§2 Gruppen wirken

Viele Gruppen tauchen in der Mathematik als "Symmetriegruppen" auf. Zum Beispiel ist $GL_n\mathbb{R}$ die Gruppe aller Permutation von $\mathbb{R}^n$, die die Vektorraumstruktur von $\mathbb{R}^n$ respektieren. Um solche Gruppen geht es in diesem Kapitel.

1. Theorem (Satz von Cayley)
Jede Gruppe G ist isomorph zu einer Untergruppe einer (geeigneten) Symmetrischen Gruppe $\mathrm{Sym}(X)$.

Beweis Wir setzen $G = X$ als Menge. Für jedes $g \in G$ betrachten wir die Abbildung

$$\lambda_g : G \to G, \quad x \longmapsto gx$$

Dann gilt: $\lambda_a \circ \lambda_b (x) = abx = \lambda_{ab}(x)$

insbesondere $\lambda_a \circ \lambda_{a^{-1}}(x) = x$, d.h. jedes λ_a ist eine Permutation der Menge $X = G$.

Die Abbildung $G \to \mathrm{Sym}(X)$

$$g \longmapsto \lambda_g$$

ist ein Homomorphismus, denn $\lambda_a \circ \lambda_b = \lambda_{ab}$.

Dieser Homomorphismus ist injektiv:

$\lambda_a = id_G \Leftrightarrow ax = x$ für alle $x \in G$

$\Rightarrow ae = e \Rightarrow a = e$, siehe §1.23.

Wir setzen $H = \{\lambda_g \mid g \in G\} \leq Sym(X)$. Dann ist die Abbildung $\lambda: G \to H$, $g \mapsto \lambda_g$ bijektiv, also ein Gruppenisomorphismus. □

Also $G \cong H \subseteq Sym(X)$.

2. Gruppenwirkungen ("Gruppenaktionen")

1. Zugang. Sei G eine Gruppe, $X \neq \emptyset$ eine Menge, sei $\varphi: G \to Sym(X)$ ein Homomorphismus.

φ ordnet also jedem Gruppenelement $g \in G$ eine Permutation $\varphi(g): X \to X$ zu. (im Bsp oben $\varphi(g) = \lambda_g$)

Wir schreiben kurz $\varphi(g)(u) = gu$ für $g \in G$, $u \in X$

Warnung! Die rechte Seite hängt von φ ab, das ist in dieser Notation nicht sichtbar.

Da φ ein Homomorphismus ist, gilt folgendes:

$\varphi(e)(u) = id_X(u) = u \Rightarrow eu = u$ für alle $u \in X$

$\varphi(ab)(u) = \varphi(a)(\varphi(b)(u)) \Rightarrow (ab)u = a(bu)$ für alle $a, b \in G$, $u \in G$

Insbesondere folgt

$a^{-1}(au) = (a^{-1}a)u = u$ für alle $a \in G$, $u \in X$.

2. Zugang Eine Wirkung von G auf X ist eine Abbildung $G \times X \to X$, $(g, u) \mapsto gu$ mit folgenden Eigenschaften:

(W1) $eu = u$ für alle $u \in X$ (e Neutralelement in G)

(W2) $(ab)u = a(bu)$ für alle $a, b \in G$, $u \in X$

Wir haben oben gesehen: jeder Homomorphismus $\varphi: G \to \mathrm{Sym}(X)$ gibt uns eine Wirkung.

Das gilt aber auch umgekehrt. Wenn $G \times X \to X$ eine Wirkung ist, so definieren wir für $g \in G$ die Abbildung $\varphi(g): X \to X$, $u \mapsto gu$

Wegen $\varphi(g) \circ \varphi(g^{-1}) = id_X = \varphi(g^{-1}) \circ \varphi(g)$ folgt:

$\varphi(g)$ ist bijektiv, also $\varphi(g) \in \mathrm{Sym}(X)$ und

$\varphi(ab) = \varphi(a)\varphi(b) \Rightarrow \varphi: G \to \mathrm{Sym}(X)$ ist ein Homomorphismus wie im 1. Zugang.

Also sind Zugang 1 und Zugang 2 gleich wertig, wir werden hier Blickwinkel benutzen.

3. Def (Stabilisatoren, Bahnen, Kern)

Sei $G \times X \to X$ eine Wirkung wie oben.

Für $u \in X$ definieren wir den Stabilisator von u

als $G_u = \{ g \in G \mid gu = g \}$ alle g, die u fest lassen;

also $G_u \subseteq G$.

Die Bahn (oder der Orbit) von $u \in X$ ist

$G(u) = \{ gu \mid g \in G \} \subseteq X$ alle $v \in X$, in denen sich u bewegen lässt.

Der Kern der Wirkung ist $\bigcap_{u \in X} G_u = \{ g \in G \mid gu = u \text{ für alle } u \in X \}$

Lemma A Stabilisatoren sind stets Untergruppen.

Beweis Sei $u \in X$, sei $a, b \in G_u$.

Dann gilt: $e \in G_u \Rightarrow G_u \neq \emptyset$

$(ab)u = a(bu) = au = u \Rightarrow ab \in G_u$

$a^{-1}u = a^{-1}(au) = eu = u \Rightarrow a^{-1} \in G_u$ □

Lemma B Sei $v \in G(u)$. Dann ist $G(v) = G(u)$.

Folgerung: Bahnen sind entweder gleich oder disjunkt.

Beweis $v \in G(u) \Rightarrow v = gu$ für ein $g \in G$.

Dann ist $G(v) = \{ \tilde{g} v \mid \tilde{g} \in G \} = \{ \tilde{g} g u \mid \tilde{g} \in G \}$

$= G(u)$

Sind also $G(u)$, $G(w)$ beide Bahn mit

$v \in G(u) \cap G(w)$, so folgt $\left.\begin{matrix} G(v) = G(u) \\ G(v) = G(w) \end{matrix}\right] \Rightarrow G(u) = G(w)$ □

Lemma C Der Kern der Wirkung ist ein Normalteiler in G.

Beweis Sei $\varphi: G \to Sym(X)$ der zur Wirkung gehörige Homomorphismus. Dann gilt: $g \in G$ liegt im Kern der Wirkung $\Leftrightarrow \varphi(g) = id_X \Leftrightarrow g \in ker(\varphi)$, also ist $ker(\varphi)$ genau der Kern der Wirkung und damit ein Normalteiler. #

Lemma D Für jedes $u \in X$ erhält man eine bijektive Abbildung

$$G/G_u \longrightarrow G(u)$$
$$gG_u \longmapsto gu$$

Beweis (a) Die Abbildung ist wohldefiniert.

Ist $gG_u = \tilde{g}G_u$, so $\tilde{g} = gh$ für ein $h \in G_u$.

Dann ist $\tilde{g}u = ghu = gu$. □

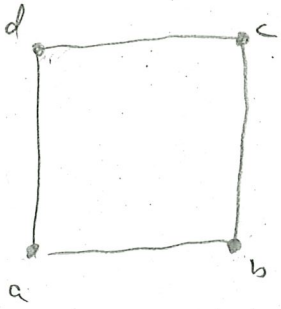
(b) Die Abbildung ist surjektiv. (klar) □

(c) Die Abbildung ist injektiv.

Angenom., $gu = \tilde{g}u$. Dann ist $g^{-1}\tilde{g}u = u$

$\Rightarrow h = g^{-1}\tilde{g} \in G_u \Rightarrow \tilde{g} = gh \Rightarrow \tilde{g}G_u = gG_u$ □

4. Beispiel Die Symmetrien eines Quadrates.



Informell Welche Symmetrie sehen wir?

Rotation um $0°, 90°, 180°, 270°$
$\varepsilon \quad \alpha \quad \alpha^2 \quad \alpha^3$

Spiegelungen

insgesamt 8 Symmetrien (?)

Sei G die Gruppe aller Symmetrien.

Der Stabilisator von a ist $\langle\delta\rangle = \{e, \delta\}$
(wenn a fest bleibt, dann auch c und dann können nur noch b und d vertauscht werden).

Die Bahn von a ist $G(a) = \{a, b, c, d\}$ (angenommen $\alpha, \alpha^2, \alpha^3$). Weg $|G(a)| = 4 = [G : G_a]$ und $|G_a| = 2$ folgt $|G| = 8$, wie vermutet.

Wieviele Erzeuger braucht man für G mindestens?

Beobachtung: G ist nicht abelsch, $\alpha\beta\alpha^{-1} = \gamma \neq \beta$, also nicht zyklisch $\Rightarrow$ wir brauchen mindestens 2 Erzeuger.

$|\langle\alpha\rangle| = 4$ und $\beta \notin \langle\alpha\rangle$, also ist das Erzeugnis $\langle\{\alpha, \beta\}\rangle = H \subseteq G$ mit $|H| > 4$. Nach Lagrange ist $|H|$ ein Teiler von $|G| = 8 \Rightarrow H = G$.

Es gibt auch andere Erzeug. Etwa:

$\beta \circ \delta = \alpha \rightsquigarrow \langle \{\beta, \delta\} \rangle = G$, denn $\langle \{\beta, \alpha\} \rangle = G$.

Also wird G von 2 Spiegelungen erzeugt.

Übung

Bem $[G : \langle \alpha \rangle] = 2 \Rightarrow \langle \alpha \rangle \trianglelefteq G$

5. Die Bahnengleichung

Def Gegeben sei eine Gruppenwirkung $G \times X \to X$.

Eine Teilmenge $S \subseteq X$ heißt Schnitt (oder Transversale), wenn S genau ein Element aus jeder Bahn enthält. Schnitte existieren immer; wähle aus jeder Bahn $G(x) \subseteq X$ ein Element aus. (Wenn es unendlich viele Bahnen gibt, braucht man dafür das Auswahlaxiom.)

Satz (Die Bahnengleichung) Sei $G \times X \to X$ eine Gruppenwirkung. Wenn die Menge X endlich ist, dann gilt

$$|X| = \sum_{s \in S} [G : G_s]$$

wobei $S \subseteq X$ irgendein Transversale ist.

Beweis: Es gilt $X = \bigcup_{s \in S} G(s)$ und für $s,t \in S$ mit $s \neq t$ ist $G(s) \cap G(t) = \emptyset$. Damit folgt

$$|X| = \sum_{s \in S} |G(s)| = \sum_{s \in S} |G/G_s| = \sum_{s \in S} [G : G_s]$$

(↑ §2.3 Lemma 3) □

6. Automorphismen und Konjugation

Sei G eine Gruppe. Wir setzen

$$\mathrm{Aut}(G) = \{\varphi : G \to G \mid \varphi \text{ ist Isomorphismus}\}$$

Automorphismengruppe von G. Die Elemente von $\mathrm{Aut}(G)$ heißen Automorphismen von G.

Explizit: $\varphi : G \to G$ Automorphismus $\Leftrightarrow$ φ ist ein Homomorphismus und bijektiv (vgl §1.25)

Klar: $\psi, \varphi \in \mathrm{Aut}(G) \Rightarrow \psi \circ \varphi \in \mathrm{Aut}(G)$, $\mathrm{id}_G \in \mathrm{Aut}(G)$ und $\varphi^{-1} \in \mathrm{Aut}(G)$ (↑ Umkehrabbildung)

Folglich ist $\mathrm{Aut}(G)$ eine Gruppe bzgl. Komposition von Abbildungen.

7. Beispiel Sei $a \in G$. Wir definieren eine Abbildung

$\gamma_a : G \to G$, $g \mapsto aga^{-1}$, die Konjugationsabbildung, Konjugieren mit a.

Für $a, b \in G$ gilt $\gamma_a \circ \gamma_b (g) = \gamma_a(bgb^{-1}) = abgb^{-1}a^{-1}$

$\overset{!}{=} (ab)g(ab)^{-1} = \gamma_{ab}(g)$, sowie $\gamma_{a^{-1}} = (\gamma_a)^{-1}$.

Damit erhalten wir einen Homomorphismus

$$\gamma : G \to Aut(G), \quad a \mapsto \gamma_a$$

Das ist insbesondere eine Wirkung von G auf G, die Konjugationswirkung

$$G \times G \to G \qquad (a, g) \mapsto aga^{-1}$$

Was ist der Kern dieser Wirkung?

$$\gamma_a(g) = g \iff ag = ga$$

damit ist $kr(\gamma) = \{ a \in G \mid \text{Für alle } g \in G \text{ gilt } ag = ga \}$

Man nennt das das Zentrum der Gruppe G,

$$Cen(G) = \{ a \in G \mid \text{Für alle } g \in G \text{ ist } ag = ga \}$$

Also G abelsch $\Leftrightarrow$ $Cen(G) = G$.

Bsp $Cen(Sym(3)) = \{id\}$, vgl §1.4.

8. Die Konjugationswirkung. Wir betrachten mit der Konjugationswirkung $\gamma: G \to Aut(G)$ von G auf sich, $G \times G \to G$, $(a,g) \mapsto aga^{-1}$

Der Stabilisator von $g \in G$ ist die Gruppe

$Cen_G(g) = \{a \in G \mid ag = ga\}$, man nennt das den Zentralisator von g. Es gilt stets $g \in Cen_G(g)$.
$\Rightarrow \langle g \rangle \subseteq Cen_G(g)$

Bsp in $Sym(3)$ $\alpha: \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{cases}$

$\alpha\rho \neq \rho\alpha$ $\alpha\tau \neq \tau\alpha$, usw $\Rightarrow$ $Cen_\alpha(Sym(3)) = \langle \alpha \rangle$

Bsp $g \in Cen(G) \Leftrightarrow Cen_G(g) = G$

Die Bahn von g ist die Menge

$C_G(g) = \{aga^{-1} \mid a \in G\} \subseteq G$, die

Konjugiertenklasse von g.

Das ist im allgemeinen keine Untergruppe, sondern nur ein Teilmenge von G. #

Bsp $\alpha \in Sym(3)$ vgl. §1.4

$\beta \alpha \beta^{-1} = \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \end{cases} = \gamma$, $\quad \gamma \alpha \gamma^{-1} = \beta$

$\delta \alpha \delta^{-1} = \delta \alpha \varepsilon = \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \end{cases} = \gamma$ etc. $\Rightarrow$

$C_{Sym(3)}(\alpha) = \{\alpha, \beta, \delta\}$

Das Bild von G in $Aut(G)$ heißt die Gruppe der innereren Automorphismen

$$Inn(G) = \{\tau_a \mid a \in G\} \subseteq Aut(G)$$

9. Satz (Die Klassengleichung)

Sei G eine endliche Gruppe, sei $S \subseteq G$ ein Schnitt der Konjugationsäquivalenz. Das bedeutet: S enthält aus jeder Konjugiertenklasse in G genau ein Element. Weiter sei $\mathcal{K} = S - Zen(G)$, Das sind also die Elemente $s \in S$ mit $Cen_G(s) \neq \{G\}$ (d.h.: $C_G(s) \neq \{s\}$). Dann gilt die Klassengleichung

$$|G| = |Cen(G)| + \sum_{s \in \mathcal{K}} [G : Cen_G(s)]$$

Beweis: Nach der Bahnformel ist

$$|G| = \sum_{s \in S} [G : \mathrm{Cen}_G(s)] = \sum_{s \in \mathrm{Cen}(G)} [G : \mathrm{Cen}_G(s)] + \sum_{s \in K} [G : \mathrm{Cen}_G(s)]$$

denn $\mathrm{Cen}(G) \subseteq S$. Aber für $s \in \mathrm{Cen}(G)$ ist

$\mathrm{Cen}_G(s) = G \Rightarrow [G : \mathrm{Cen}_G(s)] = [G : G] = 1$, also

$$|G| = |\mathrm{Cen}(G)| + \sum_{s \in K} [G : \mathrm{Cen}_G(s)]. \qquad \square$$

10. Korollar: Sei p eine Primzahl und sei G eine Gruppe mit $|G| = p^m$ für ein $m \geq 1$.

Dann ist $\mathrm{Cen}(G) \neq \{e\}$.

Vgl. mit §1.16, Korollar B: $|G| = p \Rightarrow G$ abelsch.

Beweis: Angenommen $g \in G$, $g \notin \mathrm{Cen}(G)$.
(sonst ist nichts zu zeigen)
Dann ist $\mathrm{Cen}_G(g) \neq G$. Mit dem Satz von Lagrange folgt $|\mathrm{Cen}_G(g)| = p^l$ mit $0 \leq l < m$.
und $[G : \mathrm{Cen}_G(g)] = p^{m-l} > 1$. Damit ist
p ein Teiler von $\sum_{s \in K} [G : \mathrm{Cen}_G(s)]$, also
auch ein Teiler von $|\mathrm{Cen}(G)| \Rightarrow |\mathrm{Cen}(G)| \neq \{e\}$

$\square$

11. Def Sei p eine Primzahl. Eine endliche Gruppe G heißt p-Gruppe, falls gilt

$|G| = p^m$ für ein $m \geq 1$.

Korollar §2.10 sagt also: jede p-Gruppe G hat ein Zentrum $Cen(G) \neq \{e\}$.

12. Beispiel Um interessante p-Gruppen zu sehen, kommt wir endliche Körper.

Konstruktion Sei $m \in \mathbb{N}$, $m \geq 2$ fest gewählt.

Wir wissen schon: $\mathbb{Z}/m\mathbb{Z}$ ist eine zyklische Gruppe der Ordnung m, mit Addition

$$(k + m\mathbb{Z}) + (l + m\mathbb{Z}) = k + l + m\mathbb{Z}$$

vgl. §1.18. Wir können $m\mathbb{Z}$-Nebenklassen addieren und erhalten eine Gruppe (mit Addition).

Hier können wir Nebenklassen aber auch multiplizieren.

Denn $(k + ma) \cdot (l + mb) = k \cdot l + \underbrace{m(al + kb + mab)}_{\in m\mathbb{Z}}$

Wir definieren also $(k + m\mathbb{Z}) \cdot (l + m\mathbb{Z}) = kl + m\mathbb{Z}$.

Die Rechtfertigung ist: diese Multiplikation ist wohldefiniert.

Multiplikation ist auch assoziativ, kommutativ und die Distributivgesetze gelten. Wenn wir die Kurzschreibweise (*) $\overline{k} = k + m\mathbb{Z}$ einführen, dann gilt:

$$\overline{k} + \overline{l} = \overline{k+l} \quad \rightsquigarrow \text{Gruppe}$$

$$\overline{k} \cdot \overline{l} = \overline{k \cdot l} = \overline{lk} = \overline{l}\,\overline{k}$$

sowie $(\overline{k} + \overline{l})\,\overline{u} = \overline{k+l} \cdot \overline{u} = \overline{ku + lu} = \overline{k}\,\overline{u} + \overline{l}\,\overline{u}$ usw.

$$\overline{1} \cdot \overline{k} = \overline{k}$$

Fazit: $\mathbb{Z}/m\mathbb{Z}$ wird mit den Verknüpfungen + und · ein kommutativer Ring.

Erinnerung: $(R, +, \cdot)$ ist ein kommutativer Ring, wenn gilt: (R1) $(R, +)$ ist abelsche Gruppe, mit einem Neutralelement $0 \in R$

(R2) Die Multiplikation · ist assoziativ, kommutativ und distributiv [$(a \cdot v) \cdot w = u \cdot (v \cdot w)$, $u \cdot v = v \cdot u$, $u \cdot (v+w) = uv + uw$, $(v+w)u = vu + wu$]

(R3) Die Multiplikation hat ein Neutralelement $1 \in R$, d.h. $1 \cdot u = u \cdot 1 = u$ gilt für alle $u \in R$

Bsp $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$ sind kommutative Ringe.
$(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ist auch ein kommutativer Ring.

(*) Wenn man eine Kurzschreibweise benutzt, muss man klar dazu sagen, welches m gerade gemeint ist !!!

Def Ein **Körper** $(K,+,\cdot)$ ist ein kommutativer Ring mit folgender Zusatzeigenschaft:

(i) $0 \neq 1$

(ii) Für jedes $u \neq 0$ gibt es v mit $u \cdot v = 1$.

Bsp $\mathbb{R}, \mathbb{Q}$ sind Körper

$\mathbb{Z}$ ist kein Körper, es gibt kein $v \in \mathbb{Z}$ mit $2 \cdot v = 1$.

13. **Satz** Der kommutative Ring $\mathbb{Z}/m\mathbb{Z}$, mit $m \geq 2$, ist genau dann ein Körper, wenn m eine Primzahl ist.

Beweis Es gilt $\bar{0} \neq \bar{1}$, denn $1 \notin m\mathbb{Z}$ (weil $m \geq 2$).

Angenommen, m ist keine Primzahl. Dann ist $m = k \cdot l$, $k, l \geq 2$. Es folgt $\bar{k} \cdot \bar{l} = \bar{m} = \bar{0}$ und $\bar{k}, \bar{l} \neq \bar{0}$ (weil $2 \leq k, l < m$ ist $k, l \notin m\mathbb{Z}$)

Wäre $\bar{u} \cdot \bar{k} = \bar{1}$, so wäre $\bar{u}\,\underbrace{\bar{k} \cdot \bar{l}}_{=\bar{0}} = \bar{1} \cdot \bar{l} = \bar{l} \neq \bar{0}$ ↯

$\Rightarrow \mathbb{Z}/m\mathbb{Z}$ ist kein Körper.

Angenommen, m ist eine Primzahl. Sei $\bar{u} \neq \bar{0}$

Beh Für $\bar{v} \neq \bar{0}$ ist dann $\bar{u} \cdot \bar{v} \neq \bar{0}$.

Denn: $\bar{u} \cdot \bar{v} = \bar{0} \Leftrightarrow p$ teilt $u \cdot v$

Aber dann teilt p entweder u oder v (Primfaktorzerlegung von $u \cdot v$) $\Rightarrow \bar{u} = \bar{0}$ oder $\bar{v} = \bar{0}$.

Es folgt: $\bar{u} \cdot \bar{v} = \bar{u} \cdot \bar{w} \Leftrightarrow \bar{u}(\bar{v} - \bar{w}) = \bar{0} \Leftrightarrow \bar{v} = \bar{w}$, d.h. die Abbildung $\bar{v} \mapsto \bar{u} \cdot \bar{v}$ ist injektiv. Da $\mathbb{Z}/m\mathbb{Z}$ endlich ist, ist diese Abbildung auch surjektiv $\Rightarrow$ es gibt $\bar{v}$ mit $\bar{u} \cdot \bar{v} = \bar{1}$ $\Rightarrow \mathbb{Z}/m\mathbb{Z}$ ist ein Körper. □

Ist p eine Primzahl, so schreibt man $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Bsp $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$ (mod 2 Arithmetik)

$\mathbb{F}_3 = \{\bar{0}, \bar{1}, -\bar{1}\}$ usw.

Zurück zu Gruppen.

14. Die Heisenberg-Gruppen

Sei R ein kommutativer Ring. Wir setzen

$$\mathrm{Heis}(R) = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; x, y, z \in R \right\} \subseteq R^{3\times 3}.$$

Dann gilt

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \tilde{x} & \tilde{z} \\ 0 & 1 & \tilde{y} \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+\tilde{x} & z+\tilde{z}+x\tilde{y} \\ 0 & 1 & y+\tilde{y} \\ 0 & 0 & 1 \end{pmatrix}$$

und damit ist jede solche Matrix invertierbar, mit

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x & xy-z \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{pmatrix}$$

Folglich ist $\mathrm{Heis}(R)$ eine Gruppe bzgl. Matrizenmultiplikation. Die Formel zeigt auch, dass $\mathrm{Heis}(R)$ nicht abelsch ist, falls $1 \neq 0$ gilt.

Denn:
$$\begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix}$$

Ist nun $R = \mathbb{F}_p$, so folgt $|\mathrm{Heis}(\mathbb{F}_p)| = p^3$. Korollar §2.10 besagt, dass $\mathrm{Cen}(\mathrm{Heis}(\mathbb{F}_p)) \neq \{1\!\!1\}$. #

Erinnerung: Der Satz von Lagrange hatte folgendes Korollar: ist $g \in G$ und ist G endlich, dann teilt $o(g)$ die Ordnung $|G|$, denn $o(g) = |\langle g \rangle|$ und $|G| = [G : \langle g \rangle] \cdot |\langle g \rangle|$.

Es gilt aber nicht immer, dass es zu jedem Teiler m von $|G|$ ein Element der Ordnung m in G gibt.

Bsp $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, in G hat jedes Element Ordnung 1 oder 2, aber $|G| = 4$.

15. Theorem (Satz von Cauchy) Sei G eine endliche Gruppe, sei p ein Primzahl.

Wenn p ein Teiler von $|G|$ ist, dann enthält G ein Element der Ordnung p.

Beweis Wir setzen $X = \{ (g_1, \dots, g_p) \mid g_i \in G \text{ mit } g_1 \cdots g_p = e \}$

Wir können $g_1, \dots, g_{p-1}$ frei wählen, also $|X| = |G|^{p-1}$.

Gesucht ist also ein $g \in G$ mit $g \neq e$ $(g, g, \dots, g) \in X$.

Wir setzen $K = \mathbb{Z}/p\mathbb{Z}$. Dann wirkt K auf X durch "Rotation des Indizes": $\bar{k} \in K$

$$\bar{k} \cdot (g_1, \dots, g_p) = (g_{\overline{1+k}}, g_{\overline{2+k}}, \dots, g_{\overline{p+k}})$$

denn $g_1 \cdots g_p = e \Rightarrow g_2 \cdots g_p = g_1^{-1} \Rightarrow g_2 \cdots g_p g_1 = e$

usw.

Da $|K| = p$ hat jede K-Bahn Länge 1 oder Länge p, vgl §2.3 Lemma D. Sei $S \subseteq X$ ein Schnitt. Es folgt mit der Bahnformel

$$|X| = \sum_{s \in S} [K : K_s]$$

und $(e, e, e \dots e)$ hat eine Bahn der Länge 1

Da p ein Teiler von $|X|$ ist, kann nicht jede andere Bahn Länge p haben.

Es gibt also (mindestens) eine weitere Bahn der Länge 1, d.h. es gibt $(g_1, \dots, g_p) \in X$ mit $(g_1, \dots, g_p) = (g_{i+k}, \dots, g_{p+k})$ für alle k, d.h. $g = g_1 = g_2 = \dots = g_p \neq e$. Es folgt $g^p = e$. $\square$
$\Rightarrow o(g) = p$ (!)

16. Def Eine Wirkung $G \times X \to X$ heißt transitiv, wenn es für alle $u, v \in X$ ein $g \in G$ gibt mit $gu = v$. Äquivalent dazu: es gibt genau eine Bahn in X (nämlich $X = G(u)$).

Bsp Ist $G \times X \to X$ irgend eine Wirkung, $Y \subseteq X$ eine Bahn (also $Y = G(u)$ für ein $u \in X$), Dann wirkt G transitiv auf Y, denn:
$g \in G$, $y \in Y \Rightarrow gy \in G(y) = G(u)$.

Def Wir nennen $u \in X$ einen Fixpunkt einer Wirkung $G \times X \to X$, falls $gu = u$ für jedes $g \in G$ gilt. Äquivalent: $G(u) = \{u\}$.

Bsp $\mathrm{Sym}(X)$ wirkt immer transitiv auf X; zu allen $u, v \in X$ gibt es eine Permutation $\alpha \in \mathrm{Sym}(X)$ mit $\alpha(u) = v$. Etwa: α vertauscht u und v und lässt alle anderen Punkte in X fest.

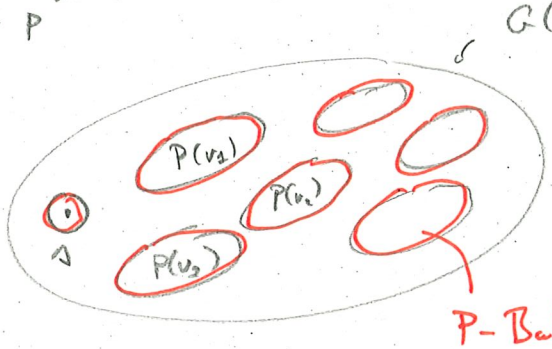
17. Lemma Sei $G \times X \to X$ eine Wirkung, seien G, X beide endlich, sei p eine Primzahl. Angenommen, es gilt folgendes.

(*) Für jedes $u \in X$ gibt es eine p-Gruppe $P \leq G$ mit $P(u) = \{u\}$ und $P(v) \neq \{v\}$ für alle $v \neq u$.

Dann wirkt G transitiv auf X und $|X| = 1 + k \cdot p$ für ein $k \geq 0$.

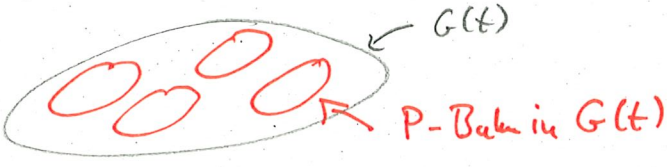
Beweis: Sei $S \subseteq G$ ein Schnitt, sei $s \in S$, sei $P \subseteq G$ eine p-Gruppe wie in (*), also $P(s) = \{s\}$ und $P(v) \neq \{v\}$ für alle $v \neq u$. Für die Bahn $G(s)$ folgt dann $|G(s)| = k \cdot p + 1$, denn für $v \neq u$ ist $|P(v)|$ ein Vielfaches von p, weil

$$\underbrace{|P(v)|}_{>1} \cdot \underbrace{[P : P_v]}_{>1} = |P| = p^m$$



Beh $S = \{s\}$

Denn sonst gibt es $t \in S$, $t \neq s$. Dann gilt für jede P-Bahn in $G(t)$, also $P(w) \subseteq G(t)$, dass $|G(w)|$ ein Vielfaches von p ist. Ausserdem ist $|G(t)| = 1 + k' \cdot p$ wie oben $\neq 0$. Also gibt es kein $t \in S$ mit $t \neq s$



Damit ist $S = \{s\}$ und $X = G(s)$ mit

$|X| = 1 + k \cdot p$ □

18. Def Sei G eine Gruppe, sei $H \leq G$ eine Untergruppe. Der Normalisator von H in G ist

$$N_G(H) = \{ g \in G \mid gHg^{-1} = H \}$$
$$= \{ g \in G \mid gH = Hg \}$$

wobei $gHg^{-1} = \{ ghg^{-1} \mid h \in H \}$

Satz $N_G(H)$ ist eine Untergruppe von G und $H \trianglelefteq N_G(H)$.

Beweis $a, b \in N_G(H) \Rightarrow abH = aHb = Hab$

$$a^{-1}H = \{ (ha)^{-1} \mid h \in H \}$$
$$= \{ (ah)^{-1} \mid h \in H \}$$
$$= Ha^{-1}$$

$\Rightarrow N_G(H)$ ist Untergruppe.

Für alle $g \in N_G(H)$ gilt $gHg^{-1} = H \Rightarrow$

$H \trianglelefteq N_G(H)$ (daher der Name "Normalisator").

□

19. Lemma Sei G eine Gruppe, seien $K, N \subseteq G$ Untergruppen. Falls $N \trianglelefteq G$ normal ist, so ist auch $KN = \{kn \mid k \in K, n \in N\}$ eine Untergruppe von G, und $KN = NK$.

Beweis $e \in KN$. Für $k_1, k_2 \in K$ $n_1, n_2 \in N$ ist $k_1 n_1 k_2 n_2 = k_1 k_2 \underbrace{k_2^{-1} n_1 k_2}_{= \tilde{n} \in N} n_2 \in KN$

sowie $(k_1 n_1)^{-1} = n_1^{-1} k_1^{-1} = k_1^{-1} \underbrace{k_1 n_1^{-1} k_1^{-1}}_{= \tilde{\tilde{n}} \in N} \in KN$ □ #

Korollar Ist $H \subseteq G$ Untergruppe, $K \subseteq N_G(H)$ Untergruppe, so ist auch $HK \subseteq N_G(H)$ eine Untergruppe. □

20. Def Sei G eine endliche Gruppe, sei p eine Primzahl, die $|G|$ teilt. Schreibe $|G| = p^m \cdot r$, wobei p kein Teiler mehr von r ist.

Ein Untergruppe $P \subseteq G$ mit $|P| = p^m$ heißt Sylow-p-Gruppe in G.

Wir setzen $Syl_p(G) = \{P \subseteq G \mid P \text{ ist Sylow-}p\text{-Gruppe}\}$

(P. Sylow, 1832 - 1918, norweg. Mathematiker)

Beobachtung: Ist $P \subseteq G$ eine p-Gruppe und $a \in G$, so ist $\underbrace{aPa^{-1}}_{=\tau_a(P)}$ ebenfalls eine p-Gruppe, denn τ_a ist bijektiv.

Q1. Theorem (Die Sylow-Sätze)

Sei G eine endliche Gruppe, sei p eine Primzahl, die $|G|$ teilt, mit $|G| = p^m \cdot r$, p kein Teiler von r. Es gilt folgendes.

(1) $Syl_p(G) \neq \emptyset$, es gibt Sylow-p-Gruppen in G.

(2) G wirkt transitiv auf der Menge $Syl_p(G)$ durch Konjugation: für $P, Q \in Syl_p(G)$ gibt es stets ein $a \in G$ mit $aPa^{-1} = Q$.

(3) $|Syl_p(G)| = k \cdot p + 1$ für ein $k \geq 0$.

(4) Ist $H \subseteq G$ eine p-Gruppe, so gibt es $P \in Syl_p(G)$ mit $H \subseteq P$.

Weiter ist $r = s \cdot (kp+1)$, insbesondere teilt $kp+1$ die Zahl r.

Beweis: Sei A die Menge aller p-Gruppen in G.

Nach Cauchys Satz §2.15 ist $A \neq \emptyset$.

Sei $\Omega \subseteq A$ die Menge aller maximalen p-Gruppen in G

($P \in \Omega \Leftrightarrow P \in A$ und es gibt kein $Q \in A$ mit $P \subsetneq Q$).

Dann ist $\Omega \neq \emptyset$. Die Gruppe G wirkt auf A

und Ω durch Konjugation wie folgt:

$$G \times A \to A \qquad G \times \Omega \to \Omega$$
$$(g, P) \longmapsto gPg^{-1} \qquad (g, P) \longmapsto gPg^{-1}.$$

Es gilt jedenfalls $Syl_p(G) \subseteq \Omega$.

1. Schritt: G wirkt transitiv auf Ω und es gibt $|\Omega| = kp+1$ für ein $k \geq 0$.

Beweis: Sei $P \in \Omega$. Dann ist P der einzige Fixpunkt von P in der Wirkung von P auf Ω.

Denn: $g \in P \Rightarrow gPg^{-1} = P$, also P ist Fixpunkt.

Ist $Q \in \Omega$ ein P-Fixpunkt, so folgt

$$P \subseteq Nor_G(Q) = \{ g \in G \mid gQg^{-1} = Q \}$$

Dann ist $Q \trianglelefteq Nor_G(Q)$, also ist $PQ \subseteq Nor_G(Q)$

eine Untergruppe, vgl. §2.19. Korollar.

Wir will $|PQ| = [PQ:Q] \cdot |Q|$ (Lagrange)

Betrachte die Abbildung $f: P \to PQ \to PQ/Q$

$g \longmapsto g \longmapsto gQ$

mit $\ker(f) = P \cap Q$ und Bild $\{gQ \mid g \in P\} =$

$\{ghQ \mid g \in P, h \in Q\} = PQ/Q$. Nach dem Homomorphie-

satz (⊗) §1.24 folgt $P/_{P\cap Q} \cong PQ/Q$

Damit ist $[PQ:Q] = [P:P\cap Q]$ eine p-Potenz, also

ist PQ eine p-Gruppe mit $PQ \geq P$. Aber P war

maximal, also $PQ = P \Rightarrow Q \leq P \Rightarrow Q = P$ □

Mit §2.17 folgt Schritt 1. □

2. Schritt Es gilt $\Omega = Syl_p(G)$

Beweis: Sei $P \in \Omega$, $|P| = p^e$. Wir müssen zeigen, dass

$p^e = p^m$. Nach Schritt 1 gilt jedenfalls

$$|G| = p^m \cdot r = |Nor_G(P)| \cdot \underbrace{|\Omega|}_{=[G:Nor_G(P)]}, \quad \text{vgl. §2.3 Lemma D}$$

$$= |Nor_G(P)| \cdot (k_p + 1)$$

(⊗) Das ist der 1. Isomorphiesatz

und damit $|Nor_G(P)| = p^m \cdot s$ für ein $s \geq 1$.

Angenommen, $l < m$. Betrachte den Homomorphismus

$$f: Nor_G(P) \longrightarrow Nor_G(P)/P = K$$
$$g \longmapsto gP$$

$\Rightarrow |K| = \underbrace{p^{m-l}}_{>1} \cdot s$. Nach Cauchy § 2.15 gibt es

ein p-Gruppe $R \subseteq K$. Betrachte $f^{-1}(R) = L \subseteq K$

Das ist eine Untergruppe, denn: $a, b \in f^{-1}(R)$ $\Rightarrow$

$ab \in f^{-1}(f(ab))$ $a^{-1} \in f^{-1}(f(a))$.

Also $R \cong L/P$ $\Rightarrow |L| = |P| \cdot \underbrace{[L:P]}_{=|R|}$

$\Rightarrow$ L ist p-Gruppe und $L \supsetneq P$ ↯ weil P maximal war. ⌋

Folglich ist $l = m$ und $\Omega = Syl_p(G)$. ⌋

Damit sind (1), (2), (3) bewiesen.

Zu (4): Ist $Q \in A$, so gibt es $P \in \Omega = Syl_p(G)$

mit $Q \subseteq P$.

□

Addendum. Es gilt $r = s \cdot (kp+1)$ mit den

Bezeichnungen von oben, also $k \cdot p + 1 = |Syl_p(G)|$

$|Nor_G(P)| = p^m \cdot s$, $|G| = p^m \cdot r$.

22. Beispiel einer Anwendung der Sylow-Sätze.

Satz Seien p, q Primzahlen mit $p < q$. Wenn G ein Gruppe ist mit $|G| = p \cdot q$ und wenn p kein Teiler von $q-1$ ist, dann ist G abelsch. #

Beweis Wir schreiben $|Syl_p(G)| = 1 + k \cdot p$

$|Syl_q(G)| = 1 + l \cdot q$

$\Rightarrow \quad q = s(kp+1)$

1. Fall $s = 1 \Rightarrow q = kp+1 \Rightarrow q-1 = kp$ ↯ zur Annahme

2. Fall $s \geq 2 \Rightarrow k = 0 \Rightarrow$ es gibt genau ein Sylow-p-Gruppe

$P \subseteq G \Rightarrow G = Nor_G(P)$, d.h. $P \trianglelefteq G$.

Jetzt $p = s'(lq+1)$ aber $p < q \Rightarrow l = 0$

$\Rightarrow$ es gibt genau ein Sylow-q-Gruppe Q und wieder $Q \trianglelefteq G$. Weiter $|P| = p$, $|Q| = q \Rightarrow P \cap Q = \{e\}$.

Für $a \in P$, $b \in Q$ folgt $ab = ba$ (ÜA, betrachte $aba^{-1}b^{-1} \in P \cap Q$) und damit ist die Abbildung

$P \times Q \to G$

$(a,b) \mapsto ab$ ein Homomorphismus mit trivialem Kern, surjektiv, also ein Isomorphismus, $G \cong P \times Q$.

Nach §1.16 Korollar D sind P, Q abelsch $\Rightarrow G$ ist abelsch. □

Also zum Beispiel: $|G| = 5 \cdot 7 \Rightarrow G$ abelsch.

Dagegen: $|Sym(3)| = 6 = 2 \cdot 3$ ist nicht abelsch (und 2 teilt 3-1).

23. Bemerkung zum Beweis der Sylow-Sätze

1. Wir haben bemerkt: wenn X die Menge aller Untergruppen einer Gruppe G ist, dann wirkt G auf X, $G \times X \to X$
$(g, H) \mapsto gHg^{-1} = \gamma_g(H)$

Wir nennen $H, K \subseteq G$ konjugiert, wenn es $g \in G$ gibt mit $gHg^{-1} = K$.

Der Stabilisator von $H \in X$ ist $Nor_G(H)$, denn
$Nor_G(H) = \{g \in G \mid gHg^{-1} = H\}$
Die Bahn von H ist die Menge $\{gHg^{-1} \mid g \in G\}$ aller Untergruppen, die konjugiert sind zu H.

2. Wir hatten bemerkt: wenn $H, N \subseteq G$ Untergruppen sind mit $N \trianglelefteq G$, dann ist HN auch eine Untergruppe (das war §2.19).

3. Wir haben in §2.22 bemerkt: wenn $N, M \trianglelefteq G$ Normalteiler sind mit $M \cap N = \{e\}$, dann gilt $mn = nm$ für alle $m \in M$, $n \in N$. Folglich ist die Untergruppe MN isomorph zu $M \times N$.

4. Wir haben den Isomorphiesatz bemerkt.

24. Die Isomorphiesätze

1. Isomorphiesatz Sei G eine Gruppe, seien $N, H \leq G$ Untergruppen mit $H \leq Nor_G(N)$. Dann ist $NH \leq G$ eine Untergruppe, $N \trianglelefteq NH$ sowie $N \cap H \trianglelefteq H$ und die Abbildung

$$f: \begin{array}{ccc} H/N\cap H & \longrightarrow & NH/N \\ g(N\cap H) & \longmapsto & gN \end{array} \quad \text{ist ein Isomorphismus.}$$

("Körperpost")

Beweis Es gilt $hN = Nh$ für alle $h \in H \Rightarrow HN = NH$,

denn $(HN)(HN) = HNNH = HNH = HHN = HN$

sowie $(HN)^{-1} = NH = HN \Rightarrow HN$ ist Untergruppe.

Weiter $N \trianglelefteq NH$, denn: $n \in N$, $h \in H \Rightarrow nhN = nNh = Nh = Nnh$.

Betrachte $\tilde{f}: H \to NH/N$, $h \mapsto hN$

$\ker(\tilde{f}) = \{h \in H \mid h \in N\} = N \cap H \Rightarrow N \cap H \trianglelefteq H$

$\tilde{f}$ ist surjektiv, nach dem Homomorphiesatz erhalten wir ein Isomorphismus f.

$$\begin{array}{ccc} H & \xrightarrow{\tilde{f}} & NH/N \\ \downarrow & \nearrow_{f} & \\ H/H\cap N & & \end{array}$$

2. Isomorphiesatz Sei G eine Gruppe, $M, N \trianglelefteq G$ seien Normalteiler mit $N \subseteq M$. Dann gilt $N \trianglelefteq M$ und $M/N \trianglelefteq G/N$. Es gibt einen Isomorphismus

$$G/M \cong \frac{G/N}{M/N} \qquad \text{("Kürzungsregel")}$$

Beweis Mit dem Homomorphiesatz erhalten wir aus

$$\begin{array}{ccc} G & \longrightarrow & G/M \\ \downarrow & \overset{f}{\nearrow} & \\ G/N & \overset{\exists!}{} & \end{array}$$

einen Homomorphismus $G/N \xrightarrow{f} G/M$, $gN \mapsto gM$, der surjektiv ist.

Der Kern von f ist $\{gN \mid g \in G, gM = M\}$
$= \{gN \mid g \in M\} = M/N \subseteq G/N$,

also ist $M/N \trianglelefteq G/M$. Da f surjektiv ist, folgt wieder mit dem Homomorphiesatz $\frac{G/N}{\ker(f)} \cong G/M$ □

Zurück zu den Sylow-Sätzen

25. Lemma Sei p, q Primzahl, $p < q$ und sei G eine Gruppe mit $|G| = p \cdot q$. Dann gibt es einen Normalteiler $N \trianglelefteq G$ mit $\{e\} \neq N \neq G$.

(Sogar: $|N| = q$)

Beweis: $|Syl_q(G)| = l \cdot q + 1$ und $p = l \cdot (lq+1)$
nach §2.21. Da $p < q$ folgt $l = 0$ $\rightsquigarrow$ es gibt
genau eine Sylow-q-Gruppe $Q \leq G$, d.h. $gQg^{-1} = Q$
für alle $g \in G$ $\rightsquigarrow$ $Q = N \trianglelefteq G$, $|Q| = q$. □

Nun betrachten wir p-Gruppen genauer.

26. Satz: Sei G eine p-Gruppe, p Primzahl, etwa
$|G| = p^m$, $m \geq 1$. Dann gibt es Normalteiler
$G_k \trianglelefteq G$ mit $|G_k| = p^k$, für $0 \leq k \leq m$
und mit $G_0 = \{e\} \subsetneq G_1 \subsetneq G_2 \subsetneq \dots \subsetneq G_m = G$

Beweis: Induktion nach m. Für $m = 1$ ist nichts
zu zeigen. Sei nun $m \geq 2$. Nach §2.10 ist
$Z = Cen(G) \neq \{e\}$, $|Z| = p^l$, $1 \leq l \leq m$. Nach
Cauchy §2.15 gibt es $z \in Z$ mit $o(z) = p$.
Setze $N = \langle z \rangle$. Dann ist $gN = Ng$ für alle $g \in G$
(weil $N \subseteq Cen(G)$) $\rightsquigarrow$ $N \trianglelefteq G$. Betrachte $\tilde{G} = G/N$
mit Ordnung $|\tilde{G}| = p^{m-1}$. Nach Induktionsannahme gibt
es $\tilde{G}_k \trianglelefteq \tilde{G}$, $0 \leq k \leq m-1$ mit $\tilde{G}_0 \subsetneq \tilde{G}_1 \subsetneq \dots \subsetneq \tilde{G}_{m-1} = \tilde{G}$
$|\tilde{G}_k| = p^k$. Betrachte $f: G \to \tilde{G} = G/N$, $g \mapsto gN$
und setze $G_{k+1} = f^{-1}(\tilde{G}_k)$ sowie $G_0 = \{e\}$. #

Wegen $\tilde{G}_k \trianglelefteq \tilde{G}$ ist $G_k \trianglelefteq G$ (ü4), mit

$G_0 \subseteq G_1 \subseteq \dots \subseteq G_m = G$ und $|G_{k+1}| = \underbrace{|N|}_{=p} \cdot \underbrace{[G_{k+1} : N]}_{=p^k} = p^{k+1}$ □

27. Korollar Sei G eine endliche Gruppe, p eine Primzahl, sei p^l ein Teiler von $|G|$. Dann gibt es eine Untergruppe $H \subseteq G$ mit $|H| = p^l$.

Beweis OE $l \geq 1$. Schreibe $|G| = p^m \cdot r$, r teilerfremd zu p $\Rightarrow l \leq m$. Sei $P \in Syl_p(G)$ (vgl. §2.21) $\Rightarrow |P| = p^m$. Nach §2.26 hat P eine Untergruppe $H \subseteq P$ mit $|H| = p^l$. □

28. Def Sei G eine Gruppe mit Untergruppen $G = G_m \supseteq G_{m-1} \supseteq \dots \supseteq G_1 \supseteq G_0 = \{e\}$. Falls für alle $k < m$ $G_k \trianglelefteq G_{k+1}$ gilt, so heißt $G_m \supseteq G_{m-1} \supseteq \dots \supseteq G_0$ eine Normalreihe in G. Die Gruppen G_{k+1}/G_k heißen Faktoren der Normalreihe.

Falls G eine Normalreihe mit abelschen Faktoren hat, so heißt G auflösbar.

Beispiele (a) Abelsche Gruppen sind auflösbar

(setze $m=1$, $G_1 = G$, $G_0 = \{e\}$)

(b) $|G| = p \cdot q$ mit Primzahlen $p < q$

$\Rightarrow$ G auflösbar.

Denn es gibt $N \in Syl_q(G)$, $N \trianglelefteq G$ (vgl. §2.25)

$|N| = q \Rightarrow N$ abelsch (sogar zyklisch, vgl §1.16)

$|G/N| = p \Rightarrow G/N$ auch zyklisch $\Rightarrow$ Normalreihe

$G \supseteq N \supseteq \{e\}$

Insbesondere ist $Sym(3)$ auflösbar (aber nicht abelsch).

(c) Jede p-Gruppe G ist auflösbar. Denn:

Nach §2.26 gibt es Normalteiler $G_k \trianglelefteq G$

$G_0 = \{e\} \subseteq G_1 \subseteq \dots \subseteq G_m = G$, $|G_k| = p^k$.

Es folgt $|G_{k+1}/G_k| = p \Rightarrow G_{k+1}/G_k$ abelsch.