§ Gruppentheorie

Gruppenoperationen. Sei G eine Gruppe und M eine Menge. ein Monoidhom. $\varphi: G \to S(M) = \{f: M \to M \text{ bijektiv}\}$ definiert eine Gruppenoperation von G auf M, statt $\varphi(g)(m)$ schreiben wir oft $g \cdot m$

Beispiele 5.1 a) G operiert auf G durch links und rechtsmultiplikation:

$$l: G \to S(G) \; ; \; l(g)(h) = g \cdot h \quad , \quad r: G \to S(G) \; r(g)(h) = h \cdot g^{-1}$$

b) G operiert durch konjugation auf G:

$$C: G \to S(G) \; ; \; c(g)(h) = g \cdot h \cdot g^{-1}$$

c) für $H \leq G$ UG, so operiert G auf G/H durch linksmultpl:

$$G \to S(G/H) \; ; \; g \mapsto ([g'] \mapsto [gg'])$$

d) K Körper, $f \in K[X]$, L Zerfällungskörper von f, (siehe S.59 Bem) dann operiert $Gal(L/K)$ auf der Menge der Nullstellen von f.

Definition 5.2 Sei M eine Menge auf welcher G operiert.

1) für $m \in M$ ist die G-Bahn (oder der G-orbit) von m die Menge $\mathcal{O}_m = \{g \cdot m \mid g \in G\} \subseteq M$. Die Menge der G-Bahnen ist M/G

2) für $m \in M$ ist der Stabilisator von m die Untergruppe $G_m = \{g \in G \mid gm = m\} \leq G$ von G.

3) die Fixpunktmenge M^G der operation ist $M^G = \{m \in M \mid gm = m \; \forall g \in G\} = \{m \in M \mid G_m = G\}$

Lemma 5.3 Sei M eine Menge auf welcher G operiert. Dann gelten

1) $M = \dot{\bigcup}_{[m] \in M/G} \mathcal{O}_m$

2) G wirkt transitiv auf $M \Leftrightarrow \exists m \in M: \mathcal{O}_m = M \Leftrightarrow \forall m \in M \; \mathcal{O}_m = M$

3) G wirkt trivial auf $M \Leftrightarrow M^G = M$, $m \in M^G \Leftrightarrow \mathcal{O}_m = \{m\}$

Beweis: 1) offenbar gilt $M = \bigcup_{m \in M} \mathcal{O}_m$. genügt also zu sehen, dass $\mathcal{O}_m \cap \mathcal{O}_{m'} \neq \emptyset \Leftrightarrow \mathcal{O}_m = \mathcal{O}_{m'}$. ist $x \in \mathcal{O}_m \cap \mathcal{O}_{m'} \Rightarrow \exists g, g' \in G$

sodass $gm = x = g'm'$ und somit $g^{-1} \cdot g \cdot m = m'$ also $m' \in \mathcal{O}_m$ und somit $\mathcal{O}_{m'} \subseteq \mathcal{O}_m$. analog gilt $\mathcal{O}_m \subseteq \mathcal{O}_{m'}$.

2) und 3) sind Übungsaufgaben. ∎

Beispiele 5.4 a) operiert G durch links oder rechtsmultiplikation auf G
ist die Wirkung transitiv, die Fixpunktmenge ist leer falls $G \neq \{e\}$
ist $g \in G$ so ist der Stabilisator $G_g = \{e\} \subseteq G$

b) operiert G durch konjugation auf G, so ist die Wirkung nicht transitiv falls $G \neq e$ (die Bahn von e, $\mathcal{O}_e = \{e\}$).
die wirkung ist trivial $\Leftrightarrow$ G ist abelsch
für $g \in G$ ist der Stabilisator gegeben durch $\{h \in G : hgh^{-1} = g\} \subseteq$,
man nennt dies auch den Zentralisator von g in G ($Z_G(g)$)

c) G operiert transitiv auf G/H, der Stabilisator von $[e]$ ist H.

d) $f \in K[X]$, L Zerfällungskörper, $Gal(L/K)$ wirkt i.A. nicht transitiv auf den NS von f, doch aber falls f irreduzibel ist (siehe S.59 Bem)

Beispiel 5.5 Sei $G = GL_n(K)$, K ein Körper. Lasse G auf sich selbst durch Konjugation wirken. Für $A \in GL_n(K)$ ist $\mathcal{O}_A$ die Menge der zu A ähnlichen Matrizen, und G_A die Menge der mit A kommutierenden Matrizen.

Lemma 5.6 Sei G eine Gruppe welche auf einer Menge M operiere und $m \in M$ die Abbildung $G \to M$, $g \mapsto gm$, definiert eine Bijektion $G/G_m \xrightarrow{\cong} \mathcal{O}_m$
Insbesondere: $|\mathcal{O}_m| = [G : G_m]$ und

$$|M| = \sum_{[m] \in M/G} |\mathcal{O}_m| = \sum_{[m] \in M/G} [G : G_m]$$

Beweis: Per Konstruktion wirkt G transitiv auf $\mathcal{O}_m$ mit Stabilisator G_m es folgt, dass die Abbildung $G/G_m \to \mathcal{O}_m$ wohldefiniert, injektiv und surj. ist. der Rest folgt aus 5.3. ∎

Definition 5.7 Sei G eine Gruppe. Das ZENTRUM $Z(G)$ von G ist die Untergruppe $Z(G) = \{h \in G \mid \forall g \in G: gh = hg\}$.

Bem: a) $Z(G) = \bigcap_{g \in G} Z_G(g)$. $Z(G)$ ist abelsch und ein Normalteiler in G.

b) wirkt G per Konjugation auf G, so ist $Z(G)$ die Fixpunktmenge der Konjugationswirkung.

c) $g \in Z(G) \Leftrightarrow G_g^{conj} = G \Leftrightarrow O_g^{conj} = \{g\}$

aus 5.6 ergibt sich die Klassengleichung

$$|G| = |Z(G)| + \sum_{\substack{[g] \text{ s.d.} \\ |O_g^{conj}|>1}} |O_g^{conj}| \qquad (Z(G) = \{g \in G \mid |O_g^{conj}| = 1\})$$

$\leftsquigarrow = [G : G_g^{conj}]$

Definition 5.8 Sei G eine Gruppe. Wir nennen G eine p-Gruppe falls $|G| = p^n$ für ein $n > 0$, p prim.

Lemma 5.9 Sei G eine p-Gruppe welche auf einer Menge M operiert. Dann gilt $|M^G| \equiv |M| \mod p$.

Beweis: nach 5.3 gilt $M = \coprod_{[m] \in M/G} (O_m) = \coprod_{\substack{[m] \in M/G \\ \text{s.d. } |O_m|=1}} (O_m) \amalg \coprod_{\substack{[m] \in M/G \\ \text{s.d. } |O_m|>1}} (O_m)$

$$= M^G \amalg \coprod_{\substack{[m] \in M/G \\ |O_m|>1}} O_m$$

$$\Rightarrow |M| = |M^G| + \sum_{\substack{[m] \in M/G \\ |O_m|>1}} |O_m| = |M^G| + \sum_{\substack{[m] \in M/G \\ |O_m|>1}} [G : G_m] \equiv |M^G| \mod p.$$

$p \mid [G : G_m] > 1$ und Teiler von $|G|$ nach Lagrange

Korollare 5.10 1) Sei G eine p-Gruppe. Dann ist $Z(G) \neq \{e\}$.

2) Sei G eine Gruppe mit $|G| = p^2$, so ist G abelsch.

Beweis: 1) $|Z(G)| = |G^{conj;G}| \overset{5.9}{\equiv} 0 \mod p$. Wegen $e \in Z(G)$ folgt $|Z(G)| \geq p$

2) Angenommen, G ist nicht abelsch $\Rightarrow Z(G) \subsetneq G$.

nach 1) folgt $G/Z(G)$ eine Gruppe mit p Elementen, also zyklisch.

Daraus $|Z(G)| = p$ zyklisch. Sei $z \in Z(G)$ ein Erzeuger und $g \in G$

sodass $\bar{x}(g) \in G/Z(G)$ ein Erzeuger ist. Betrachte die von z und g aufgespannte UG von G. Diese ist abelsch, da $z \in Z(G)$ und hat Ordnung $> p$ ($g \notin Z(G)$ nach Annahme). $\Rightarrow G = \langle \{z, g\} \rangle$ und somit abelsch $\lightning$.

Korollar 5.11 p-Gruppen sind auflösbar.

Beweis: Induktion über $|G|$: ist $|G| = p$ oder p^2 so ist G abelsch $\Rightarrow$ auflösbar.
Im allgemeinen betrachte $Z(G) \leq G$, dies ist ein abelscher normalteiler und $G/Z(G)$ ist eine p-Gruppe mit $|G/Z(G)| < |G|$ wegen 5.10, daher auflösbar nach Induktion. Also G auflösbar nach 4.29. ∎

Bemerkung: p-Gruppen sind i.A. nicht abelsch, z.B werden wir später die Diedergruppen D_n betrachten ($|D_n| = 2n$) und D_4 ist nicht abelsch (von Ordnung $2^3 = 8$)

Definition 5.12 Sei G eine Gruppe $|G| = p^n \cdot m$, $p \nmid m$. Eine Sylow p-UG P von G ist eine p-UG maximaler Ordnung, also $|P| = p^n$.

Satz 5.13 (Sylow) Sei G eine Gruppe, $|G| = p^n \cdot m$, $p \nmid m$.

(1) $\forall\, 1 \leq s \leq n$ gibt es eine UG $U_s \leq G$ mit $|U_s| = p^s$. Insbesondere hat G eine Sylow-p-UG.

(2) Sei $U \leq G$ UG mit $|U| = p^s$ und $P \leq G$ eine Sylow p-UG. Dann existiert ges. g mit $gUg^{-1} \leq P$. Insbesondere sind je zwei Sylow p-UG konjugiert.

(3) Sei n_p die Anzahl der Sylow p-UG von G. Dann gelten
$$n_p \mid m \quad \text{und} \quad n_p \equiv 1 \bmod p.$$

Bemerkungen: A) Eine Konsequenz von 1) ist Cauchy's Satz: ist eine Primzahl p ein Teiler von $|G|$, so existiert ein UG von Ordnung p, und somit ein Element von Ordnung p.

B) Ist P eine Sylow p-UG von G, so ist P genau dann ein Normalteiler, falls $n_p = 1$.

Beweis 5.13 (1)+(2): Sei $1 \le s \le n$ wie in (1).

Sei $M = \{A \le G \mid |A| = p^s\}$. G operiert auf M durch Linksmultiplikation in G ($|gA| = |A| = p^s$). es folgt

$$|M| = \sum_{[A] \in M/G} |G_A| \text{, außerdem } |M| = \binom{p^n \cdot m}{p^s}.$$

Ann: $p^{n-s+1} \nmid \binom{p^n \cdot m}{p^s}$. Folglich existiert $A \in M$ sodass

$|G_A| \not\equiv 0 \mod p^{n-s+1}$. Sei G_A der Stabilisator von A, sodass $G_A \cong G/G_A$ und folglich $|G_A| = \frac{|G|}{|G_A|}$, Da p^{n-s} die größte p-Potenz ist, welche $|G_A|$ teilen kann folgt $|G_A| \ge p^s$ (da $p \nmid m$, $|G| = p^n \cdot m$)

nun beobachten wir, dass die Linksmultiplikationswirkung von G auf G zu einer Linksmultipl.wirkung von G_A auf $A \subseteq G$ einschränkt (per Definition von Stabilisatoren). Für jedes $a \in A$ gilt dann aber, dass die Abbildung $G_A \to A$, $g \mapsto ga$ injektiv ist. Daher gilt $|G_A| = p^s$ und G_A ist die gesuchte UG U_s.

(2) die UG U von G operiert per Linksmultiplikation auf G/P.

da U ein p-Gruppe ist, und G/P in Bahnen zerfällt (welche Kardinalität = Teiler von p haben) und $|G/P| = m$ mit $p \nmid m$ folgt, dass es $[g] \in G/P$ gibt, sodass U trivial auf $[g] = gP$ operiert. Für alle $u \in U$ gilt also, dass $ugP = gP$ und damit dass $g^{-1}ug \in P \Rightarrow g^{-1}Ug \le P$ ∎

Für den Beweis von Teil 3 des Sylow Satzes brauchen wir etwas mehr:

Definition 5.14 Sei $U \le G$ eine UG. Der NORMALISATOR $N_G(U)$ von U in G ist die größte UG von G, in welcher U ein Normalteiler ist; es gilt

$$N_G(U) = \{g \in G \mid gU = Ug\} \; ; \; U \trianglelefteq N_G(U).$$

Bem: G wirkt durch Konjugation auf der Menge $M = \{U \le G \mid U \text{ UG}\}$.

$N_G(U)$ ist der Stabilisator dieser G-wirkung von $U \in M$.

Lemma 5.15 G Gruppe, p primteiler von $|G|$, P eine Sylow-p-Gruppe. Es gelten:

a) ist $\pi: N_G(U) \to N_G(U)/U$ die projektion, $g \in N_G(U)$ sd. $\operatorname{ord}(\pi(g)) = p^k$

für ein $k \geq 0$, so ist $g \in P$ (das heißt $k=0$).

b) ist $g \in G$ mit $\text{ord}(g) = p^k$ und $gPg^{-1} = P \Rightarrow g \in P$.

Beweis: a) sei $|G| = p^n \cdot m$ mit $p \nmid m$. wir haben $P \leq N_G(P) \leq G$. es folgt, dass $|N_G(P)/P|$ ein Teiler von m ist da $p \nmid m$ folgt für $x \in N_G(P)/P$ mit $x^{p^k} = e$, dass $k=0$.

b) wegen $gPg^{-1} = P \Rightarrow g \in N_G(P)$ es folgt dass auch $\pi(g)$ Ordnung p^k hat und somit nach a), dass $g \in P$. ∎

Beweis von 5.13 (3): sei M die Menge der Sylow p-UG von G.

Nach 5.13 (2) wirkt G durch Konjugation auf M, und diese Wirkung ist transitiv, Stabilisator von P in M gegeben durch $N_G(P)$ (siehe Bem. nach 5.14). wir haben also $M \cong G/N_G(P)$ und, wie schon vorher beobachtet folgt, dass $|M| = \frac{|G|}{|N_G(P)|}$ ein Teiler von m ist ($|G| = p^n \cdot m$, $p \nmid m$).

Wir betrachten nun die Menge $M = \{ U \leq G \mid U = gPg^{-1} \text{ für ein } g \in G \}$ für eine fest gewählte Sylow p-UG P von G. P wirkt durch Konjugation auf dieser Menge. Der Stabilisator von $P \in M$ ist P. sei P' eine von P verschiedene Sylow-p-UG, sei $P' = gPg^{-1}$. ist $\overset{\text{alle}}{\underset{p \in P}{\forall}}$ $pgPg^{-1}p^{-1} = gPg^{-1}$, wende 5.15 auf $g \, p \in G$ und $P' \Rightarrow p \in P'$ daher $P \leq P'$ und somit $P = P'$ $\lightning$. also ist der Stabilisator $P_{P'}$ der P Wirkung on $P' \in M$ eine echte UG von P.

$$\Rightarrow M = \coprod_{[P' \in M/P]} \mathcal{O}_{P'} = \coprod_{[P' \in M/P]} P/P_{P'} = P/P \amalg \coprod_{\substack{[P' \in M/P] \\ P' \neq P}} P/P_{P'}$$

$$\Rightarrow |M| = 1 + \sum \underbrace{[P : P_{P'}]}_{>1 \text{ und Teiler von } |P| = p^n} \equiv 1 \mod p.$$ ∎

Wir geben zwei Anwendungen der Sylow-Sätze:

Beispiel 5.16 a) seien $p < q$ Primzahlen mit $p \nmid q-1$. Wir zeigen: ist G eine Gruppe mit $|G| = pq$, so ist $G \cong \mathbb{Z}/pq\mathbb{Z}$:

seien n_p und n_q die Anzahl der p- und q- Sylow UG. es gilt:

$n_q \in \{1,p\}$ und $n_q \equiv 1 \bmod q \overset{p<q}{\Rightarrow} n_q = 1$

$n_p \in \{1,q\}$ und $n_p \equiv 1 \bmod p \overset{p \nmid q-1}{\Rightarrow} n_p = 1$.

seien x und y erzeuger der Sylow-p-UG und der Sylow-q-UG. $P, Q \leq G$

Da $P \cap Q = \{e\}$ gilt $xyx^{-1}y^{-1} \in P \cap Q = \{e\}$ sodass x und y kommutieren.
$\in P$, da $P \trianglelefteq$

wir bekommen einen Gruppenhomom.

$$\mathbb{Z}/pq\mathbb{Z} \overset{\text{chin. Rest}}{\cong} \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \longrightarrow G, \quad (1,0) \mapsto x, \quad (0,1) \mapsto y.$$

Per Konstruktion ist $0 \times \mathbb{Z}/q\mathbb{Z} \to G \to G/P$ injektiv, da $\text{Bild}(\mathbb{Z}/q\mathbb{Z} \to G) = Q$ und $Q \cap P = \{e\}$. es folgt, dass $0 \times \mathbb{Z}/q\mathbb{Z} \to G \to G/P$ ein Isomorphismus ist.

UA: es folgt, dass $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \to G$ auch ein Isomorphismus ist.

b) sei G eine Gruppe mit $|G| = 30 = 2 \cdot 3 \cdot 5$. wir zeigen: es gibt einen Normalteiler $N \trianglelefteq G$ mit $N \cong \mathbb{Z}/15$ (Insbesondere: G ist auflösbar)

es genügt eine UG $U \subseteq G$ zu finden mit $|U| = 15$. Dann folgt mit a), dass $U \cong \mathbb{Z}/15$, und da $[G:U] = 2$ ist U automatisch normal.

sei P_3 eine Sylow 3-UG und P_5 eine Sylow 5-UG. Die Teilmenge $P_3 \cdot P_5 \subseteq G$ hat 15 Elemente, da $P_3 \cap P_5 = \{e\}$ (als UG von P_3 ist $|P_3 \cap P_5| \in \{1,3\}$, und als UG von P_5 ist $|P_3 \cap P_5| = \{1,5\}$). es folgt für $x, x' \in P_3$, $y, y' \in P_5$, dass $x \cdot y = x' \cdot y' \Leftrightarrow x = x'$ und $y = y'$. Ist P_3 oder P_5 ein Normalteiler, so ist $P_3 P_5$ eine UG von G (siehe Satz 1.14 1)).

aus dem Sylow-Satz folgt $n_3 \mid 10$ und $n_3 \equiv 1 \bmod 3 \Rightarrow n_3 \in \{1,10\}$ und $n_5 \mid 6$ und $n_5 \equiv 1 \bmod 5 \Rightarrow n_5 \in \{1,6\}$. Seien P, P' zwei q-Sylow UG von G mit $q \in \{3,5\}$. Dann gilt $P \cap P' = \{e\}$ oder $P = P'$ ($P \cap P'$ UG von P und $|P| = q$ prim)

~~angen~~ ~~außerdem~~ angenommen $n_3 = 10$ und $n_5 = 6$. Dann gibt es $6 \cdot 4$ nicht-triviale Elemente von Ordnung 5 (die $\neq e$ Elemente der 6 Sylow 5-UG) und $10 \cdot 2$ nicht-triviale Elemente von Ordnung 3. Da $6 \cdot 4 + 10 \cdot 2 = 44 > 30$ muss $n_3 \neq 10$ oder $n_5 \neq 6$, also $n_5 = 1$ oder $n_3 = 1$ gelten.

Klassifikation endlicher Gruppen (kleiner Ordnung).

Wir beginnen mit abelschen Gruppen (diese werden wir etwas allgemeiner im kommenden Semester klassifizieren, und halten die Diskussion hier daher kurz).

Definition 5.17 Sei A eine endliche abelsche Gruppe und p eine Primzahl. Wir setzen $A_{(p)} = \{a \in A \mid \mathrm{ord}(a) = p^{\alpha(a)} \text{ für ein } \alpha(a) \in \mathbb{N}\} \subseteq A$. und nennen $A_{(p)}$ den p-PRIMÄREN ANTEIL von A.

Bemerkung: 1) $A_{(p)} \subseteq A$ ist eine UG

2) $A_{(p)}$ ist eine p-Gruppe: sei q ein Primteiler von $|A_{(p)}|$. nach Cauchy's Satz (siehe Bem. A) nach 5.13) gibt es $a \in A_{(p)}$ mit $\mathrm{ord}(a) = q$. Da aber auch $\mathrm{ord}(a) = p^{\alpha(a)}$ folgt, dass $q = p$.

3) Die Konstruktion $A \mapsto A_{(p)}$ ist ein Spezialfall einer LOKALISIERUNG, wie wir sie im kommenden Semester studieren werden; die Lokalisierung von A an dem Primideal (p) von $\mathbb{Z}$ (dies ergibt Sinn, da A ein $\mathbb{Z}$-Modul ist)

Satz 5.18 1) Sei A eine endliche abelsche Gruppe. Dann ist die kanonische Abbildung

$$\bigoplus_{p \in P} A_{(p)} \to A \text{ ein Isomorphismus}$$

2) sei B eine endl. abelsche p-Gruppe, $|B| = p^k$. Dann existiert eine eindeutige Partition $k = l_1 + \dots + l_n$ mit $1 \le l_1 \le l_2 \le \dots \le l_n < k$ und ein Isomorphismus $\bigoplus_{i=1}^{n} \mathbb{Z}/p^{l_i}\mathbb{Z} \xrightarrow{\cong} B$

Bemerkung: Zusammen mit dem chinesischen Restsatz beschreibt Satz 5.18 alle endl. abelschen Gruppen. Zum Beispiel:

- $|A| = 4 \Rightarrow A \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ oder $A \cong \mathbb{Z}/4\mathbb{Z}$
- $|A| = 6 \to A \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$
- $|A| = 8 \Rightarrow A \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ oder $\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ oder $\cong \mathbb{Z}/8\mathbb{Z}$

Freie Gruppen und Präsentationen

Definition 5.19 Sei M eine Menge. Ein Paar $(F(M), i: M \to F(M))$ bestehend aus einer Gruppe $F(M)$ zusammen mit einer Abbildung i von M in die unterliegende Menge der Gruppe $F(M)$ heißt eine FREIE GRUPPE auf M, falls für alle Gruppen G, die von der Abbildung i induzierte Abbildung

$$\mathrm{Hom}_{\mathrm{Gruppen}}(F(M), G) \xrightarrow{i^*} \mathrm{Hom}_{\mathrm{Mengen}}(M, G)$$

eine Bijektion ist.

Lemma 5.20 Zu jeder Menge M existiert eine (eindeutig bis auf eindeutige Isomorphie bestimmte) freie Gruppe auf M.

Beweis: betrachte die Menge $\tilde{M} = \{ m^{\varepsilon} \mid m \in M, \varepsilon \in \{\pm 1\} \}$ bestehend aus Symbolen der Form m und m^{-1} für $m \in M$.

Betrachte dann die Menge aller Wörter aus der Menge $\tilde{M}$:

$$W(\tilde{M}) = \{ m_1^{\varepsilon_1} m_2^{\varepsilon_2} \cdots m_n^{\varepsilon_n} \mid n \geq 0, m_i^{\varepsilon_i} \in \tilde{M} \}$$ (für $n=0$ bekommt man das leere Wort $\emptyset$)

Definiere eine Äquivalenzrelation auf $W(\tilde{M})$ erzeugt von der Relation $x \cdot m \cdot m^{-1} \cdot y \sim x \cdot y$, $x,y \in W(\tilde{M})$, $m \in M$, wobei $\cdot$ für die Konkatenation von Wörtern steht. Dann induziert die Operation $(x,y) \mapsto x \cdot y$ eine wohldefinierte Gruppenstruktur auf $W(\tilde{M})/\sim$, der Menge der Äquivalenzklassen von $W(\tilde{M})$ mit $[\emptyset]$ als neutralem Element und $[m_1^{\varepsilon_1} \cdots m_n^{\varepsilon_n}]^{-1} = [m_n^{-\varepsilon_n} \cdots m_1^{-\varepsilon_1}]$. Diese Gruppe kommt mit einer Abbildung von M daher $(m \mapsto [m^1])$ und erfüllt offenbar die universelle Eigenschaft einer freien Gruppe. ∎

Notation: für $M = \{1, \dots, n\}$ schreibt man oft F_n statt $F(\{1, \dots, n\})$ und $i(k)$ wird oft mit x_k beschrieben.

Definition 5.21 Sei M eine Menge und $R \subseteq F(M)$ eine Teilmenge der freien Gruppe auf M. Sei $N(R) \trianglelefteq F(M)$ der von R erzeugte Normalteiler. Wir definieren eine Gruppe $\langle M \mid R \rangle$ als den Quotienten $F(M)/N(R)$.

$\langle M \mid R \rangle$ ist also eine Gruppe welche von den Elementen von M erzeugt werden, modulo den Relationen die durch R beschrieben sind.

Beispiele 5.22 a) $\langle x \mid \underbrace{x \cdot \ldots \cdot x}_{k\text{-mal}} \rangle \cong \mathbb{Z}/k\mathbb{Z}$, $\langle x \mid \phi \rangle \cong \mathbb{Z}$

b) $\langle x, y \mid xyx^{-1}y^{-1} \rangle \cong \mathbb{Z} \times \mathbb{Z}$

c) $\langle s_1, \ldots, s_{n-1} \mid s_i^2 , s_k s_\ell s_k^{-1} s_\ell^{-1} , s_a s_b s_a s_b^{-1} s_a^{-1} s_b^{-1} , \; a,b,k,\ell,i \in \{1,\ldots,n-1\}, |k-\ell| \geq 2, |a-b|=1 \rangle$

$\cong S_n$ (Übungsaufgabe) d) $\langle x, y \mid x^2 y^{-3}, x^3 y^{-5} \rangle \cong \{e\}$.

Definition 5.23 1) [Diedergruppen] für $n \geq 3$, setze

$$D_n = \langle x, y \mid x^2, y^2, (xy)^n \rangle \cong \langle z, a \mid z^n, a^2, (za)^2 = zaza^{-1} \rangle$$

2) [Quaternionengruppen] für $n \geq 2$, setze

$$Q_{4n} = \langle x, y \mid x^{2n}, x^n y^{-2}, yxy^{-1}x \rangle$$

Lemma 5.24 1) D_n ist isomorph zu der von $(1,2,\ldots,n) \in S_n$ und $\tau \in S_n$ gegeben durch $\tau(i) = \begin{cases} 1 & i=1 \\ n+2-i & i \geq 2 \end{cases}$ erzeugten Untergruppe.

2) D_n ist die Symmetriegruppe eines regelmäßigen n-Ecks in der Ebene (x, y sind benachbarte Spiegelungen)

3) D_n ist isomorph zu dem semidirekten Produkt $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ wobei $\mathbb{Z}/2\mathbb{Z}$ auf $\mathbb{Z}/n\mathbb{Z}$ durch Multiplikation mit (-1) operiert. Insbesondere gilt $|D_n| = 2n$.
(Multiplikation auf $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ ist $(x,\varepsilon) \bullet (x',\varepsilon') = (x + \varepsilon x', \varepsilon \cdot \varepsilon')$)

Beweis: Übungsaufgabe. §4

Lemma 5.25 Sei $U \subseteq GL_2(\mathbb{C})$ die von den Matrizen $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ und $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ erzeugte UG. Dann ist Q_8 isomorph zu U. $|Q_8| = 8$

[Q_8 ist eine Untergruppe von $\mathbb{H}^\times$]

Beweis: • $Q_8 \to U$, $x \mapsto A$, $y \mapsto B$ definiert einen Isomorphismus (nachrechnen)

• die Elemente von Q_8 sind $\{e, x, y, x^2, y^{-1}, x^3, xy, yx\}$. ∎

Satz 5.26 1) Sei $p>2$ prim, G Gruppe $|G|=2p$. Dann ist entweder $G \cong \mathbb{Z}/2p\mathbb{Z}$ (falls G abelsch) oder $G \cong D_p$ (falls G nicht abelsch)

2) Sei G nicht-abelsch, $|G|=8$. Dann ist $G \cong D_4$ oder $G \cong Q_8$.

Beweis: 1) nach 5.13 gilt $n_p = 1$ und $n_2 \in \{1, p\}$. Ist $n_2 = 1$, so folgt wie im Beispiel 5.16 a), dass $G \cong \mathbb{Z}/2p\mathbb{Z}$. Sei also $n_2 = p$. Sei P die (eindeutige) p-Sylow UG, $P \trianglelefteq G$. Wegen $|P| = p \Rightarrow P \cong \mathbb{Z}/p\mathbb{Z}$. und man hat $G/P \cong \mathbb{Z}/2\mathbb{Z}$. Jede Sylow-2 UG Q erfüllt, dass $Q \subseteq G \to G/P \cong \mathbb{Z}/2\mathbb{Z}$ ein Isomorphismus ist. es folgt (ÜA), dass G isomorph zu einem semidirekten Produkt $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ ist. es gibt aber nur 2 solche, wovon einer ($\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$) abelsch ist. Wegen $n_p \neq 1$ ist G nicht abelsch und daher isom. zu D_p nach 5.24 3).

2) Zunächst sehen wir, dass es ein $g \in G$ gibt mit $\mathrm{Ord}(g) = 4$. tatsächlich gilt $\mathrm{ord}(g) \in \{1, 2, 4, 8\}$, gäbe es g mit $\mathrm{ord}(g) = 8 \Rightarrow G \cong \mathbb{Z}/8\mathbb{Z}$ ($\not\!\!\lightning$ zu G nicht abelsch) und wäre $\forall g \in G$ $\mathrm{ord}(g) \neq 4$ so folgt dass $\forall g \in G$ $g^2 = e$ und somit wieder dass G abelsch wäre (vgl.). sei $H \cong \mathbb{Z}/4\mathbb{Z}$ die UG von G erzeugt von einem Element h der Ordnung 4. Dann gilt $[G:H] = 2$ also $H \trianglelefteq G$. Sei $g \in G \setminus H$. Dann ist G erzeugt von g und h. Wegen $ghg^{-1} \in H$ da H normal, und $\mathrm{ord}(ghg^{-1}) = \mathrm{ord}(h) = 4$ muss $ghg^{-1} \in \{h, h^{-1}\}$. ist $ghg^{-1} = h$ so wäre G abelsch (erzeugt von kommutierenden Erzeugern) also gilt $ghg^{-1} = h^{-1}$.

Da $G/H \cong \mathbb{Z}/2\mathbb{Z}$ folgt, dass $g^2 \in H$ und $\mathrm{ord}(g^2) \in \{1, 2\}$ (wäre $\mathrm{ord}(g^2) = 4$, so wäre $\mathrm{Ord}(g) = 8$, aber es gibt kein element der Ordnung 8 in G).

Ist $g^2 = e$ so erhalten wir die Präsentation $\langle h, g \mid h^4, g^2, hghg \rangle$ welches auch eine Präsentation von $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist (oder man vgl. direkt mit der definierenden Präsentation).

Ist $g^2 \neq e$, so ist $g^2 = h^2$ und wir erhalten die Präsentation $\langle h, g \mid h^4, h^{2-2}, ghg^{-1}h \rangle$ und somit $G \cong Q_8$. ($h \mapsto y$, $g \mapsto x$)

Für $|G| = n \leq 11$ ergeben sich folgende Klassifikationen für G bis auf Isomorphie

$n = 2$	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}$, $D_3 = S_3$
7	$\mathbb{Z}/7\mathbb{Z}$
8	$(\mathbb{Z}/2\mathbb{Z})^3$, $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, D_4 , Q_8
9	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$
10	$\mathbb{Z}/10\mathbb{Z}$, D_5
11	$\mathbb{Z}/11\mathbb{Z}$

Definition 5.27 Eine Gruppe G heißt einfach, falls $\{e\}$ und G die einzigen Normalteiler von G sind.

Bem: • einfache Gruppen sind auflösbar genau dann, wenn sie abelsch sind.
• abelsche Gruppen sind einfach, genau dann wenn ihre Ordnung prim ist.

Satz 5.28 Die Gruppe A_5 ist einfach. Insbesondere sind A_n und S_n für $n \geq 5$ nicht auflösbar.

Beweis: Wir betrachten die Konjugationswirkung von A_5 auf sich selbst.
Betrachte folgende Elemente von A_5 und deren Stabilisatoren

Element	Stabilisator
id	A_5
(12345)	$\mathbb{Z}/5\mathbb{Z}$ erzeugt von (12345)
$(12345)\circ(12345)$	$\mathbb{Z}/5\mathbb{Z}$ — " — $(12345)^2$
$(12)(34)$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ — " — $(12)(34)$ und $(13)(24)$
(123)	$\mathbb{Z}/3\mathbb{Z}$ — " — (123)

dies muss man natürlich genau nachrechnen, wir machen das hier aber nicht.

Die Bahnen-Zerlegung von A_5 in Konjugationsklassen ergibt dann

$A_5 = A_5/A_5 \amalg A_5/\mathbb{Z}/5\mathbb{Z} \amalg A_5/\mathbb{Z}/3\mathbb{Z} \amalg A_5/\mathbb{Z}/2\mathbb{Z}\mathbb{Z}/2\mathbb{Z} \amalg A_5/\mathbb{Z}/3\mathbb{Z}$

$|A_5| = 1 + 12 + 12 + 15 + 20$

sei nun $N \trianglelefteq A_5$ ein Normalteiler. Jedes Element von N lebt in einer der obigen Konjugationsklassen, und da N normal ist lebt die entsprechende Konjugationsklasse ganz in N, außerdem $e \in N$.

Daher ist $|N| = 1 + a \cdot 12 + b \cdot 12 + c \cdot 15 + d \cdot 20$ mit $a,b,c,d \in \{0,1\}$

auf der anderen Seite ist $|N|$ ein Teiler von $|A_5| = 60$.

das heißt $|N| \in \{1,2,3,4,5,10,12,15,20,30,60\}$

die einzigen Möglichkeiten hierfür sind $|N| = 1$ oder $|N| = 60$, daher ist A_5 einfach.

Bemerkung 1) A_5 ist eine nicht-abelsche einfache Gruppe minimaler Ordnung. Tatsächlich sagt ein Satz von Burnside (hier unbewiesen) dass $|G|$ mindestens 3 verschiedene Primteiler haben muss, damit G nicht auflösbar sein kann. Für $|G| < 60$ ergeben sich damit nur $|G| = 2 \cdot 3 \cdot 5$ und $|G| = 2 \cdot 3 \cdot 7$. Im ersten Fall haben wir in Bsp. 5.16 b) gesehen, dass G einen nicht-trivialen Normalteiler hat. Im zweiten Fall gilt $n_7 \in \{1,2,3,6\}$ und $n_7 \equiv 1 \bmod 7$ nach dem 3. Sylow Satz, daher $n_7 = 1$ und somit existiert wieder ein nicht-triv. Normalteiler.

2) Tatsächlich ist A_n für $n \geq 5$ einfach. Es gibt noch mehr solche "Familien" einfacher endlicher Gruppen, z.B.: K endl. Körper, $n > 2$

so ist $SL_n(K)/Z(SL_n(K))$ einfach.

es gibt noch weitere "sporadische" einfache Gruppen, deren Konstruktion kein simples Muster erkennen lassen. Die kleinste sporadische Gruppe hat 7920 Elemente, die größte (die sogenannte Monstergruppe) hat Ordnung

$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$

Polynome mit Galoisgruppe S_n (nicht vollständig bewiesen)

Wir werden folgenden Satz benutzen:

Satz 5.29 Sei p eine Primzahl, $f \in \mathbb{Z}[X]$ primitiv, $\bar{f} \in \mathbb{F}_p[X]$ die Reduktion mod p. Sei $\mathrm{Gal}(f) = \mathrm{Gal}(L(f)/\mathbb{Q})$, $\mathrm{Gal}(\bar{f}) = \mathrm{Gal}(L(\bar{f})/\mathbb{F}_p)$. Ist $\bar{f}$ separabel, so ist auch f separabel, ist $\mathrm{grad}(f) = n$, und fassen wir $\mathrm{Gal}(f)$, $\mathrm{Gal}(\bar{f})$ als Untergruppen von S_n auf, so gilt $\mathrm{Gal}(\bar{f}) \subseteq \mathrm{Gal}(f)$.

Der Beweis benötigt Begriffe wie integrale Ringerweiterungen, und Liftungssätze von Primidealen entlang solcher Erweiterungen – dies wird üblicherweise in der Vorlesung "Komm. Algebra" gemacht.

Lemma 5.30 $\forall n \geq 1$ existiert ein irreduzibles Polynom $f \in \mathbb{F}_p[X]$ mit $\mathrm{grad}(f) = n$.

Beweis: Betrachte $\mathbb{F}_{p^n}/\mathbb{F}_p$. Da $\mathbb{F}_p$ perfekt ist dies eine separable, endl. Erweiterung vom Grad n. Nach dem Satz vom primitiven Element gibt es $a \in \mathbb{F}_{p^n}$ sodass $\mathbb{F}_{p^n} = \mathbb{F}_p(a)$. Das Minimalpolynom von a erfüllt alles was wir behaupten. ☑

Lemma 5.31 Sei $f \in \mathbb{Z}[X]$ primitiv, $g_1 \cdot \ldots \cdot g_r = \bar{f} \in \mathbb{F}_p[X]$, $\bar{f}$ separabel, $\mathrm{grad}(\bar{f}) = n$, g_i irreduzibel in $\mathbb{F}_p[X]$, p prim. Sei $d_i = \mathrm{grad}(g_i)$. Dann enthält $\mathrm{Gal}(f)$ Zykel der Länge d_i, $i = 1, \ldots, r$.

Beweis: $\mathrm{Gal}(\bar{f}) \subseteq \mathrm{Gal}(f)$ (5.29); außerdem ist $\mathrm{Gal}(\bar{f})$ zyklisch (jede endl. Erw. eines endl. Körpers ist zyklisch). Die NS von $\bar{f}$ zerlegt sich unter der $\mathrm{Gal}(\bar{f})$-Wirkung in die disjunkte Vereinigung der NS aller g_i und diese sind von der Form $\mathrm{Gal}(\bar{f})/\mathrm{Gal}(L(\bar{f})/L(g_i))$ (als $\mathrm{Gal}(\bar{f})$-Menge) mit anderen Worten: die Wirkung von $\mathrm{Gal}(\bar{f})$ auf $\{$Nullstellen von $\bar{f}\}$ faktorisiert durch den Homomorphismus $S_{d_1} \times \ldots \times S_{d_r} \subseteq S_{d_1 + \ldots + d_r} = S_n$, wobei der induz. Hom. $\mathrm{Gal}(\bar{f}) \to S_{d_i}$ gegeben ist durch $\mathrm{Gal}(\bar{f}) \twoheadrightarrow \mathrm{Gal}(g_i)$ ($L(\bar{f}) \supseteq L(g) \supseteq \mathbb{F}_p$) und die kan. Inklusion $\mathrm{Gal}(g_i) \subseteq S_{d_i}$.

Wir haben gesehen, dass $\mathrm{Gal}(g_i) = \mathbb{Z}/d_i\mathbb{Z} \subseteq S_{d_i}$, erzeugt von einem d_i-Zykel (Frobenius). ☑

Satz 5.32 Für jedes $n \geq 2$ existiert $f \in \mathbb{Q}[X]$ irreduzibel mit $\mathrm{Gal}(f) \cong S_n$.

Beweis: wir wählen wie folgt Polynome aus $\mathbb{Z}[X]$ vom grad n.

- f_1 sodass $\bar{f}_1 \in \mathbb{F}_2[X]$ faktorisiert als $\bar{f}_1 = g \cdot h$, (g irreduzibel vom grad $n-1$ (solche existieren nach 5.30). f_1 kann primitiv gewählt werden.
- f_2 sodass $\bar{f}_2 \in \mathbb{F}_3[X]$ faktorisiert als $\bar{f}_2 = s \cdot t$, s irreduzibel $\mathrm{grad}(s)=2$ t produkt von $n-2$ Linearfaktoren. f_2 kann auch primitiv gewählt werden

~~g, h, s, t~~ (g, h, s, t können normiert gewählt werden)

Betrachte dann $f = 3f_1 - 2f_2 + 6f_3 \in \mathbb{Z}[X]$. , $f_3 \in \mathbb{Z}[X]$ $\mathrm{grad}(f_3) = n-1$

Dann ist f primitiv und kongruent f_1 mod 2 und kongruent f_2 mod 3; primitiv denn betrachte Koeff. von X^n modulo p für p prim beliebig wähle nun f_3 so, dass alle Koeff. von X^i, $0 \leq i \leq n-1$ durch 5 teilbar sind, und der konst. Term nicht durch 25 teilbar ist. Dann ist f irreduzibel nach Eisenstein, und normiert, $\mathrm{Gal}(f)$ operiert daher transitiv auf den Nullstellen von f in $L(f)$ – einem Zerfällungskörper von f. (siehe Bem. 5.59 2)). Nach 5.31 enthält $\mathrm{Gal}(f) \leq S_n$ einen $(n-1)$-Zykel ($p=2$) und eine Transposition ($p=3$). Untergruppen von S_n welche einen $n-1$ Zykel und eine Transposition enthalten sind aber ganz S_n (ÜA). ∎

Bemerkung: Ein anderer Beweis geht (wieder ohne Details) wie folgt:

1) Betrachte für k ein beliebigen Körper den Körper $k(T_1, \dots, T_n) = \mathbb{Q}(k[T_1, \dots, T_n])$
   Betrachte $f = X^n + T_1 X^{n-1} + \dots + T_{n-1} X + T_n \in K[X]$
   man zeigt: f ist separabel, irreduzibel und $\mathrm{Gal}(f) = S_n$
2) für $k = \mathbb{Q}$ zeigt man, dass es elemente $a_1, \dots, a_n \in \mathbb{Q}$ gibt sodass das Bild $\bar{f}$ von f unter $\mathbb{Q}[T_1, \dots, T_n) \xrightarrow{T_i \mapsto a_i} \mathbb{Q}$ wieder irreduzibel (und separabel) ist.
   und $\mathrm{Gal}(\bar{f}) = S_n$