

Vorträge 10 + 11 — Freie Gruppen; Gruppen in Erzeugern und Relationen

Sei X eine Menge. Sei $X^\pm := \{x^{+1} : x \in X\} \sqcup \{x^{-1} : x \in X\}$. D.h. $X^\pm$ ist die Menge der Symbole x^{+1} , x^{-1} , wobei $x \in X$.

Sei $F_0(X)$ die Menge der endlichen Wörter in $X^\pm$. Ein Element von $F_0(X)$ ist also von der Form $x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ mit $x_i \in X$ und $\varepsilon_i \in \{-1, +1\}$. Das leere Wort werde zur Kenntlichmachung mit dem Symbol 1 bezeichnet.

Sind $u, v \in F_0(X)$, so bezeichne uv deren Aneinandersetzung.

Definiere auf $F_0(X)$ die Relation $(\rightsquigarrow)$ dadurch, daß für $u, v \in F_0(X)$ und $x \in X$ stets $ux^{+1}x^{-1}v \rightsquigarrow uv$ und $ux^{-1}x^{+1}v \rightsquigarrow uv$ gelte.

Sei $(\approx)$ die Äquivalenzrelation, die von $(\rightsquigarrow)$ erzeugt wird. Sei $F(X) := F_0(X)/\approx$ die Menge der Äquivalenzklassen. Bezeichne $[u] \in F(X)$ die Äquivalenzklasse von $u \in F_0(X)$.

Lemma. Wir können auf $F(X)$ eine Multiplikation definieren durch $[u][v] := [uv]$. Dies definiert auf $F(X)$ eine Gruppenstruktur.

Wir nennen $F(X)$ die *freie Gruppe* auf X .

Beweis. Seien $u, u', v, v' \in F_0(X)$. Ist $u \rightsquigarrow u'$ und $v \rightsquigarrow v'$, dann ist $uv \rightsquigarrow u'v \rightsquigarrow u'v'$. Also folgt aus $u \approx u'$ und $v \approx v'$, daß $uv \approx u'v \approx u'v'$. Damit ist die Multiplikation auf $F(X)$ wohldefiniert.

Assoziativität folgt aus der Assoziativität des Aneinandersetzens.

Die Eins ist durch $[1]$ gegeben.

Das Inverse zu $[x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}]$ ist gegeben durch $[x_n^{-\varepsilon_n} \dots x_1^{-\varepsilon_1}]$, wobei $x_i \in X$, $\varepsilon_i \in \{-1, +1\}$. □

Lemma. Sei G eine Gruppe. Sei $X \xrightarrow{f} G$ eine Abbildung. Dann gibt es genau einen Gruppenmorphismus $F(X) \xrightarrow{\hat{f}} G$ derart, daß $\hat{f}([x_i]) = f(x_i)$ für alle $i \in [1, n]$.

Beweis. Eindeutigkeit folgt daraus, daß jedes Element von $F(X)$ ein Produkt von Elementen der Form $[x]$ mit $x \in X$ und ihrer Inversen ist.

Zur Existenz setzen wir

$$\hat{f}([x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}]) := f(x_1)^{\varepsilon_1} \dots f(x_n)^{\varepsilon_n}$$

für $x_i \in X$, $\varepsilon_i \in \{-1, +1\}$.

Seien $u, u' \in F_0(X)$. Ist $u \rightsquigarrow u'$, dann ist $\hat{f}([u]) = \hat{f}([u'])$. Also folgt aus $u \approx u'$, daß $\hat{f}([u]) = \hat{f}([u'])$. Damit ist $\hat{f}$ wohldefiniert.

Ferner ist $\hat{f}$ Morphismus von Gruppen. □

Wir schreiben nun auch kurz (und unter Mißbrauch von Bezeichnungsweisen) x statt x^{+1} für $x \in X$.

Sei H eine Gruppe, sei I eine Menge, und sei $N_i \trianglelefteq H$ für alle $i \in I$. Dann ist $\bigcap_{i \in I} N_i$ Normalteiler von H . Also gibt es zu jeder Teilmenge T von H einen eindeutig

kleinsten Normalteiler von H , der T enthält, nämlich den Schnitt aller Normalteiler, die T enthalten, geschrieben $\langle\langle T \rangle\rangle$, und genannt das *Normalteilererzeugnis* von T . Dieses ist gleich dem Untergruppenerzeugnis von $\bigcup_{h \in H} hTh^{-1}$.

Seien $n, m \geq 0$. Sei $X = \{x_1, \dots, x_n\}$ eine endliche Menge, $x_i \neq x_j$ für $i \neq j$. Seien $r_1, \dots, r_m \in F_0(X)$. Schreibe

$$\langle x_1, \dots, x_n : r_1, \dots, r_m \rangle := F(\{x_1, \dots, x_n\}) / \langle\langle [r_1], \dots, [r_m] \rangle\rangle$$

für die durch die *Erzeugenden* $x_1, \dots, x_n$ und die *Relationen* $r_1, \dots, r_m$ definierte Gruppe.

Schreibe $N := \langle\langle [r_1], \dots, [r_m] \rangle\rangle \trianglelefteq F(X)$.

Lemma. Sei G eine Gruppe. Sei $X \xrightarrow{f} G$ eine Abbildung. Sei $\hat{f}([r_i]) = 1_G$ für alle $i \in [1, m]$. Dann gibt es genau einen Gruppenmorphismus

$$\langle x_1, \dots, x_n : r_1, \dots, r_m \rangle \xrightarrow{\tilde{f}} G$$

derart, daß $\tilde{f}([x]N) = f(x)$ für alle $x \in X$.

Beweis. Eindeutigkeit folgt daraus, daß jedes Element von

$$F(X)/N = \langle x_1, \dots, x_n : r_1, \dots, r_m \rangle$$

ein Produkt von Bildern der x_i in $F(X)/N$ und ihrer Inversen ist.

Zur Existenz bemerken wir, daß aus $\hat{f}([r_i]) = 1_G$ für alle $i \in [1, m]$ folgt, daß $\hat{f}(N) = \{1_G\}$. Also ist die Abbildung $\hat{f}$ mit

$$\tilde{f}(uN) := \hat{f}(u)$$

für $u \in F(X)$ wohldefiniert. Ferner ist $\tilde{f}$ ein Gruppenmorphismus. □

Das Bild von $u \in F_0(X)$ in $F(X)/N$ modulo N wird (unter Mißbrauch von Bezeichnungen) auch kurz wieder u geschrieben.

Sei nun $\mathcal{D}_8 := \langle a, b : aaaa, bb, baba \rangle \stackrel{\text{kurz}}{=} \langle a, b : a^4, b^2, (ba)^2 \rangle$.

Lemma. Es hat $\mathcal{D}_8$ höchstens 8 Elemente.

Beweis. Da $ba = a^{-1}b$ und $ba^{-1} = ab$, ist jedes Element in $\mathcal{D}_8$ von der Form $a^i b^j$ für gewisse $i \in [0, 3]$ und $j \in [0, 1]$. □

Lemma. Es gibt einen Gruppenmorphismus $\mathcal{D}_8 \rightarrow \mathcal{S}_4$, $a \mapsto (1, 2, 3, 4)$, $b \mapsto (1, 3)$. Dieser ist injektiv. Es ist $|\mathcal{D}_8| = 8$.

Beweis. Es ist $(1, 2, 3, 4)^4 = \text{id}$, es ist $(1, 3)^2 = \text{id}$ und es ist $((1, 3) \circ (1, 2, 3, 4))^2 = \text{id}$.

Mit vorvorigem Lemma existiert $\mathcal{D}_8 \rightarrow \mathcal{S}_4$ wie angegeben auf eindeutige Weise.

Bleibt die Injektivität zu zeigen. Die von $(1, 2, 3, 4)$ und $(1, 3)$ in $\mathcal{S}_4$ erzeugte Untergruppe U hat 8 Elemente. Also ist $\mathcal{D}_8 \rightarrow U$ eine surjektive Abbildung, deren Urbildbereich ≤ 8 und deren Bildbereich = 8 Elemente hat. Es folgt, daß auch $\mathcal{D}_8$ aus 8 Elementen besteht. □

(Wir merken noch ohne Beweis an, daß $\mathcal{D}_8$ isomorph zur Symmetriegruppe des Quadrates ist, letztere gebildet bezüglich $O_2(\mathbf{R})$.)

Ein *Automorphismus* f einer Gruppe H ist ein bijektiver Gruppenmorphismus von H nach H . Ein solcher heißt *inner*, wenn es ein $y \in H$ so gibt, daß $f(h) = {}^y h = yhy^{-1}$ für alle $h \in H$.

Bemerkung. Es ist $\mathcal{D}_8 \longrightarrow \mathcal{D}_8$, $a \longmapsto a$, $b \longmapsto ab$ ein Automorphismus von $\mathcal{D}_8$. Dieser ist nicht inner.

Beweis. Es ist $a^4 = 1$, $(ab)^2 = 1$ und $(ab \cdot a)^2 = 1$. Also existiert der Gruppenmorphismus von $\mathcal{D}_8$ nach $\mathcal{D}_8$ wie angegeben. Da jedes Element von $\mathcal{D}_8$ Produkt von Elementen aus $\{a, ab\}$ ist, ist dieser Morphismus surjektiv. Da $\mathcal{D}_8$ endlich ist, ist er mithin auch injektiv.

Ferner gibt es kein $y \in \mathcal{D}_8$ mit ${}^y b = ab$. Also ist unser Automorphismus nicht inner. ◻