val} A) + \mu(\operatorname{val} B)$

ker val?

↳ $A(\xi_i) = 0 \quad \forall i = 1, ..., n \quad \Rightarrow \quad A \mapsto (0, 0, ..., 0)$

↳ $(X - \xi_1)$ Teiler von A

$$N := \prod_{i=1}^{n} (X - \xi_i) = X^n - (\xi_1 + ... + \xi_n) X^{n-1} + ... + \xi_1 \xi_2 \cdots \xi_n$$

5.2. Interpolationssatz

Zu jedem $v = (v_1, ..., v_2) \in K^n$ existiert genau ein Polynom $A \in K_n[X]$ mit $\operatorname{val} A = (v_1, ..., v_n)$.

Interpolationsoperator:

Sei $\Pi : K^n \to K_n[X]$ die Umkehrabbildung von val′

$\Pi r = A \quad \Leftrightarrow \quad \operatorname{val} A = r$

$\Pi \underbrace{(\operatorname{val} A)}_{=r} = A$

$$v = \begin{pmatrix} 1 & \xi_1 & \xi_1^2 & \cdots \xi_1^{n-1} \\ 1 & \xi_2 & \xi_2^2 & \xi_2^{n-1} \\ \vdots & & & \vdots \\ 1 & \xi_n & \xi_n^2 & \cdots \xi_n^{n-1} \end{pmatrix}$$

$$v = \mathrm{val}' A = v \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}$$

$$V^{-1} v = \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix}$$

d.h. Zu der linearen Abbildung val' gehört die Matrix V und zu der Abbildung Π gehört die Matrix V^{-1}.