Algorithmische Gruppentheorie

Vorlesung 1

Eine Konstruktion der freien Gruppe

1.1. Definition. Eine Gruppe F heißt *frei*, wenn sie eine Teilmenge X hat, so dass jedes Element $f \in F$ auf genau eine Weise in der Form $f = x_1 x_2 \dots x_n$ geschrieben werden kann, wobei $x_i \in X^{\pm}$ und $x_i x_{i+1} \neq 1$ für alle i ist. Diese Form heißt *irreduzibel.* Die Menge X heißt *Basis* von F.

Die *Länge von $f \in F$ bezüglich X* ist n und wird als $|f|$ bezeichnet.

1.2. Satz. Für jede Menge X existiert eine freie Gruppe mit der Basis X. Alle freien Gruppen mit der Basis X sind isomorph. (Wir bezeichnen eine als $F(X)$.)

1.3. Satz. Eine Gruppe F ist frei mit der Basis X nur dann, wenn für jede Gruppe G und jede Abbildung $X \xrightarrow{\phi} G$ ein einziges Homomorphismus $F \xrightarrow{\phi^*} G$ mit $\phi^*|_X = \phi$ existiert.

1.4. Satz. Alle Basen einer freien Gruppe haben dieselbe Kapazität.

Diese Kapazität heißt *Rang* der freien Gruppe.

1.5. Behauptung. Sei (u, v) eine Basis der freien Gruppe F. Dann gelten:
1) (u, vu^{ε}) und $(u, u^{\varepsilon}v)$, $\varepsilon = \pm 1$, die Basen von F sind,
2) (v, u) ist eine Basis von F,
3) (u, v^{-1}) ist eine Basis von F.

1.6. Frage. Wie kann man algorithmisch erkennen, ob eine Untermenge U von freien Gruppe $F(X)$ eine Basis von $F(X)$ ist?

Vorlesungen 2-3

Nielsen-Methode

2.1. Sei $U = (u_1, \dots, u_m)$ ein Tupel der Elemente aus einer freien Gruppe $F(X)$.

Nielsen-Transformationen sind:

(T1) ein u_i nach u_i^{-1} ersetzen,
(T2) ein u_i nach $u_i u_j$ ersetzen, wobei $i \neq j$ ist,
(T3) u_i ausstreichen, wenn $u_i = 1$ ist.

U heißt *Nielsen-irreduzibel*, wenn für alle $v_1, v_3, v_3 \in U^{\pm}$ gilt

(N1) $v_1 \neq 1$,
(N2) aus $v_1 v_2 \neq 1$ folgt $|v_1 v_2| \geqslant |v_1|, |v_2|$,
(N3) aus $v_1 v_2 \neq 1$ und $v_2 v_3 \neq 1$ folgt $|v_1 v_2 v_3| > |v_1| - |v_2| + |v_3|$.

2.2. Behauptung. Transformieren wir ein Tupel U an ein anderes Tupel U'. Dann gilt $\langle U\rangle = \langle U'\rangle$.

2.3. Behauptung. Sei $U_{Nirr} = (u_1, \dots, u_m)$ ein Nielsen-irreduziebles Tupel in $F(X)$. Sei $v = v_1 v_2 \dots v_k$ ein Produkt, wobei $k \geqslant 0$, $v_i \in U^{\pm}_{Nirr}$ und $v_i v_{i+1} \neq 1$ ist. Dann ist $|v| \geqslant k$. Insbesondere, ist $\langle U_{Nirr}\rangle$ eine freie Gruppe mit der Basis U_{Nirr}.

2.4. Satz. Man kann jedes Tupel $U = (u_1, \dots, u_m)$ der Elemente einer freien Gruppe F nach ein Nielsen-irreduziebles Tupel U_{Nirr} mit Hilfe der Nielsen-Transformationen transformieren.

2.5. Folgerung. Die Gruppe $\langle U\rangle$ ist frei mit der Basis $\langle U_{Nirr}\rangle$. Insbesondere, jede endlich erzeügte Untergruppe einer freien Gruppe ist frei.

2.6. Folgerung. Ein Tupel $U \subseteq F(X)$ ist eine Basis von $F(X)$ nur dann, wenn $U_{Nirr} = X$ bis Inversionen in X.

Vorlesungen 4

Fundamentale Gruppe eines Graphes. Stallings-Faltungen

4.1. Sei Γ ein zusammengehängender Graph. Seine Eckpunkte bezeichnen wir als Γ^0, seine Kanten als Γ^1. Der Anfang einer Kante e wird als $\alpha(e)$ bezeichnet, und das Ende als $\omega(e)$. Ein *Weg* in Γ ist eine endliche Folge der Kanten: $p = e_1 e_2 \dots p_k$, so dass $\alpha(e_{i+1}) = \omega(e_i)$ ist. Der Weg heißt *irreduzibel*, wenn $e_{i+1} \neq \overline{e_i}$ für alle i ist.

Fixieren wir ein Eckpunkt v in Γ. Sei $P(\Gamma, v)$ die Menge aller Wege in Γ mit Anfang und Ende v. Zwei Wege p_1 und p_2 heißen *homotop*, wenn man p_2 aus p_1 mit Hilfe der elementaren Transformationen bekommen kann, wobei eine elementare Transformation eine Einfügung oder eine Kürzung von $e\overline{e}$ ist. Die Homotopieklasse des Weges p wird als $[p]$ bezeichnet.

4.2. Lemma. In jede Homotopieklasse existiert genau ein irreduzibler Weg.

4.3. Satz-Definition. Die Menge $\pi_1(\Gamma, v) = \{[p] \,|\, p \in P(\Gamma, v)\}$ ist eine Gruppe bezüglich der Multiplikation $[p_1][p_2] = [p_1 p_2]$. Diese Gruppe heißt *fundamentale Gruppe* von Γ bezüglich v.

Sei v_1 ein anderer Eckpunkt von Γ. Dann sind die Gruppen $\pi_1(\Gamma, v)$ und $\pi_1(\Gamma, v_1)$ isomorph. In der Tat, sei q ein Weg in Γ von v nach v_1. Dann ist die Abbildung $[p] \mapsto [q^{-1}pq]$ der gewünschte Isomorphismus.

Sei T ein maximaler Baum in Γ. Insbesondere $T^0 = \Gamma^0$. Orientieren wir $\Gamma^1 \setminus T^1$ und bezeichnen wir die Menge der orientierten Kanten als $(\Gamma^1 \setminus T^1)^+$.

Für jeden Eckpunkt $v \in \Gamma^0$ sei p_v ein irreduzibler Weg in T von x zu v. Für jede Kante $e \in \Gamma^1$ sei $p_e = p_{\alpha(e)} e p^{-1}_{\omega(e)}$.

4.4. Satz. Die fundamentale Gruppe eines zusammenhängenden Graphes Γ ist frei. Mit der oberen Bezeichnungen ist die Basis von $\pi_1(\Gamma, v)$

$$\{[p_{\alpha(e)} e p^{-1}_{\omega(e)}] \,|\, e \in (\Gamma^1 \setminus T^1)^+\}.$$

4.5. Definition. Sei Γ ein zusammenhängender Graph und sei X eine Untermenge einer Gruppe G. Eine X-*Markierung* von Γ ist eine Abbildung $\varphi : \Gamma^1 \to X^{\pm}$, so dass $\varphi(e^{-1}) = \varphi(e)^{-1}$ für alle $e \in \Gamma^1$ ist. Der Graph Γ mit der X-Markierung heißt X-*Graph*.

Für einen Weg $p = e_1 e_2 \dots e_m$ in Γ definieren wir seine Markierung $\varphi(p)$ mit der Formel $\varphi(p) = \varphi(e_1)\varphi(e_2)\dots\varphi(e_m)$. Dann ist die Abbildung

$$\phi_* : \pi_1(\Gamma, v) \to G,$$

$$[p] \mapsto \varphi(p)$$

ein Homomorphismus.

4.6. Definition. Sei Γ ein X-Graph. Wenn zwei verschiedene Kanten e_1, e_2 einen gleichen Anfang und eine gleiche Markierung x haben, falten wir die zwei Kanten in eine neue Kante e mit der Markierung x. Den neuen X-Graph bezeichnen wir als Γ' und sagen, dass Γ nach Γ' *gefaltet* ist.

4.7. Satz. Sei Γ ein X-Graph, wobei X eine Untermenge einer Gruppe G ist.

(1) Wenn Γ nach Γ' gefaltet ist, dann sind die Bilder von ϕ_* und ϕ'_* gleich.

(2) Wenn Γ nicht weiter gefaltet werden kann, dann ist $\phi_* : \pi_1(\Gamma, v) \to F(X)$ ein Monomorphismus.

4.8. Satz-Folgerung. Sei $U = (u_1, \dots, u_m)$ ein Tupel der Elemente in der freien Gruppe $F(X)$.

(1) Es existiert ein X-Graph Γ (eine Rose), so dass das Bild von ϕ_* gleich $\langle U \rangle$ ist.

(2) Sei $\Gamma \succ \Gamma_1 \succ \Gamma_2 \succ \dots \succ \Gamma_n$ eine Faltungs-Reihe und Γ_n kann nicht weiter gefaltet werden. Dann ist $(\phi_n)_* : \pi_1(\Gamma_n, v) \to \langle U \rangle$ ein Isomorphismus.

Insbesondere ist die Gruppe $\langle U \rangle$ frei mit der Basis $(\phi_n)_*(S)$, wobei S eine Basis von $\pi_1(\Gamma_n, v)$ ist.

Vorlesungen 5-6

Präsentationen der Gruppen. Tietze-Transformationen

Sei $R \subseteq F(X)$ eine Untermenge. Ein *normaler Abschluss* von R in $F(X)$ ist die Menge

$$R^{F(X)} = \{\prod_{i=1}^{k} f_i^{-1} r_i^{\varepsilon_i} f_i \mid f_i \in F(X), r_i \in R, \varepsilon_i = \pm 1, k = 0, 1, \dots\}.$$

Es ist leicht zu verstehen, dass $R^{F(X)}$ eine normale Untergruppe von $F(X)$ ist. Außerdem ist $R^{F(X)}$ die kleinste normale Untergruppe von $F(X)$, die R enthält.

5.1. Lemma. Sei $r \in R$. Dann gilt $urv \in R^{F(X)} \Leftrightarrow uv \in R^{F(X)}$.

5.2. Definition. Sei G eine Gruppe. Dann existiert eine freie Gruppe $F(X)$ und ein Epimorphismus $\varphi : F(X) \to G$. Sei R eine beliebige Untermenge von $F(X)$, mit $R^{F(X)} = \operatorname{Ker} \varphi$. Dann heißt $\langle X \mid R \rangle$ eine *Präsentation* von G. Diese Präsentation heißt *endlich*, wenn X und R endlich sind.

5.3. Beispiele. 1) S_3 hat die Präsentation $\langle x, y \mid x^2, y^2, (xy)^3 \rangle$.

2) $\mathbb{Z}_3$ hat folgende Präsentationen: $\langle x \mid x^3 \rangle$ und $\langle x, y \mid x^{-5}y^2,\ x^6y^{-3} \rangle$.

3) Sei G eine Untergruppe von $GL_2(\mathbb{Q})$, wobei $A = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$ und $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ist. Dann hat G die Präsentation $\langle a, b \mid a^{-1}ba = b^n \rangle$.

4) Die Gruppe S_n hat die Präsentation

$$\langle t_1, t_2, \dots, t_{n-1} \mid t_i^2,\ t_it_{i+1}t_i = t_{i+1}t_it_{i+1},\ t_it_j = t_jt_i\ (|i-j| > 1) \rangle.$$

Eine Gruppe kann verschiedene Präsentationen haben. Aber von einer Präsentation zur anderen kann man mit Hilfe von Tietze – Transformationen gehen.

5.3. Definition.
(1) Tietze – Transformation der Type 1:

$$\langle X \mid R \rangle \to \langle X \mid R, r \rangle,$$

wobei $r \in R^{F(X)}$ ist.
(2) Tietze – Transformation der Type 2:

$$\langle X \mid R \rangle \to \langle X, y \mid R,\ y^{-1}w \rangle,$$

wobei $y \notin X^{\pm}$ und $w \in F(X)$ ist.

5.4. Satz. Seien $\langle X_1 \mid R_1 \rangle$ und $\langle X_2 \mid R_2 \rangle$ zwei endliche Präsentationen einer Gruppe G. Dann kann man die zweite Präsentation aus der ersten mit Hilfe endlicher Anwendungen der Tietze – Transformationen (1) und (2) und ihrer Inversen bekommen.

5.5. Beispiel.
1) $\langle x, y \mid xyx = yxy \rangle$ und $\langle a, b \mid a^2 = b^3 \rangle$ präsentieren dieselbe Gruppe.
2) $\langle a, b \mid a^{-1}b^2a = b^3,\ b^{-1}a^2b = a^3 \rangle$ und $\langle a, b \mid a, b \rangle$ sind zwei Präsentationen der trivialen Gruppe $\{1\}$.

Vorlesungen 7-8

Schreier-Transversal. Reidemeister–Schreier–Methode

7.1. Definition. Sei H eine Untergruppe einer freien Gruppe $F(X)$. Eine Untermenge $T \subseteq F(X)$ heißt *rechtes Schreier-Transversal* für H in $F(X)$, wenn
1) in jeder rechten Nebenklasse Hg genau ein Element aus T liegt;
   in H das Element $1 \in T$ liegt;
2) für jedes $t = x_1x_2 \dots x_m \in T$ Elemente $x_1x_2 \dots x_i$ auch in T liegen, $i = 1, 2, \dots, m$.

Für $g \in F(X)$ bezeichnen wir als $\overline{g}$ ein Element aus T mit $Hg = H\overline{g}$.
Für $t \in T$ und $x \in X \cup X^{-1}$ setzen wir $\gamma(t, x) = tx \cdot \overline{tx}^{-1}$.

7.2. Behauptung. Sei H eine Untergruppe einer freien Gruppe $F(X)$.
1) Es existiert ein rechtes Schreier-Transversal für H in $F(X)$.
2) Es gilt $\gamma(t,x) \in H$.
3) Es gilt $\gamma(t,x^{-1}) = \gamma(\overline{tx^{-1}},x)^{-1}$.
4) Sei $w = x_1x_2\dots x_n \in H$. Dann gilt

$$w = \gamma(1,x_1)\cdot\gamma(\overline{x_1},x_2)\cdot\gamma(\overline{x_1x_2},x_3)\cdot\ldots\cdot\gamma(\overline{x_1x_2\dots x_{n-1}},x_n). \tag{1}$$

7.3. Satz. Die Gruppe H ist frei mit der Basis $Y = \{\gamma(t,x)\,|\,t\in T, x\in X\}$.

Sei $\tau(w)$ das Aufschreiben der Elemente $w \in H$ in der Basis Y (siehe die Formel (1)).

7.4. Satz. Sei G eine Gruppe mit der Präsentation $\langle X\,|\,R\rangle$ und sei G_1 eine Untergruppe von G. Sei $\varphi : F(X) \to G$ der kanonische Epimorphismus, sei $H = \varphi^{-1}(G_1)$ und T ein rechtes Schreier-Transversal für H in $F(X)$. Dann hat G_1 die Präsentation

$$\langle Y\,|\,\tau(trt^{-1}), t\in T, r\in R\rangle,$$

wobei Y und $\tau(w)$ in 7.3 definiert sind.

7.5. Beispiel. Definieren wir einen Homomorphismus $G = \langle a,b\,|\,a^2=b^3\rangle \xrightarrow{\theta} S_3$ mit der Regel $a\mapsto(12), b\mapsto(123)$. Dann hat $\mathrm{Ker}(\theta)$ die Präsentation $\langle x,y,z\,|\,yz=zy, xz=zx\rangle$ und so ist $\mathrm{Ker}(\theta)\cong F_2\times\mathbb{Z}$.

Vorlesungen 9-10

Todd–Coxeter–Methode

Sei G eine Gruppe mit der Präsentation $\langle x_1,\dots,x_n\,|\,r_1,\dots,r_m\rangle$, sei G_1 eine Untergruppe von G, und seien $w_1(x_1,\dots,x_n),\dots,w_k(x_1,\dots,x_n)$ Erzeugende von G_1. Wenn der Index $|G:G_1|$ endlich ist, dann kann man folgende Datei mit Hilfe der Todd–Coxeter–Methode berechnen:

1) Index von G_1 in G;
2) Cayley-Graph von G bezüglich G_1;
3) Schreier-Transversal für G_1 in G.

9.1. Beispiel. 1) Seien $G = \langle x,y\,|\,x^4,y^3,(xy)^2\rangle$ und $G_1 = \langle x\rangle \leqslant G$. Daraus kann man konsequent die folgende Information bekommen: $|G:H| = 6$, $|x| = 4$, $|G| = 24$, $G\cong S_4$.

2) Seien $F(2,5) = \langle x,a,b,c,d\,|\,xa=b, ab=c, bc=d, cd=x, dx=a\rangle$ und $G_1 = \langle x\rangle \leqslant G$. Dann ist $|G:H| = 1$ und $F(2,5)\cong\mathbb{Z}_{11}$.

Vorlesungen 11-12

Fox-Calculus

11.1. Definition. Sei G eine Gruppe. Betrachten wir die Menge aller endlichen formalen Summen $\sum'_{g\in G} n_g g$, wobei $n_g \in \mathbb{Z}$ ist. Die Endlichkeit bedeutet, dass alle Koeffizienten n_g ausser einer endlichen Anzahl gleich 0 sind.

Man kann zwei solche Summen addieren und multiplizieren. Daraus entsteht ein Ring, der *Gruppenring* von G heißt. Der Ring wird als $\mathbb{Z}G$ bezeichnet.

11.2. Definition. Sei $F = F(X)$ eine freie Gruppe mit der Basis X und sei $\mathbb{Z}F$ der *Gruppenring* von F. Für jedes $x \in X$ definieren wir eine Fox-Ableitung

$$\frac{\partial}{\partial x} : F \to \mathbb{Z}F$$

nach der folgenden Regel:

$$\frac{\partial w}{\partial x} = u_1 + \cdots + u_k - x^{-1}v_1 - \cdots - x^{-1}v_s,$$

wobei $u_1, \dots, u_k$ die Endsegmente von w sind, die nach Auftreten von x in w stehen, und $v_1, \dots, v_s$ die Endsegmente von w sind, die nach Auftreten von x^{-1} in w stehen.

11.3. Beispiel.
1) $\frac{\partial}{\partial x}(x^{-1}y^{-1}xy) = y - x^{-1}y^{-1}xy$,

2) $\frac{\partial}{\partial y}(x^{-1}y^{-1}xy) = e - y^{-1}xy$,

3) $\frac{\partial}{\partial x}(x^n) = e + x + \cdots + x^{n-1}$.

11.4. Behauptung. Seien $x, y \in X$ und $u, v \in F$. Dann gelten die Formeln

1)
$$\frac{\partial y}{\partial x} = \begin{cases} 1, & \text{wenn } x = y \text{ ist,} \\ 0, & \text{wenn } x \neq y \text{ ist,} \end{cases}$$

2)
$$\frac{\partial}{\partial x}(x^{-1}) = -x^{-1},$$

3)
$$\frac{\partial}{\partial x}(uv) = \frac{\partial u}{\partial x}v + \frac{\partial v}{\partial x}.$$

11.5. Satz (Kettenregel). Seien $v_1, \dots, v_k \in F(X)$ und $w = w(v_1, \dots, v_k)$. Dann gilt

$$\frac{\partial w}{\partial x} = \sum_{i=1}^{k} \frac{\partial v_i}{\partial x} \cdot \frac{\partial w}{\partial v_i}$$

für alle $x \in X$.

11.6. Satz (Teilor-Formel). Für alle $w \in F(x_1, \dots, x_n)$ gilt

$$w - e = \sum_{i=1}^{n} (x_i - e) \cdot \frac{\partial w}{\partial x_i}.$$

Vorlesungen 13-14

Module

13.1. Einführendes Beispiel. Sei G eine Gruppe. Dann ist $G = F/R$, wobei F eine freie Gruppe und R eine normale Untergruppe von F ist.

Betrachten wir die Kommutator-Untergruppe von R:

$$R' = \langle [r_1, r_2] \,|\, r_1, r_2 \in R \rangle.$$

Dann ist die Faktorgruppe R/R' abelsch. Außerdem operiert G auf R/R' nach der folgenden Regel. Sei $R'r \in R/R'$ und sei $Rf \in G = F/R$. Dann setzen wir

$$R'r \cdot Rf = R'f^{-1}rf.$$

13.2. Definition. Sei A eine abelsche Gruppe (mit der Verknüpfung $+$) und sei G eine Gruppe, die auf A (von rechts) operiert, so dass

$$\begin{aligned}&(a+b)g = ag + bg,\\ &a(gh) = (ag)h,\\ &a1 = a\end{aligned}$$

für alle $a, b \in A$ und $g, h \in G$ gilt. Dann heißt A *ein G-Modul*.

13.3. Weitere Definitionen. Sei A ein G-Modul. Eine Untergruppe B von A heißt *G-Untermodul*, wenn $BG \subseteq B$ ist.

Sei B ein G-Untermodul von A. Dann ist A/B ein *G-Faktormodul*: $(a+B)g = ag+B$.

Seien A_1 und A_2 zwei G-Module. Eine Abbildung $\theta : A_1 \to A_2$ heißt *G-Homomorphismus*, wenn θ ein Homomorphismus von Gruppen ist und

$$\begin{aligned}&(a+b)\theta = a\theta + b\theta,\\ &(a\theta)g = (ag)\theta.\end{aligned}$$

für alle $a, b \in A_1$ und alle $g \in G$ gilt.

Bemerken wir, dass $\mathrm{Ker}(\theta)$ ein G-Untermodul von A_1 ist und $\mathrm{Im}(\theta)$ ein G-Untermodul von A_2 ist.

Seien $A_1, \dots, A_n$ G-Module. Dann kann man die direkte Summe von abelschen Gruppen $A_1 \oplus \dots \oplus A_n$ als G-Modul betrachten:

$$(a_1, \dots, a_n)g := (a_1 g, \dots, a_n g), \qquad a_i \in A_i, g \in G.$$

Eine Untermenge X eines G-Moduls A heißt *erzeugende Untermenge*, wenn gilt

$$A = \{x_1 g_1 + \dots + x_n g_n \,|\, x_i \in X, g_i \in G, n \in \mathbb{N}\}.$$

Ein G-Modul A heißt *trivial*, wenn $ag = a$ für alle $a \in A$ und $g \in G$ gilt.

13.4. Beispiel. Sei G eine Gruppe. Definieren wir eine abelsche Gruppe[1]:

$$A = \{\sum_{g\in G}{}' n_g g \,|\, n_g \in \mathbb{Z}\}.$$

Dann ist A ein G-Modul:

$$(\sum_{g\in G}{}' n_g g) \cdot h = \sum_{g\in G}{}' n_g (gh), \qquad h \in H.$$

Das Modul heißt *Gruppenring* von G und wird als $\mathbb{Z}G$ bezeichnet.

13.5. Beispiel. Sei $G = \mathbb{Z}_3 = \{e, g, g^2\}$. Dann hat der Gruppenring $\mathbb{Z}G$ einen Nullteiler:

$$(e - g)(e + g + g^2) = 0.$$

13.6. Definition. Ein G-Modul A heißt *frei mit der Basis* X, wenn für jedes G-Modul B und jede Abbildung $X \xrightarrow{\phi} B$ ein einziger G-Homomorphismus $A \xrightarrow{\phi^*} B$ mit $\phi^*|_X = \phi$ existiert.

Die Kapazität $|X|$ heißt *Rang* von G-Modul A.

13.7. Beispiel. $A = \underbrace{\mathbb{Z}G \oplus \mathbb{Z}G \oplus \cdots \oplus \mathbb{Z}G}_{n}$ ist ein freies G-Modul des Ranges n.

13.8. Satz. Sei B ein G-Modul, das von n Elementen erzeugt ist. Dann ist B ein Bild des freien G-Moduls aus 13.7.

13.9. Definition. Betrachten wir $\mathbb{Z}$ als triviales G-Modul. Definieren wir einen G-Homomorphismus $\varepsilon : \mathbb{Z}G \to \mathbb{Z}$ nach der Regel $\sum\limits_{g\in G}{}' n_g g \mapsto \sum\limits_{g\in G}{}' n_g$. Das G-Modul

$$U = \mathrm{Ker}(\varepsilon) = \{\sum_{g\in G}{}' n_g g \,|\, \sum_{g\in G}{}' n_g = 0\}$$

heißt *Augmentations-Ideal* von $\mathbb{Z}G$.

13.10. Satz. Sei $G = \langle X\rangle$ eine Gruppe und sei U das Augmentations-Ideal von $\mathbb{Z}G$. Dann ist das G-Modul U von $Y = \{x - e \,|\, x \in X\}$ erzeugt. Wenn G eine freie Gruppe mit der Basis X ist, ist U ein freies G-Modul mit der Basis Y.

[1] Das Symbol $\sum'$ bedeutet eine endliche Summe.

Vorlesungen 15-16

Augmentationsideal und Relationsmodul

Sei G eine Gruppe und sei $\varphi : F(X) \to G$ ein Epimorphismus, wobei $F(X)$ eine freie Gruppe mit einer Basis X ist und R eine normale Untergruppe von $F(X)$ ist. Sei $X = \{x_1, \dots, x_n\}$.

Betrachten wir 3 wichtige G-Module:

- Das *Relationsmodul* von G ist das G-Modul $R_{ab} = R/R'$ aus dem Punkt 13.1.
- Das *Augmentationsideal* $U \subseteq \mathbb{Z}G$ aus dem Punkt 13.9.
- Die *direkte Summe* $A = \underbrace{\mathbb{Z}G \oplus \mathbb{Z}G \oplus \dots \oplus \mathbb{Z}G}_{n}$, wobei $n = |X|$ ist.

15.1. Satz. 1) Definieren wir eine Abbildung $\beta : A \to U$ nach der Regel

$$(\gamma_1, \dots, \gamma_n) \overset{\beta}{\mapsto} \sum_{i=1}^{n} (\varphi(x_i) - e)\gamma_i.$$

Dann ist β ist ein G-Homomorphismus. Außerdem gelten

(a) $\mathrm{Im}(\beta) = U$,

(b) $\mathrm{Ker}(\beta) = \{\big(\varphi(\frac{\partial r}{\partial x_1}), \dots, (\varphi(\frac{\partial r}{\partial x_n})\big) \,|\, r \in R\}$.

(c) Sei $\langle x_1, \dots, x_n \,|\, r_1, \dots, x_m\rangle$ eine endliche Präsentation von G. Dann ist das G-Modul $\mathrm{Ker}(\beta)$ von Tupels $\big(\varphi(\frac{\partial r_i}{\partial x_1}), \dots, (\varphi(\frac{\partial r_i}{\partial x_n})\big)$, $i = 1, \dots, m$, erzeugt.

2) Definieren wir eine Abbildung $\psi : R_{ab} \to \mathrm{Ker}(\beta)$ nach der Regel

$$R'r \overset{\psi}{\mapsto} \Big(\varphi(\frac{\partial r}{\partial x_1}), \dots, (\varphi(\frac{\partial r}{\partial x_n})\Big).$$

Dann ist ψ ein G-Isomorphismus.

Vorlesungen 17-18

Alexander-Matrix und elementare Ideale

17.1. Definition. Sei G eine Gruppe mit einer endlichen Präsentation $\mathcal{P} = \langle x_1, \dots, x_n \,|\, r_1, \dots, x_m \rangle$. Die Alexander-Matrix der Präsentation ist

$$Ab \begin{pmatrix} \varphi\big(\frac{\partial r_1}{\partial x_1}\big) & \dots & \varphi\big(\frac{\partial r_1}{\partial x_n}\big) \\ \vdots & & \vdots \\ \varphi\big(\frac{\partial r_m}{\partial x_1}\big) & \dots & \varphi\big(\frac{\partial r_m}{\partial x_n}\big) \end{pmatrix},$$

wobei Ab den Abelianisierungshomomorphismus $\mathbb{Z}G \to \mathbb{Z}(G/G')$ bezeichnet.

Wir definieren *elementare Ideale* $E_i(\mathcal{P})$, $i = 1, 2, \dots$ in dem Gruppenring $\mathbb{Z}(G/G')$ nach der folgenden Regel:

$E_1(\mathcal{P})$ ist von Determinanten aller Minoren der Größe $l = \min(n, m)$ erzeugt.
$E_2(\mathcal{P})$ ist von Determinanten aller Minoren der Größe $l - 1$ erzeugt.
...
$E_l(\mathcal{P})$ ist von Determinanten aller Minoren der Größe 1 erzeugt.
$E_s(\mathcal{P}) = \mathbb{Z}(G/G')$ für $s \geqslant l + 1$.

Falls $G/G' \cong \mathbb{Z}$ ist, definiert man auch *Alexander-Polynom* von $\mathcal{P}$ als ggT aller Elemente der Alexander-Matrix.

17.2. Satz. Seien $\mathcal{P}_1 = \langle X_1 \,|\, R_1 \rangle$ und $\mathcal{P}_2 = \langle X_2 \,|\, R_2 \rangle$ zwei endliche Präsentationen einer Gruppe G. Dann sind die elementaren Ideale von $\mathcal{P}_1$ und $\mathcal{P}_2$ gleich.
Falls $G/G' \cong \mathbb{Z}$ ist, sind die Alexander-Polynome von $\mathcal{P}_1$ und $\mathcal{P}_2$ gleich.

Vorlesungen 19-20

Anwendungen zur Knoten-Theorie

Ein Knoten in $\mathbb{R}^3$ ist eine injektive und stetige Abbildung von dem Kreis

$$\{e^{i\varphi} \,|\, 0 \leqslant \varphi \leqslant 2\pi\}$$

in $\mathbb{R}^3$. Wir betrachten nur die Knoten, die unendlich differenzierbar sind.
Man muss
1) die Definition der fundamentalen Gruppe eines Knotens kennen;
2) die Wirtinger-Präsentation dieser Gruppe aufschschreiben können;
3) verstehen, warum die Abelianisierung dieser Gruppe isomorph $\mathbb{Z}$ ist;
4) die Alexander-Matrix, die elementaren Ideale und das Alexander-Polynom der Präsentation berechnen.

19.1. Satz. Äquivalente Knoten haben isomorphe fundamentale Gruppen und isomorphe elementare Ideale. Außerdem haben sie gleiche Alexander-Polynome.

Vorlesung 21

Freie Produkte, amalgamierte Produkte und HNN-Erweiterungen

21.1. Definition. Seien G_1 und G_2 zwei Gruppen. Ihr *freies Produkt* $G_1 * G_2$ ist die Menge aller formalen alternierenden Produkte[2] $x_1 x_2 \dots x_n$ bezüglich der natürlichen Multiplikation.

21.2. Behauptung. Die Gruppen G_1 und G_2 sind in ihr freies Produkt eingebettet. Wenn G_i $(i = 1, 2)$ die Präsentationen $\langle X_i \,|\, R_i \rangle$ haben, dann hat $G_1 * G_2$ die Präsentation $\langle X_1 \cup X_2 \,|\, R_1 \cup R_2 \rangle$.

21.3. Definition. Seien G_1 und G_2 zwei Gruppen und seien $A \leqslant G_1$ und $B \leqslant G_2$ zwei isomorphe Untergruppen. Sei $\varphi : A \to B$ ein Isomorphismus. Das *amalgamierte Produkt* von G_1 und G_2 bezüglich $\varphi : A \to B$ ist die Faktorgruppe von

$$G_1 * G_2$$

bezüglich des normalen Abschlusses der Menge $\{\varphi(a)a^{-1} \,|\, a \in A\}$ und wird als

$$G_1 \underset{A=B}{*} G_2$$

bezeichnet.

21.4. Satz. Die Gruppen G_1 und G_2 sind in ihr amalgamiertes Produkt eingebettet. Wenn G_i $(i = 1, 2)$ die Präsentationen $\langle X_i \,|\, R_i \rangle$ haben, dann hat $G_1 \underset{A=B}{*} G_2$ die Präsentation

$$\langle X_1 \cup X_2 \,|\, R_1 \cup R_2, a = \varphi(a)\, (a \in A) \rangle.$$

21.5. Definition. Sei $H = \langle X \,|\, R \rangle$ eine Gruppe und seien A, B zwei isomorphe Untergruppen von H. Sei $\varphi : A \to B$ ein Isomorphismus. Die *HNN-Erweiterung* von H bezüglich A, B, φ ist die Gruppe

$$\langle X, t \,|\, R, t^{-1}at = \varphi(a) \rangle.$$

21.6. Satz. Die Gruppe H ist in die obere HNN-Erweiterung eingebettet.

• Man soll die Definitionen von Normalformen in dem amalgamierten Produkt und in der HNN-Erweiterung kennen. Jedes Element der Gruppen hat eine einzige Normalform.

[2] Das bedeutet, dass alle x_i in G_1 oder in G_2 liegen und die benachbarten x_i, x_{i+1} nicht in derselben Gruppe liegen.

Vorlesung 22

Gruppen mit einer definierenden Relation

22.1. Freiheitssatz (Magnus). Sei $G = \langle X \,|\, r \rangle$ eine Gruppe mit einer definierenden Relation r, wobei r zyklisch reduziert ist. Sei $L \subset X$ eine Untermenge, die einen Buchstaben von r nicht enthält. Dann erzeugt L eine freie Untergruppe von G. Außerdem ist L eine Basis dieser Untergruppe.

22.2. Satz (Magnus). Sei $G = \langle X \,|\, r \rangle$ eine Gruppe mit einer definierenden Relation r. Sei L eine rekursiv abzählbare Untermenge von X. Dann ist das Mitgliedschaftsproblem $\mathrm{MP}(\langle L \rangle, G)$ algorithmisch lösbar. Insbesondere ist das Wortproblem $\mathrm{WP}(G)$ lösbar.

Vorlesungen 23-24

Gruppen mit wenig Kürzungen (Small cancelation groups)

Sei $G = \langle X \mid R \rangle$ eine endliche Präsentation, wobei alle Wörter aus R zyklisch reduziert sind. Wir bezeichnen durch R^* die Menge aller zyklischen Permutationen des Wortes von R und ihren Inversen. Weiterhin werden wir annehmen, dass $R = R^*$ ist.

23.1. Definition. Ein Wort u in der freien Gruppe $F(X)$ heißt *Teil* bezüglich der Menge R, wenn zwei Wörter $r_1, r_2 \in R$ existieren, so dass $r_1 = ur_1'$, $r_2 = ur_2'$ ist.

23.2. Definition. Sei p eine natürliche Zahl. Die Präsentation $G = \langle X \,|\, R \rangle$ erfüllt die Bedingung $C(p)$, wenn kein $r \in R$ Produkt von weniger als p Teiler ist.

23.3. Definition. Sei $q \geqslant 3$ eine natürliche Zahl. Die Präsentation $G = \langle X \,|\, R \rangle$ erfüllt die Bedingung $T(q)$, wenn $r_1, r_2, \dots, r_q \in R$ existieren, so dass $r_{i+1} \neq r_i^{-1}$ ist und $r_i r_{i+1}$ nicht reduziert ist (Addition von Indexen ist Modulo q).

23.4. Definition. Sei D eine reduzierte Karte. Die Karte D erfüllt die Bedingung $C(p)$, wenn jede innere Region den Grad nicht weniger als p hat.

Eine Karte D erfüllt die Bedingung $T(q)$, wenn jeder innere Eckpunkt den Grad nicht weniger als q hat.

23.5. Satz. Sei D eine zusammenhängende Karte ohne Eckpunkte des Grades 1 oder 2.

1) Wenn D die Bedingung $C(7)$ erfüllt, dann ist $|D^2| \leqslant 4|\partial D|$.

2) Wenn D die Bedingungen $C(5)\&T(4)$ oder $C(4)\&(5)$ erfüllt, dann ist $|D^2| \leqslant 8|\partial D|$.

23.6. Folgerung. Sei G eine Gruppe mit der Präsentation, die eine der Bedingungen $C(7)$, $C(5)\&T(4)$ oder $C(4)\&(5)$ erfüllt. Dann ist das Wortproblem für G lösbar.

Vorlesung 25

Hyperbolische Gruppen

25.1. Definition. Ein geodäter metrischer Raum (X, d) heißt δ-*hyperbolisch*, wenn für jedes geodäte Dreieck ABC und jede zwei Punkte $X \in [A, B]$ und $Y \in [A, C]$ mit

$$|AX| = |AY| \leqslant \frac{1}{2}(|AB| + |AC| - |BC|)$$

gilt $|XY| \leqslant \delta$.

25.2. Definition. Eine Gruppe G heißt δ-*hyperbolisch* bezüglich ihres endlichen Systems S von Erzeugenden, wenn ihr Cayley-Graph $\Gamma(G, S)$ ein δ-hyperbolischer Raum ist.

25.3. Satz. Sei G eine δ-hyperbolische Gruppe bezüglich eines endlichen Systems S von Erzeugenden. Dann ist $\langle X \mid r \in F(X),\ |r| \leqslant 2\delta + 2,\ r \underset{G}{=} 1\rangle$ eine Präsentation von G. Insbesondere hat jede hyperbolische Gruppe eine endliche Präsentation.

Die Präsentation $\langle X \mid r \in F(X),\ |r| \leqslant 8\delta,\ r \underset{G}{=} 1\rangle$ ist eine Dehnsche Präsentation. Insbesondere ist das Wortproblem für hyperbolische Gruppen lösbar.