09.12.2015

Nicht-Euklidische Geometrie (Weiss) WS 2015-16 Vorlesungsnotizen, Woche 8

8.1. Für den Überblick: Wirkungen von Gruppen

Definition 8.1.1. Eine Wirkung einer Gruppe G auf einer Menge S (englisch: action of a group G on a set S) ist eine Abbildung

$$\alpha\colon G \times S \longrightarrow S$$

die die folgenden Bedingungen erfüllt:

- $\alpha(1, t) = t$ für alle $t \in S$ (wobei 1 das neutrale Element von G bezeichnet);
- *Assoziativität*: $\alpha(x, \alpha(y, t)) = \alpha(xy, t)$ für alle $x, y \in G$ und $t \in S$.

Statt $\alpha(x, t)$ schreibt man oft xt (wobei $x \in G$ und $t \in S$, und dann $xt \in S$). Dann lauten die Bedingungen so: $1t = t$ für alle $t \in S$, und $x(yt) = (xy)t$ für alle $x, y \in G$ und $t \in S$.

Bemerkung 8.1.2. Eine Wirkung α von G auf S ist genau dasselbe wie ein Gruppenhomomorphismus $\psi\colon G \to \Sigma_S$.

Ganz kurz skizziert: Gegeben Wirkung α von G auf S. Wir bauen den entsprechenden Gruppenhomomorphismus $\psi\colon G \to \Sigma_S$ wie folgt. Für $x \in G$ ist $\psi(x)$ die bijektive Abbildung von S nach S definiert durch $t \mapsto \alpha(x, t)$ für beliebige $t \in S$. (Sie ist wirklich bijektiv, weil eine Inverse dazu gegeben ist durch $t \mapsto \alpha(x^{-1}, t)$.) — Umgekehrt, gegeben Gruppenhomomorphismus $\psi\colon G \to \Sigma_S$. Die entsprechende Wirkung α von G auf S ist definiert durch $\alpha(x, t) = \psi(x)(t)$ für beliebige $x \in G$ und $t \in S$. Das ist sinnvoll, weil $\psi(x)$ eine bijektive Abbildung von S nach S ist und als solche auf $t \in S$ losgelassen werden kann.

Beispiel 8.1.3. Die Gruppe G der reellen 5×5-Matrizen mit Determinante $\neq 0$ macht eine Wirkung α auf der Menge $\mathbb{R}^5$ wie folgt: $\alpha(A, v) = Av$ für $A \in G$ und $v \in \mathbb{R}^5$. Hierbei soll $v \in \mathbb{R}^5$ als Spaltenvektor (genauer, als 5×1-Matrix) gelesen werden. $Av \in \mathbb{R}^5$ ist dann das Matrixprodukt, wieder eine 5×1-Matrix.

Beispiel 8.1.4. Sei T die Teilmenge von Σ_4 bestehend aus den bijektiven Abbildungen $f\colon \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$, die $f \circ f = \mathrm{id}$ erfüllen und $f(x) \neq x$ für alle $x \in \{1, 2, 3, 4\}$. Die Menge T hat drei Elemente. Eine Wirkung α von Σ_4 auf T kann wie folgt definiert werden: für $g \in \Sigma_4$ und $f \in T$ ist $\alpha(g, f) = g \circ f \circ g^{-1} \in T$.

Die Wirkung α entspricht einem Gruppenhomomorphismus von Σ_4 nach Σ_T. Er ist ganz interessant. Weil T genau 3 Elemente hat, die wir durchnummerieren können, können wir hier auch Σ_3 statt Σ_T schreiben.

Definition 8.1.5. Sei $\alpha\colon G\times S \to S$ eine Wirkung von Gruppe G auf Menge S. Für festes $t \in S$ sei

$$G_t = \{x \in G \mid xt = t\}.$$

Es ist leicht zu sehen, dass G_t eine Untergruppe von G ist. Sie heisst *Standgruppe*[1] von t (für die Wirkung α).

Sei $\alpha\colon G \times S \to S$ eine Wirkung von Gruppe G auf Menge S. Wir führen eine Relation b_α auf S ein. Für $s, t \in S$ soll gelten $(s, t) \in b_\alpha$ falls $x \in G$ existiert mit $\alpha(x, s) = t$; in Kurzschreibweise, $xs = t$.

Lemma 8.1.6. *Diese Relation b_α auf S ist eine Äquivalenzrelation.*

Beweis. Reflexiv: für $t \in S$ ist $1t = t$, also $(t, t) \in b_\alpha$. Symmetrisch: wenn $(s, t) \in b_\alpha$, dann $xs = t$ für ein $x \in G$, also $s = x^{-1}t$ für dasselbe x, also $(t, s) \in b_\alpha$. Transitiv: wenn $(s, t) \in b_\alpha$ und $(t, r) \in b_\alpha$, dann $xs = t$ für ein $x \in G$ und $yt = r$ für ein $y \in G$, also $(yx)s = y(xs) = yt = r$ und damit $(s, r) \in b_\alpha$. $\square$

Definition 8.1.7. Die Äquivalenzklassen von b_α heissen *Bahnen* (englisch *orbits*) der Wirkung α. (Also: zwei Elemente $s, t \in S$ gehören zur selben Bahn der Wirkung genau dann, wenn $x \in G$ existiert mit $xs = t$. Weil die Bahnen Äquivalenzklassen sind, ist S die disjunkte Vereinigung der verschiedenen Bahnen.)

Manchmal ist es hilfreich, die Sache so auszudrücken. Sei $t \in S$. Die *Bahn von* t (bei der gegebenen Wirkung) ist

$$Gt = \{xt \mid x \in G\},$$

eine Teilmenge von S. Daran ist auf den ersten Blick nichts, was schwierig aussieht. Aber: diese Bahnen können eben auch als Äquivalenzklassen einer Äquivalenzrelation definiert werden. Deswegen gilt für beliebige $s, t \in S$: entweder $Gt = Gs$ oder $Gt \cap Gs = \emptyset$. Das ist bemerkenswert.

Beispiel 8.1.8. Sei G die Gruppe der 2×2-Matrizen mit Einträgen in $\mathbb{Z}$ und Determinante 1. Sei $\mathbb{Z}^2$ die Menge der 2×1-Matrizen mit Einträgen in $\mathbb{Z}$. (Sie dürfen die Elemente von $\mathbb{Z}^2$ auch *Spaltenvektoren* mit ganzzahligen Einträgen nennen, aber Vorsicht, $\mathbb{Z}^2$ ist kein Vektorraum in irgendeinem

[1]Oder auch Stabilisatorgruppe, oder auch Isotropiegruppe ...

vernünftigen Sinn). Durch Multiplikation von 2×2-Matrizen mit 2×1-Matrizen erhalten wir in der üblichen Weise eine Wirkung von G auf $\mathbb{Z}^2$. Es stellt sich heraus, dass zwei Elemente

$$\begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}$$

von $\mathbb{Z}^2$ genau dann zur selben Bahn der Wirkung gehören, wenn

$$\text{g.g.t}(a, b) = \text{g.g.t}(c, d).$$

(Wahrscheinlich ist das eine Übungsaufgabe.)

Definition 8.1.9. Die Wirkung α heisst *transitiv*, falls zu beliebigen $s, t \in S$ ein $x \in G$ existiert mit $\alpha(x, s) = t$, in Kurzschreibweise, $xs = t$. Gleichwertig dazu: die Wirkung hat nur eine Bahn.

Sei α eine *transitive* Wirkung von G auf S und sei $t \in S$ ein ausgewähltes Element. Dann haben wir die Standgruppe G_t , Untergruppe von G. Es soll demnächst gezeigt werden, dass man in gewisser Weise die Menge S und die Wirkung α rekonstruieren kann aus der der Standgruppe G_t als Untergruppe von G. Dazu brauchen wir aber noch ... den folgenden Abschnitt.

8.2. F.d.Ü.: Nebenklassen, normale Untergruppen und Homomorphiesatz

Definition 8.2.10. Sei G eine Gruppe und $H \subset G$ eine Untergruppe. Wir führen eine Äquivalenzrelation η_H auf G ein wie folgt. Für $x, y \in G$ soll gelten $(x, y) \in \eta_H$ genau dann, wenn $z \in H$ existiert mit $x = yz$. (Es ist wirklich eine Äquivalenzrelation; siehe Bemerkung 8.2.12.)

Für jedes $x \in G$ kann die Äquivalenzklasse von x nach dieser Äquivalenzrelation beschrieben werden als

$$xH = \{xz \mid z \in H\},$$

Teilmenge von G. (Siehe Bemerkung 8.2.12.) Diese Äquivalenzklassen heissen *Linksnebenklassen von* H *in* G. Die Menge der Äquivalenzklassen wird mit G/H bezeichnet.

Manchmal ist es hilfreich, die Sache so auszudrücken. Für jedes $x \in G$ ist $xH = \{xz \mid z \in H\}$ diejenige Linksnebenklasse von H, die x enthält. An dieser Beschreibung von xH ist nichts, was schwierig wäre. Aber weil diese Linksnebenklassen auch als Äquivalenzklassen einer Äquivalenzrelation beschrieben werden können, gilt für beliebige $x, y \in G$: entweder $xH = yH$ oder $xH \cap yH = \emptyset$. Das ist bemerkenswert.[2]

[2]Vergleiche Definition 8.1.7. Hier gibt es offenbar eine Analogie. Man kann es so sagen: die Linksnebenklassen von H in G sind eigentlich so etwas wie Bahnen einer Wirkung der

Beispiel 8.2.11. Sei $G = \mathbb{Z}$ die (abelsche) Gruppe der ganzen Zahlen mit der üblichen Addition als Gruppenstruktur. (Wir benutzen additive Schreibweise, also $+$ statt $\cdot$ und 0 für das neutrale Element.) Sei $H = 7\mathbb{Z}$ die Menge aller ganzen Zahlen, die durch 7 teilbar sind. Das ist eine Untergruppe von G. Die Relation η_H bedeutet jetzt folgendes. Ganze Zahlen x und y sind in dieser Relation, $(x, y) \in \eta_H$, genau dann, wenn eine durch 7 teilbare ganze Zahl z existiert mit $x = y + z$. Man kann auch sagen: $(x, y) \in \eta_H$ genau dann, wenn x und y kongruent modulo 7 sind, $x \equiv y \mod 7$.

Obwohl G und H beide unendlich sind, hat H nur 7 (Links-)Nebenklassen in G. Es sind die Äquivalenzklassen der Elemente $0, 1, 2, 3, 4, 5, 6 \in G$. Weitere gibt es nicht! Wenn Sie fragen: was ist denn mit der Äquivalenzklasse von 23, dann ist die Antwort: das ist doch die Äquivalenzklasse von 2, die schon aufgeführt wurde. Die Äquivalenzklassen können also beschrieben werden als

$$7\mathbb{Z},\ 1 + 7\mathbb{Z},\ 2 + 7\mathbb{Z},\ 3 + 7\mathbb{Z},\ 4 + 7\mathbb{Z},\ 5 + 7\mathbb{Z},\ 6 + 7\mathbb{Z}\,.$$

Und wenn Sie wissen wollen, wo ihr Lieblingselement $23 + 7\mathbb{Z}$ steht in dieser Liste: es steht da, wo $2 + 7\mathbb{Z}$ steht. Um es noch deutlicher zu sagen:

$$2 + 7\mathbb{Z} = 23 + 7\mathbb{Z}.$$

Es handelt sich hier um eine Gleichheit zwischen *Teilmengen von* $\mathbb{Z}$.

Bemerkung 8.2.12. Die Relation η_H auf G ist wirklich eine Äquivalenzrelation. *Reflexivität*: Für jedes $x \in G$ ist $x = x \cdot 1$ mit $1 \in H$, also $(x, x) \in \eta_H$. *Symmetrie*: Wenn $x, y \in G$ und $(x, y) \in \eta_H$, dann $x = yz$ für ein $z \in H$, und dann ist $y = xz^{-1}$ wobei $z^{-1} \in H$ weil $z \in H$. *Transitivität*: Wenn $w, x, y \in G$ und $(w, x) \in \eta_H$ und $(x, y) \in \eta_H$, dann ist $w = xz_1$ für ein $z_1 \in H$ und $x = yz_2$ für ein $z_2 \in H$, also $w = xz_1 = (yz_2)z_1 = y(z_2 z_1)$, wobei $z_2 z_1 \in H$ weil $z_1, z_2 \in H$. □

Lemma 8.2.13. *Sei* H *eine Untergruppe von* G. *Für jede Linksnebenklasse von* H *in* G, *geschrieben etwa in der Form* xH *mit* $x \in G$, *gibt es eine Bijektion* $H \to xH$ *gegeben durch Multiplikation von links mit* x, *also* $y \mapsto xy$ *für* $y \in H$.

Beweis. Das ist eigentlich klar. Die inverse Bijektion $xH \to H$ ist gegeben durch Multiplikation von links mit x^{-1}. Beachten: diese Abbildungen hängen natürlich stark ab von der Bezeichnung xH, die wir für die Linksnebenklasse gewählt haben. Sie wissen ja, dass aus $xH = x'H$, Gleichheit von Linksnebenklassen, nicht $x = x'$ geschlossen werden kann. □

Gruppe H auf der Menge G. Das ist auch garnicht schwer zu sehen, nur muss man etwas vorsichtig sein. Diese sogenannte Wirkung ist, wie man sagt, von rechts, so dass man die Bedingung für eine Wirkung, wie wir sie kennen, etwas umschreiben müsste, um dieses Beispiel zu legitimieren.

Korollar 8.2.14. (Satz von Lagrange). *Sei* G *eine* endliche *Gruppe,* H *eine Untergruppe. Sei* $|H|$ *bzw.* $|G|$ *die Anzahl der Elemente von* H *bzw.* G*. Dann ist* $|H|$ *ein Teiler von* $|G|$*. Denn* $|G|/|H|$ *ist die Anzahl der Linksnebenklassen von* H *in* G*.*

Beweis. Da die Linksnebenklassen von H in G als Äquivalenzklassen einer Äquivalenzrelation definiert wurden, ist G die disjunkte Vereinigung der *verschiedenen*[3] Linksnebenklassen (von H in G). Da nach Lemma 8.2.13 jede Linksnebenklasse von H in G genauso viele Elemente hat wie H, muss gelten: Anzahl der Elemente von G ist gleich Anzahl der besagten Linksnebenklassen mal Anzahl der Elemente von H. □

Die *Menge* der Linksnebenklassen von H in G wird, wie schon gesagt, mit G/H bezeichnet. Die *Anzahl* der Linksnebenklassen von H in G wird oft mit $[G : H]$ bezeichnet. (Es muss keine natürliche Zahl sein.)

Beispiel 8.2.15. Sei G eine Gruppe und $y \in G$. Es gibt dann eine kleinste Untergruppe von G, die das Element y enthält. Sie wird mit $\langle y \rangle$ bezeichnet und besteht aus allen Elementen von G, die die Form y^k haben für ein $k \in \mathbb{Z}$.

Dabei ist beispielsweise y^3 zu lesen als yyy, und y^{-3} ist zu lesen als $y^{-1}y^{-1}y^{-1}$, oder auch als $(yyy)^{-1}$, was dasselbe ist. Ausserdem soll y^0 als $1 \in G$ gelesen werden.

Wir unterscheiden zwei Fälle. *Fall 1*: die Elemente y^k mit $k \in \mathbb{Z}$ sind allesamt verschieden. Dann hat $\langle y \rangle$ unendlich viele Elemente, und G erst recht. *Fall 2*: die Elemente y^k mit $k \in \mathbb{Z}$ sind nicht allesamt verschieden. Behauptung: es gibt dann eine ganze Zahl $m \geq 1$ derart, dass $\langle y \rangle$ genau m verschiedene Elemente hat, und diese sind

$$y^0, y^1, y^2, \ldots, y^{m-1}.$$

Beweis von Behptg.: Nach Voraussetzung existieren verschiedene $k, \ell \in \mathbb{Z}$ mit $y^k = y^\ell$ in G. OBdA ist $k > \ell$. Dann ist $y^{k-\ell} = 1 \in G$. Also existiert ein $m > 0$ mit $y^m = 1$. Wir suchen uns das kleinste m von dieser Art. Die Elemente $y^0, y^1, \ldots, y^{m-1}$ von G sind jetzt allesamt verschieden, denn sonst wäre $y^r = y^s$ für verschieden $r, s \in \{0, 1, \ldots, m-1\}$, mit $r < s$, und dann $y^{s-r} = 1$ im Widerspruch zur Minimalität von m. Ausserdem ist schon klar, dass diese Elemente $y^0, y^1, \ldots, y^{m-1}$ eine Untergruppe von G bilden, unter Benutzung von $y^m = 1$. (Zum Beispiel ist y^{m-1} das Inverse von $y = y^1$, denn $y^1 y^{m-1} = y^m = 1$.) Diese Untergruppe muss dann $\langle y \rangle$ sein, denn sie enthält y und kleiner geht es nicht.

[3]Vorsicht: Zwei Linksnebenklassen von H in G gelten dann als verschieden, wenn sie als Teilmengen von G verschieden sind. Ob sie verschiedene Namen haben, interessiert hier nicht so sehr. Aus $x \neq x'$ dürfen wir nicht ohne Weiteres $xH \neq x'H$ schliessen.

Korollar 8.2.16. *Sei G eine endliche Gruppe und $y \in G$. Dann gibt es eine kleinste positive ganze Zahl m mit $y^m = 1$, und dieses m ist ein Teiler von $|G|$. Demnach ist auch $y^{|G|} = 1$.*

Beweis. Die Existenz vom kleinsten m haben wir in Beispiel 8.2.15 gezeigt und dabei gesehen, dass die Untergruppe $\langle y \rangle$ von G genau m Elemente hat. Nach dem Satz von Lagrange muss also m ein Teiler von $|G|$ sein. □

Beispiel 8.2.17. Sei p eine Primzahl, $\mathbb{F}_p$ der Körper der ganzen Zahlen mod p und $\mathbb{F}_p^\times = \mathbb{F}_p \smallsetminus \{0\}$, aufgefasst als Gruppe mit der Multiplikation im Körper als Gruppenstruktur.[4] Offenbar ist $|\mathbb{F}_p^\times| = p - 1$. Also gilt für jedes $y \in \mathbb{F}_p^\times$, dass $y^{p-1} = 1 \in \mathbb{F}_p^\times$. Diese Beobachtung nennt man den *kleinen Satz von Fermat*.

Etwas weniger abstrakt ausgedrückt: wenn y eine ganze Zahl ist, die nicht durch p teilbar ist, dann ist y^{p-1} kongruent zu 1 modulo p ... das heisst, p teilt $y^{p-1} - 1$. Beispiel von Beispiel: 5 ist nicht durch 691 teilbar; also ist $5^{690} - 1$ durch 691 teilbar.[5]

Sei G eine Gruppe und H eine Untergruppe von G. Wir fragen jetzt, ob man die Menge G/H der Linksnebenklassen in vernünftiger Weise zu einer Gruppe machen kann. Folgende Definition einer Multiplikation in G/H bietet sich an:

$$xH \cdot yH := (xy)H\,.$$

Das ist aber nicht *wohldefiniert*. Denn es kann sein, dass $xH = x'H$ (obwohl zum Beispiel $x \neq x'$), und dann müssten wir darauf bestehen, dass $(xy)H = xH \cdot yH = x'H \cdot yH = (x'y)H$. Aber wir können darauf nicht bestehen, denn leider kann es passieren, dass

$$(xy)H \neq (x'y)H$$

obwohl $xH = x'H$. Wie kommt das?

Definition 8.2.18. Eine Untergruppe H von G heisst *normal*, wenn für jedes $x \in G$ gilt, dass $xHx^{-1} = H$. Dabei ist xHx^{-1} eine Abkürzung für

$$\{xyx^{-1} \mid y \in H\}.$$

[4]Wenn Sie schon wussten, dass $\mathbb{F}_p$ ein Körper ist, dann müssten Sie daraus auch sofort schliessen können, dass $\mathbb{F}_p^\times$ eine Gruppe ist, denn es geht hier nur um die Existenz von Inversen. Umgekehrt, wenn Sie Zweifel an der Existenz von Inversen für beliebige Elemente von $\mathbb{F}_p^\times$ haben, dann haben Sie vielleicht gute Gründe, müssten aber daraus sofort schliessen können, dass Sie bis jetzt garnicht wussten, dass $\mathbb{F}_p$ ein Körper ist! Ein volles Geständnis wäre dann angebracht.

[5]691 ist meine Lieblingsprimzahl.

Beispiel 8.2.19. Sei $f\colon G \to K$ ein Homomorphismus von Gruppen. Dann ist $\ker(f)$ eine normale Untergruppe von G.

Beweis: $(y \in \ker(f)) \Rightarrow (f(y) = 1) \Rightarrow (\forall x \in G : xf(y)x^{-1} = 1) \Rightarrow (\forall x \in G : f(xyx^{-1}) = 1) \Rightarrow (\forall x \in G : xyx^{-1} \in \ker(f))$.

Wenn H eine normale Untergruppe von G ist, und $x, y, x' \in G$, und ausserdem $xH = x'H$, dann dürfen wir schliessen

$$(xy)H = (x'y)H.$$

Warum? Weil $xH = x'H$, können wir schreiben $x' = xh$ für ein $h \in H$. Dann ist

$$(x'y)H = (xhy)H = xy(y^{-1}hy)H.$$

Hier ist $y^{-1}hy \in H$ nach Voraussetzung, also $xy(y^{-1}hy)H = (xy)H$ wie erhofft. Ausserdem: wenn $x \in G$ und $y, y' \in G$ mit $yH = y'H$, dann folgt ohne Probleme $(xy)H = x(yH) = x(y'H) = (xy')H$. Zusammenfassend:

Proposition 8.2.20. *Wenn* H *eine normale Untergruppe von* G *ist, dann ergibt die Formel*

$$xH \cdot yH := (xy)H$$

eine wohldefinierte Abbildung $G/H \times G/H \to G/H$*. Sie macht die Menge* G/H *zu einer Gruppe. Die Abbildung* $G \to G/H$ *gegeben durch* $x \mapsto xH$ *ist dann ein surjektiver Homomorphismus. Sein Kern ist* H*.*

Beweis: Mechanisch.

Theorem 8.2.21. (Homomorphiesatz.) *Sei* $f\colon G \to H$ *ein Homorphismus von Gruppen. Dann ist* im f *eine Untergruppe von* H*. Eine Abbildung*

$$\varphi\colon G/\ker(f) \longrightarrow \operatorname{im} f$$

ist wohl-definiert durch die Formel $\varphi(x\ker(f)) := f(x) \in H$*. Sie ist ein Isomorphismus von Gruppen.*

Beweis. im f ist Untergruppe: klar. Wohldefinierte Abbildung φ: angenommen $x, y \in G$ und $x\ker(f) = y\ker(f)$, Gleichheit von Linksnebenklassen. Dann ist $x = yz$ für ein $z \in \ker(f)$. Dann ist $f(x) = f(yz) = f(y)f(z) = f(y)$, was zu zeigen war. Abbildung φ surjektiv: klar. Gruppenhomomorphismus: klar. Abbildung φ injektiv: weil schon Homomorphismus, genügt es, zu zeigen, dass $\ker(\varphi)$ nur aus dem neutralen Element von $G/\ker(f)$ besteht. Wenn $x \in G$ und wenn die Linksnebenklasse $x\ker(f) \in G/\ker(f)$ zum Kern von φ gehört, dann ist $f(x) = 1$ und damit $x \in \ker(f)$. Also ist $x\ker(f) = \ker(f)$ in der Tat das neutrale Element von $G/\ker(f)$. $\square$

8.3. F.d.Ü.: Transitive Wirkungen und Linksnebenklassen

Sei α eine *transitive* Wirkung von einer Gruppe G auf einer Menge S. Für $x \in G$ und $s \in S$ schreiben wir wie üblich xs statt $\alpha(x, s)$.

Wir wählen jetzt ein $t \in S$. Sei G_t die Standgruppe von t, Definition 8.1.5.

Theorem 8.3.22. *Es gibt eine Bijektion von der Menge der Linksnebenklassen* G/G_t *nach* S*, definiert durch* $xG_t \mapsto xt$*.*

Beweis. Abbildung wohldefiniert: angenommen $x, y \in G$ und $xG_t = yG_t$. Dann ist $x = yz$ für ein $z \in G_t$. Demnach ist $xs = (yz)s = y(zs) = ys$, denn $zs = s$ wegen $z \in G_t$. Abbildung surjektiv: folgt aus der Transitivität der Wirkung. Abbildung injektiv: angenommen $x, y \in G$ und $xt = yt$. Dann ist $y^{-1}xt = t$, also $y^{-1}x \in G_t$. Wenn wir $z = y^{-1}x$ setzen, dann ist also $x = yz$ und $z \in G_t$. Damit ist $xG_t = yG_t$, wzbw. $\square$

Bemerkung 8.3.23. Dieser Satz und sein Beweis deuten an, dass eine transitive Wirkung von G auf einer beliebigen Menge S vollständig beschrieben werden kann, wenn wir nur die Standgruppe G_t für ein fest gewähltes $t \in S$ kennen, als Untergruppe von G.

Das ist auch richtig. Dazu sollte man sich erst Folgendes klarmachen. Sei H irgendeine Untergruppe von G. Sei G/H die Menge der Linksnebenklassen. Dann gibt es eine sehr naheliegende[6] Wirkung β von G auf G/H. Sie ist gegeben durch

$$\beta(x, yH) = (xy)H$$

(wobei $x \in G$ beliebig, $yH \in G/H$ eine beliebige Linksnebenklasse von H in G, usw.). Es ist nicht schwer zu sehen, dass die Bedingungen für eine Wirkung erfüllt sind. — Jetzt spezialisieren wir: $H = G_t$, Standgruppe wie oben. Die Bijektion von G/G_t nach S, die wir oben konstruiert haben (nennen wir sie ψ), erfüllt dann die Bedingung

$$\psi(\beta(x, yG_t)) = \alpha(x, \psi(yG_t))$$

für beliebige $x \in G$ und $yG_t \in G/G_t$ (denn beide Seiten kann man ganz mechanisch zu xyt vereinfachen). Als Gleichung ist das vielleicht ein bisschen trocken, aber in Worten ist es einleuchtend: erst ein beliebiges $x \in G$ wirken lassen (in G/G_t) und dann ψ anwenden ist dasselbe wie erst ψ anwenden und dann x wirken lassen (in S).

Der Satz 8.3.22 führt zu einer beliebten Zählmethode. Wir stellen uns vor, dass wir die Anzahl der Elemente von S bestimmen wollen. Nach dem Satz oben ist sie gleich der Anzahl der Elemente von G/G_t. Im Fall von endlichem G ist das auch gleich $|G|/|G_t|$ nach dem Satz von Lagrange.

[6] Der Standardausdruck bei Mathematikern ist *kanonisch*, was vielleicht so etwas wie heilig bedeutet.

Beispiel 8.3.24. Sei $T = \{1, 2, 3, 4, \ldots, 100\}$ und sei S die Menge der 17-elementigen Teilmengen von T. Wieviele Elemente hat S ? Sie kennen natürlich die Antwort. Aber ich will sie jetzt aus Satz 8.3.22 herleiten, um den Satz zu illustrieren und anzupreisen.

Sei also $G = \Sigma_T$ die Gruppe der bijektiven Abbildungen von T nach T. Diese Gruppe wirkt auf der Menge S durch die Formel

$$\tau \cdot K = \tau(K)$$

für $\tau \in G = \Sigma_T$ und $K \in S$. Entschlüsselung: τ ist eine Bijektion von T nach T und K ist eine 17-elementige Teilmenge von T, und $\tau(K)$ ist die 17-elementige Teilmenge von T, die wir durch Anwenden von τ auf K erhalten. — Es ist nicht schwer zu sehen, dass die Bedingungen für eine Wirkung erfüllt sind und dass diese Wirkung transitiv ist. Wir suchen uns ein besonderes $K \in S$ aus, also zum Beispiel

$$K_0 = \{1, 2, 3, \ldots, 16, 17\}.$$

Wie sieht die Standgruppe G_{K_0} aus? Sie besteht aus allen Bijektionen von T nach T, die die Teilmenge K_0 in sich selbst überführen (und daher auch $T \smallsetminus K_0$ in sich selbst überführen). So ein Ding besteht im Grunde aus einer Bijektion von K_0 nach K_0 und einer Bijektion von $T \smallsetminus K_0$ nach $T \smallsetminus K_0$. Es ist deshalb leicht zu sehen, dass

$$|G_t| = 17! \cdot (100 - 17)!\ .$$

Also ist die Anzahl der Elemente von S gleich

$$|G|/|G_t| = \frac{100!}{17! \cdot (100 - 17)!}\ .$$

Weitere Beispiele dieser Art könnten in den Übungsaufgaben kommen. Ein festlicher Kontext kann dabei nicht gänzlich ausgeschlossen werden.

Diese Zählmethode deutet an, dass bei einer transitiven Wirkung einer Gruppe G auf einer Menge S die Standgruppe G_t (für ein $t \in S$) nicht sehr stark von $t \in S$ abhängt. Denn wenn zum Beispiel G endlich ist, haben wir $|S| = |G|/|G_t|$ und daher $|G_t| = |G|/|S|$, so dass die *Anzahl* der Elemente von G_t nicht von t abhängt. Man könnte vermuten, dass G_t überhaupt nicht von t abhängt, aber ganz so einfach ist es nicht. Stattdessen:

Lemma 8.3.25. *Sei G eine Gruppe, S eine Menge, α Wirkung von G auf S; wir schreiben ys statt $\alpha(y, s)$ für $s \in S$ und $y \in G$. Für festes $t \in S$ und festes $x \in G$ gilt*

$$G_{xt} = xG_tx^{-1} = \{xyx^{-1} \mid y \in G_t\}.$$

Beweis. $y \in G_t$ ist gleichwertig zu $yt = t$, auch zu $yx^{-1}(xt) = t$, auch zu $xyx^{-1}(xt) = xt$, auch zu $xyx^{-1} \in G_{xt}$. □