Restklassengruppen

Def. G Gruppe, H eine Untergruppe von G.
Für $x, y \in G$ schreibe $x \overset{H}{\sim} y$ (bzw. $x \equiv y \bmod H$), wenn

$$y x^{-1} \in H \text{ gilt } (\Leftrightarrow y \in Hx)$$

[im Falle einer abelschen Gruppe G mit $\circ$ notiert als $+$ besagt $x \overset{H}{\sim} y$ also $y - x \in H$]

Wie man leicht nachprüft, ist $\overset{H}{\sim}$ eine Äquivalenzrelation.
Mit G/H bezeichne die Menge der zugehörigen Äquivalenzklassen; ("Restklassen")
die Abb.

δ (*)
$$\begin{aligned} G &\longrightarrow G/H \\ x &\longmapsto \bar{x} := Hx \end{aligned}$$
heißt Restklassenabbildung

Beh. Die Relation $\overset{H}{\sim}$ ist verträglich mit Multipl. von G, falls G abelsch ist (sonst i.a. nicht!): $x \overset{H}{\sim} x',\ y \overset{H}{\sim} y' \Longrightarrow xy \overset{H}{\sim} x'y'$

Bew. $$x'y'(xy)^{-1} = x'y'y^{-1}x^{-1} \overset{!}{=} \underbrace{x'x^{-1}}_{\in H} \underbrace{y'y^{-1}}_{\in H} \in H \quad \checkmark$$

Nach der Beh. gilt also: Ist G abelsch, so ist G/H eine Gruppe, für die (*) ein Homomorphismus ist.

Bem. Ist G eine beliebige Gruppe, so gilt die entsprechende Aussage für G/H genau dann, wenn für H gilt:

$$Hx = xH \quad \text{für jedes } x \in G$$

Bew. als ÜA.

δ Ist G endlich, so hat man $\#G/H = \#G / \#H$.
Denn G ist die disjunkte Vereinigung der verschiedenen Äquivalenzklassen Hx, und es gilt $\#Hx = \#H$.

<u>F2:</u> Sei G eine <u>abelsche Gruppe</u> der Ordnung n und

$$n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r}$$

sei die Primfaktorzerlegung von n. Für $1 \le i \le r$ sei

$$G_{p_i} := \{ \alpha \in G \mid \alpha^{p_i^{\nu_i}} = 1 \} \qquad \text{[Untergruppe von } G\text{]}$$

Dann ist die Abbildung

$$(1) \quad f: \prod_{i=1}^{r} G_{p_i} \longrightarrow G$$
$$(\alpha_1, \dots, \alpha_r) \longmapsto \alpha_1 \alpha_2 \cdots \alpha_r$$

ein Isomorphismus von Gruppen (G also isomorph zum direkten Produkt der Gruppen $G_{p_1}, \dots, G_{p_r}$). Ferner gilt

$$\# G_{p_i} = p_i^{\nu_i} \qquad \text{für } 1 \le i \le r$$

$q_i p_i^{\nu_i} = n$ <u>Bew.</u> $q_i := \frac{n}{p_i^{\nu_i}}$; dann $(q_1, \dots, q_r) = 1$. $\Rightarrow \exists x_1, \dots, x_r \in \mathbb{Z}$ mit

$$(2) \quad x_1 q_1 + x_2 q_2 + \dots + x_r q_r = 1, \qquad \Longrightarrow$$

$$(2') \quad \alpha = \alpha^1 = \alpha^{x_1 q_1} \alpha^{x_2 q_2} \cdots \alpha^{x_r q_r}$$

Es ist $\alpha^{x_i q_i} \in G_{p_i}$, denn $\alpha^{x_i q_i p_i^{\nu_i}} = \alpha^{n x_i} = 1$.

Betrachte nun die Abb.

$$g: G \longrightarrow \prod_{i=1}^{r} G_{p_i}, \quad \text{def. durch}$$
$$\alpha \longmapsto (\alpha^{x_1 q_1}, \alpha^{x_2 q_2}, \dots, \alpha^{x_r q_r})$$

Dann $\quad f \circ g = id_G \quad$ nach (2'). Mit $\tilde{G} := \prod_{i=1}^{r} G_{p_i}$ gilt auch

$$g \circ f = id_{\tilde{G}},$$

denn $(g \circ f)(\alpha_1, \dots, \alpha_r) = g(\alpha)$ mit $\alpha = \alpha_1 \cdots \alpha_r$ und daher

$$\alpha^{x_i q_i} = \alpha_i^{x_i q_i} \overset{(2)}{=} \alpha_i, \quad g(\alpha) = (\alpha_1, \dots, \alpha_r).$$

f ist also ein Isomorphismus; insbesondere gilt

$$\# G = \prod_{i=1}^{r} \# G_{p_i}$$

Beh. $\# G_{p_i}$ = Potenz von p_i

Ist Beh. bewiesen, so folgt aus Eindeutigkeit der Primfaktorzerlegung

$$\# G_{p_i} = p_i^{\nu_i} \quad \text{für alle } 1 \le i \le r$$

Bew. der Beh. zum Nachdenken: Zeige für Primzahl p und $\nu \in \mathbb{N}$:
Ist G endliche abelsche Gruppe mit $\alpha^{p^\nu} = 1$ für alle $\alpha \in G$, so ist $\# G$ eine Potenz von p.

⌜Bew.: o.E. $\exists \beta \neq 1$ in G. Jedenfalls $\# \langle\beta\rangle = p$-Potenz.
Betrachte die Restklassengruppe $\bar{G} := G / \langle\beta\rangle$. Dann

$$\# \bar{G} = \frac{\# G}{\# \langle\beta\rangle} < \# G, \qquad \bar{\alpha}^{p^\nu} = \bar{1} \text{ für alle } \bar{\alpha} \in \bar{G}.$$

Per Induktion ist $\# \bar{G}$ eine p-Potenz. Damit auch

$$\# G = \# \bar{G} \cdot \# \langle\beta\rangle. \quad ⌟$$

Jetzt Beweis von F1:

(i) Spezieller Fall: Sei $e = e(G)$ Potenz einer Primzahl p.
Für bel. $\alpha \in G$ ist dann $\operatorname{ord}(\alpha) = p^{\mu_\alpha}$ mit $\mu_\alpha \in \mathbb{N}_0$. Setze $\mu := \operatorname{Max}\{\mu_\alpha \mid \alpha \in G\} = \mu_\omega$ mit einem $\omega \in G$.
Dann offenbar

$$e = p^\mu = \operatorname{ord}(\omega),$$

also ist ω ein Elt. mit $\operatorname{ord}(\omega) = e$.

(ii) <u>Allgemeiner Fall:</u> Nach F2 besteht die Isomorphie

(1) $\prod_{i=1}^{r} G_{p_i} \simeq G$

Setzt man also $\tilde{G} := \prod_{i=1}^{r} G_{p_i}$, so darf man G durch $\tilde{G} \simeq G$ ersetzen. Wir behaupten, daß

(2) $\operatorname{ord}((\alpha_1,\dots,\alpha_r)) = \operatorname{kgV}(\operatorname{ord}(\alpha_1),\dots,\operatorname{ord}(\alpha_r))$ [1]

für jedes $(\alpha_1,\dots,\alpha_r) \in \tilde{G}$ gilt, sowie

(3) $e(\tilde{G}) = \operatorname{kgV}(e(G_{p_1}),\dots,e(G_{p_r}))$ [1]

Damit läßt sich die Aussage von F1 wie folgt auf den schon erledigten Fall (i) zurückführen: In jedem G_{p_i} gibt es ein ω_i mit $\operatorname{ord}(\omega_i) = e(G_{p_i})$. Damit erhält man

$$\operatorname{ord}((\omega_1,\dots,\omega_r)) \overset{(2)}{=} \operatorname{kgV}(\operatorname{ord}(\omega_1),\dots,\operatorname{ord}(\omega_r)) =$$
$$\operatorname{kgV}(e(G_{p_1}),\dots,e(G_{p_r})) \overset{(3)}{=} e(\tilde{G})$$

—

Zum Beweis von (2) und (3) betrachten wir allgemeiner ein beliebiges endliches <u>direktes Produkt</u> $\tilde{G} = G_1 \times \dots \times G_r$ endlicher (abelscher) Gruppen G_i. Sei $(\alpha_1,\dots,\alpha_r) \in \tilde{G}$ und $m \in \mathbb{Z}$. Dann hat man die Äquivalenzkette

$1 = (1,\dots,1)$

$(\alpha_1,\dots,\alpha_r)^m = 1 \Leftrightarrow \alpha_i^m = 1$ für $1 \le i \le r \Leftrightarrow \operatorname{ord}(\alpha_i) \mid m$ für $1 \le i \le r \Leftrightarrow$
$\operatorname{kgV}(\operatorname{ord}(\alpha_1),\dots,\operatorname{ord}(\alpha_r)) \mid m$; somit

(4) $(\alpha_1,\dots,\alpha_r)^m = 1 \Leftrightarrow \operatorname{kgV}(\operatorname{ord}(\alpha_1),\dots,\operatorname{ord}(\alpha_r)) \mid m$

Setze $k = \operatorname{kgV}(\operatorname{ord}(\alpha_1),\dots,\operatorname{ord}(\alpha_r))$ und $l = \operatorname{ord}((\alpha_1,\dots,\alpha_r))$. Dann ist

---

[1] wegen der paarw. Teilerfremdheit von $\operatorname{ord}(\alpha_1),\dots,\operatorname{ord}(\alpha_r)$ kann man schreiben:

$$\operatorname{ord}((\alpha_1,\dots,\alpha_r)) = \operatorname{ord}(\alpha_1) \cdot \operatorname{ord}(\alpha_2) \cdot \ldots \cdot \operatorname{ord}(\alpha_r).$$

Entsprechend ist auch

$$e(\tilde{G}) = e(G_{p_1}) \cdot e(G_{p_2}) \cdot \ldots \cdot e(G_{p_r})$$

die rechte Seite von (4) für $m=k$ erfüllt, und es folgt $(\alpha_1,\dots,\alpha_r)^k=1$, also $l \mid k$. Für $m=l$ ist die linke Seite erfüllt, also folgt $k \mid l$. Insgesamt ist also $l=k$, d.h. es gilt (2).

Die rechte Seite von (2) ist ein Teiler von $\mathrm{kgV}(e(G_1),\dots,e(G_r))$; dies gilt für alle $(\alpha_1,\dots,\alpha_r)\in\tilde{G}$, daher folgt

$$e(\tilde{G}) \mid \mathrm{kgV}(e(G_1),\dots,e(G_r))$$

Für jedes $\alpha_i\in G_i$ ist offenbar $\alpha_i^{e(\tilde{G})}=1$. Es folgt $e(G_i)\mid e(\tilde{G})$ für jedes $1\le i\le r$ und somit

$$\mathrm{kgV}(e(G_1),\dots,e(G_r)) \mid e(\tilde{G})$$

Zusammengenommen erhält man (3). q.e.d.

<u>Bem. 1:</u> G endliche Gruppe, $\alpha\in G$, $j\in\mathbb{Z}$. Dann gilt

$$\mathrm{ord}(\alpha^j) = \frac{\mathrm{ord}(\alpha)}{(\mathrm{ord}(\alpha), j)}$$

<u>Bew.</u> $k:=\mathrm{ord}(\alpha)$, $d:=(k,j)$. $(\alpha^j)^{\frac{k}{d}} = \alpha^{k\frac{j}{d}} = 1$,

$\Longrightarrow \mathrm{ord}(\alpha^j) \mid \frac{k}{d}$. Umgekehrt:

$1=(\alpha^j)^{\mathrm{ord}(\alpha^j)} \Longrightarrow \mathrm{ord}(\alpha)\mid j\,\mathrm{ord}(\alpha^j) \Rightarrow \frac{k}{d} \mid \frac{j}{d}\mathrm{ord}(\alpha^j)$

$\xRightarrow{(\frac{k}{d},\frac{j}{d})=1} \frac{k}{d} \mid \mathrm{ord}(\alpha^j)$. ✓

<u>Bem. 2</u>: Eine zyklische Gruppe G der Ordnung n hat genau $\varphi(n)$ Elemente der Ordnung n.

<u>Bew.</u> Nach Vor. ex. ein $\alpha \in G$ mit $G = \langle\alpha\rangle$.

Wissen: $\langle\alpha\rangle = \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ mit $n = \operatorname{ord}(\alpha) = \operatorname{ord}(G)$

$$\operatorname{ord}(\alpha^j) = n \overset{\text{Bem. 1}}{\iff} (\underset{\substack{\| \\ n}}{\operatorname{ord}(\alpha)}, j) = 1$$

$$\#\{\beta \in G \text{ mit } \operatorname{ord}(\beta) = n\} = \#\{j \in \mathbb{Z} \mid 0 \le j < n, (j, n) = 1\}$$
$$= \varphi(n).$$

<u>Anw.</u> $G = (\mathbb{Z}/p\mathbb{Z})^\times$ ist zyklisch von der Ordnung $p-1$.

Also gibt es genau $\varphi(p-1)$ Elemente der Ordnung $p-1$,

$\Longrightarrow$ Zusatz zu Satz 1. $\square$

<u>Nochmals</u>: G endl. Gruppe der Ordnung n, $\alpha \in G$.

$$G = \langle\alpha\rangle \iff \operatorname{ord}(\alpha) = n$$

Ein Element α von G mit $G = \langle\alpha\rangle$ heißt ein <u>Erzeuger von G</u>.

Besitzt G einen Erzeuger, so ist G <u>zyklisch</u>.

Eine zyklische Gruppe der Ordnung n besitzt genau $\varphi(n)$ Erzeuger.