1 Basics

1.1 Mengen

Lemma 1. *Sei H Teilmenge von K, dann ist $|H| \leq |K|$.*

Lemma 2. *Seien H und K Mengen. Falls $H \subseteq K$ und $|H| = |K|$, dann ist $H = K$.*

1.2 Gruppen

Lemma 3. *Seien H und K Untergruppen von G, dann ist $H \cap K$ Untergruppe von H (und K).*

Lemma 4. *Seien H und K Untergruppen von G. Falls $H \subseteq K$, dann ist H Untergruppe von K.*

1.3 Produkt von Untergruppen

Definition 1. *Seien H und K Untergruppen einer Gruppe G, dann ist das Produkt von H und K definiert als $HK := \{hk \mid h \in H, k \in K\}$.*

Lemma 5. *Seien U und P Untergruppen einer Gruppe G. Falls $u^{-1}Pu = P$ für alle $u \in U$, dann ist UP eine Untergruppe von G.*

Lemma 6. *Seien H und K Untergruppen einer Gruppe G, dann ist $K \subseteq HK$.*

Lemma 7. *Seien H und K Untergruppen einer Gruppe G. Falls $HK = K$ (als Mengen), dann ist H Unterguppe von K.*

Lemma 8. *Seien H und K Untergruppen von G, dann ist $|HK| = \frac{|H||K|}{|H \cap K|}$.*

Lemma 9. *Seien H und K p-Untergruppen von G, dann ist $|HK| = p^l$ für ein $l \in \mathbb{N}$.*

Proof. Nach Lemma 3 und dem Satz von Lagrange ist $H \cap K$ eine p-Untergruppe. Die Aussage folgt mit Lemma 8 und Rechnen mit Primzahlen. □

1.4 Gruppenoperationen

Theorem 1. *Bahnensatz*

Theorem 2. *Lagrange*

Lemma 10. *Sei $\rho : G \times M \to M$ eine Gruppenoperation. Dann ist $x \sim y \iff \exists g \in G : g \bullet_\rho x = y$ eine Äquivalenzrelation.*

Lemma 11. *Sei $\sim$ eine Äquivalenzrelation auf einer endlichen Menge M. Dann gilt $|M| = \sum_{x \in R} |[x]|$ wobei R ein Repräsentantensystem und $[x]$ die Äquivalenzklasse von x ist.*

Für $g \in G$ definiere $\alpha_g : G \to G, \quad (g,h) \mapsto g^{-1}hg$.

Lemma 12. $\alpha_g \circ \alpha_h = \alpha_{gh}$.

Lemma 13. $\alpha_1 = id$.

Lemma 14. $\alpha_g \circ \alpha_{g^{-1}} = id$.

Proof. Folgt aus Lemma 12 und 13. □

Lemma 15. *Für alle $g \in G$ ist α_g eine Bijektion.*

Proof. Folgt aus Lemma 14. □

Lemma 16. *Sei $g \in G$ und Q eine Untergruppe von G, dann ist $\alpha_g(Q)$ eine Untergruppe von G.*

Lemma 17. *Sei U Untergruppe von G, dann ist $\alpha_u(U) = U$ für alle $u \in U$.*

Lemma 18. *Sei $\rho : G \times M \to M$ eine Gruppenoperation. Falls $|Orb_\rho(m)| = 1$ für ein $m \in M$, dann ist $g \bullet_\rho m = m$ für alle $g \in G$.*

2 Hilfssätze für Sylow

Seien G eine endliche Gruppe und $p \in \mathbb{N}$ eine Primzahl. Seien $r, m \in \mathbb{N}$ sodass $|G| = p^r m$ und $p \nmid m$. Wir schreiben $\mathrm{Syl}_p(G) = \{P \leq G \mid |P| = p^r\}$ für die Menge der p-Sylow-Untergruppen.

Lemma 19. $\alpha : G \times Syl_p(G) \to Syl_p(G), \quad (g,Q) \mapsto \alpha_g(Q)$ *ist eine Gruppenoperation.*

Proof. Beachte: α_g ist formal nicht dasselbe wie $\alpha(g,\cdot)$. Erstere ist die oben definierte Abbildung, die auf Elementen von G wirkt, letztere wirkt auf Teilmengen von G.
Wir zeigen zuerst, dass α wohldefiniert ist. Dazu sei $g \in G$ und $Q \in \mathrm{Syl}_p(G)$. Nach Lemma 16 ist $\alpha_g(Q)$ eine Untergruppe und nach Lemma 15 gilt $|Q| = |\alpha_g(Q)|$, also ist $Q \in \mathrm{Syl}_p(G)$.
Die Eigenschaften $\alpha(1,\cdot) = \mathrm{id}$ und $\alpha(gh,\cdot) = \alpha(g,\cdot) \circ \alpha(h,\cdot)$ folgen aus Lemma 13 und Lemma 12. □

Theorem 3. *Es gilt $Syl_p(G) \neq \emptyset$.*

Von hier an fixiere ein $Q \in \mathrm{Syl}_p(G)$.

Lemma 20. $p^r \mid |Stab_\alpha(Q)|$

Proof. Es gilt $Q \subseteq \mathrm{Stab}_\alpha(G)$ nach Lemma 17, also $Q \leq \mathrm{Stab}_\alpha(G)$ nach Lemma 4. Mit Lagrange folgt dann $p^r = |Q| \mid |\mathrm{Stab}_\alpha(G)|$. □

Lemma 21. *Seien $a, b, c, d \in \mathbb{N}$. Angenommen $a \mid c$ und $ab = cd$, dann folgt $d \mid b$.*

Theorem 4. $|Orb_\alpha(Q)| \mid m$

Proof. Gemäß des Bahnensatzes gilt $p^r m = |G| = |\mathrm{Orb}_\alpha(Q)| \cdot |\mathrm{Stab}_\alpha(Q)|$. Weiterhin gilt $p^r \mid |\mathrm{Stab}_\alpha(Q)|$ nach Lemma 20. Also können wir Lemma 21 anwenden mit $a = p^r, b = m, d = |\mathrm{Orb}_\alpha(Q)|, c = |\mathrm{Stab}_\alpha(Q)|$, was die zu zeigende Aussage liefert. □

Lemma 22. *$\beta : U \times Orb_\alpha(Q) \to Orb_\alpha(Q), \quad (u, P) \mapsto \alpha_u(P)$ ist eine Gruppenoperation.*

Proof. β ist wohldefiniert da $\alpha_u(\alpha_g(Q)) = \alpha_{ug}(Q)$ nach Lemma 12. Die Axiome der Gruppenoperation werden wie bei α gezeigt. □

Lemma 23. *Für $P \in Orb_\alpha(Q)$ gilt $|Orb_\beta(P)| = 1$ oder $p \mid |Orb_\beta(P)|$*

Proof. Nach dem Bahnensatz ist $p^l = |U| = |\mathrm{Orb}_\beta(P)| \cdot |\mathrm{Stab}_\beta(P)|$, und die Aussage folgt aus Eigenschaften von Primzahlen. □

Sei R ein Repräsentantensystem der Bahnen von β.

Lemma 24. *Es existiert ein $P \in Orb_\alpha(Q)$ mit $|Orb_\beta(P)| = 1$.*

Proof. Angenommen $p \mid |\mathrm{Orb}_\beta(P)|$ für alle $P \in R$, dann folgt

$$p \mid \sum_{P \in R} |\mathrm{Orb}_\beta(P)|$$

nach (?). Gleichzeitig ist

$$|\mathrm{Orb}_\alpha(Q)| = \sum_{P \in R} |\mathrm{Orb}_\beta(P)|$$

nach Lemma 10 und Lemma 11, also folgt $p \mid |\mathrm{Orb}_\alpha(Q)|$. Andererseits haben wir aber $|\mathrm{Orb}_\alpha(Q)| \mid m$ nach Theorem 4. Das bedeutet $p \mid m$ nach (?), Widerspruch zur Voraussetzung. Also muss unsere anfängliche Annahme falsch gewesen sein, woraus mittels Lemma 23 die Existenz eines $P \in \mathrm{Orb}_\alpha(Q)$ mit $|\mathrm{Orb}_\beta(P)| = 1$ folgt. □

Theorem 5. *Sei U eine p-Untergruppe und $P \in Syl_p(G)$. Falls $|Orb_\beta(P)| = 1$, dann folgt $U \leq P$.*

Proof. Nach Lemma 18 und der Definition von β ist $u^{-1}Pu = P$ für alle $u \in U$.
Nach Lemma 5 ist dann UP eine Untergruppe von G.
Nach Lemma 9 ist außerdem $|UP|$ eine Potenz von p, also ist UP eine p-Untergruppe. Nach Definition ist dann $|UP| \leq p^r$.
Andererseits ist $P \subseteq UP$ nach Lemma 6 und damit $|P| \leq |UP|$ nach Lemma 1.
Da $|P| = p^r$ folgt $p^r \leq |UP|$.
Insgesamt haben wir also $p^r \leq |UP|$ und $|UP| \leq p^r$, was nach Antisymmetrie $|UP| = p^r$ bedeutet.
Aus Lemma 2 folgt nun $UP = P$.
Nach Lemma 7 ist dann U Untergruppe von P, was zu zeigen war. □

Theorem 6. *Für alle p-Untergruppen U existiert ein $P \in Orb_\alpha(Q)$ mit $U \leq P$.*

Proof. Wähle P nach Lemma 24, d.h. $P \in \mathrm{Orb}_\alpha(Q)$ mit $|\mathrm{Orb}_\beta(P)| = 1$.
Die Aussage folgt mit Theorem 5.

□

3 Sylowsätze

Theorem 7. *Seien G eine endliche Gruppe und $p \in \mathbb{N}$ eine Primzahl. Seien $r, m \in \mathbb{N}$ sodass $|G| = p^r m$ und $p \nmid m$. Wir schreiben $Syl_p(G) = \{P \leq G \mid |P| = p^r\}$ für die Menge der p-Sylow-Untergruppen und $s_P(G) = |Syl_p(G)|$ für deren Anzahl.*

(a) Es gilt $Syl_p(G) \neq \emptyset$.

(b) Für alle p-Untergruppen U existiert ein $P \in Syl_p(G)$ mit $U \leq P$.

(c) Durch Konjugation operiert G transitiv auf $Syl_p(G)$.

(d) $s_p \mid m$

(e) $s_p \equiv 1 \mod p$.

Proof. (a) Das ist Theorem 3.

(b) Nach Theorem 6 existiert ein $P \in \mathrm{Orb}_\alpha(Q)$ mit $U \leq P$, und nach Lemma 19 ist die Konjugation eine Operation auf $\mathrm{Syl}_p(G)$, d.h. $P \in \mathrm{Syl}_p(G)$.

(c) Nach Lemma 19 ist Konjugation eine Operation auf $\mathrm{Syl}_p(G)$.

Sei $U \in \mathrm{Syl}_p(G)$ beliebig, dann existiert nach Theorem 6 ein $P \in \mathrm{Orb}_\alpha(Q)$ mit $U \leq P$.

Da $U \subseteq P$ und U, P Sylowgruppen sind, folgt nach Lemma 2 dass $U = P$.

Also existiert eine surjektive Abbildung von $\mathrm{Orb}_\alpha(Q)$ nach $\mathrm{Syl}_p(G)$, und mit $\mathrm{Orb}_\alpha(Q) \subseteq \mathrm{Syl}_p(G)$ folgt mittels Lemma 2 dass $\mathrm{Orb}_\alpha(Q) = \mathrm{Syl}_p(G)$, d.h. die Operation α ist transitiv.

(d) Nach c) ist $\mathrm{Orb}_\alpha(Q) = \mathrm{Syl}_p(G)$ und nach Theorem 4 gilt $|\mathrm{Orb}_\alpha(Q)| \mid m$.

(e) Nach c) und

$$s_p = |\mathrm{Orb}_\alpha(Q)| = \sum_{P \in R} |\mathrm{Orb}_\beta(P)|$$

Nun gilt $|\mathrm{Orb}_\beta(U)| = 1$ nach Lemma 17, also insbesondere $U \in R$.

Wir behaupten, dass $p \mid |\mathrm{Orb}_\beta(P)|$ für $P \in R \setminus \{U\}$ gilt.

Angenommen nicht, dann gilt $|\mathrm{Orb}_\beta(P)| = 1$ nach Lemma 23.

Aber dann folgt $U \leq P$ nach Theorem 5.

Da $U \subseteq P$ und U, P Sylowgruppen sind, folgt nach Lemma 2 dass $U = P$, Widerspruch zu $U \neq P$.

Damit folgt $p \mid \sum_{P \in R \setminus \{U\}} |\mathrm{Orb}_\beta(P)|$, also existiert ein k sodass

$$s_p = |\mathrm{Orb}_\beta(U)| + \sum_{P \in R \setminus \{U\}} |\mathrm{Orb}_\beta(P)| = 1 + p \cdot k.$$

Schließlich ist $s_p = 1 + p \cdot k \equiv 1 \mod p$, was zu zeigen war.

□