Math 8245 Group Theory

Peter Webb

October 15, 2018

Contents

Chapter 1

Fundamental structures in group theory

1.1 Semidirect Products

We already know about direct products. We write $G = K \rtimes Q$ to mean K is a normal subgroup of G, Q is a subgroup of G, and $K \cap Q = 1$, $KQ = G$. We say G is a *semidirect product* of K by Q, and Q is a *complement* of K in G.

In Rotman's book the condition $K \triangleleft G$ is not required for a complement, and the argument for uniqueness implied there there does not work without this condition. I think it is usual to require K to be normal.

Examples 1.1.1.

- Direct products are semidirect products in which both subgroups are normal.
- $S_n = A_n \rtimes C_2$
- $D_{2n} = C_n \rtimes C_2$
- C_4 is not a semidirect product.
- Q_8 is not a semidirect product.
- The crystallographic group of the infinite pattern

$$\begin{array}{ccc} \triangleleft & \triangleleft & \triangleleft \\ \triangleleft & \triangleleft & \triangleleft \\ \triangleleft & \triangleleft & \triangleleft \end{array}$$

  is a semidirect product, but the crystallographic group of the infinite pattern

$$\begin{array}{ccccc} \rfloor & & \rfloor & & \rfloor \\ & \rceil & & \rceil & \\ \rfloor & & \rfloor & & \rfloor \end{array}$$

is not a semidirect product. The term *crystallographic group* means the group of *rigid motions* of the plane that preserve the pattern.

- C_6 and S_3 are both semidirect products of C_3 by C_2.

Class Activity. Which of the following have a non-trivial semidirect product decomposition? A_4, A_5, C_4, C_{10}. Is this easy or difficult?

Definition 1.1.2. A homomorphism $\phi : G \to Q$ is a *split epimorphism* if and only if there is a homomorphism $s : Q \to G$ so that $\phi s = 1_Q$.

Theorem 1.1.3 (Rotman 7.20 parts (i) and (iii))**.**

1. *A split epimorphism is an epimorphism.*
2. *Let $\phi : G \to Q$ be a group homomorphism. Then ϕ is split epi if and only if $G = K \rtimes Q_1$ where $K = \operatorname{Ker}\phi$, for some subgroup $Q_1 \le G$ mapped isomorphically to Q by ϕ, if and only if ϕ is surjective and $\operatorname{Ker}\phi$ has a complement in G.*

Class Activity. The kernel K may have many complements. Find an example where there is more than one.

Corollary 1.1.4. *Let $\phi : G \to Q$ and $s : Q \to G$ be group homomorphisms with $\phi s = 1_Q$. Then $G = \operatorname{Ker}\phi \rtimes sQ$.*

Example 1.1.5. For a short exact sequence of groups $1 \to K \xrightarrow{\theta} G \xrightarrow{\phi} Q \to 1$ to say that ϕ is split epi it is not equivalent to say that θ is split (i.e. has a right inverse). Consider $1 \to C_3 \to S_3 \to C_2 \to 1$. Show that θ is split if and only if $G = K \times Q_1$ for some subgroup $Q_1 \le G$ mapped isomorphically to Q by ϕ.

Definition 1.1.6. Let $K \triangleleft G$. Conjugation within G defines a homomorphism $\theta : G \to \operatorname{Aut} K$. Specifically, if $x \in G$ and $a \in K$ then $\theta_x(a) = xax^{-1}$. In general, such a homomorphism θ is an *action* of Q on K.

Definition 1.1.7. The group $\operatorname{Inn} K$ of *inner* automorphisms of K is the group of automorphisms of the form $\alpha(a) = bab^{-1}$ for some fixed $b \in K$.

Class Activity. When $G = S_n$ and $K = A_n$, does G have image in $\operatorname{Inn} A_n$?

When $G = K \rtimes Q$ the restriction of θ to Q gives a mapping $\theta : Q \to \operatorname{Aut} K$. We will say that G *realizes* θ in this situation.

Example 1.1.8. With the two semidirect products $C_6 = C_3 \rtimes C_2$ and $S_3 = C_3 \rtimes C_2$ the two homomorphisms $Q = C_2 \to K = C_3$ are different, realized by the two different semidirect products. The notation $\rtimes$ does not distinguish between them.

Definition 1.1.9. Let Q and K be groups and suppose we are given a homomorphism $\theta : Q \to \operatorname{Aut} K$. We define a group $K \rtimes_\theta Q$ to be $K \times Q$ as a set, and with multiplication $(a, x)(b, y) = (a\theta_x(b), xy)$.

Theorem 1.1.10 (Rotman 7.22)**.** *$K \rtimes_\theta Q$ is a semidirect product that realizes θ. Better: $K \rtimes_\theta Q$ has subgroups $K_1 \cong K$ and $Q_1 \cong Q$ so that it realizes the homomorphism $Q_1 \to Q \xrightarrow{\theta} \operatorname{Aut} K \to \operatorname{Aut} K_1$.*

The construction of $K \rtimes_\theta Q$ could be called the *external* semidirect product and the original definition $G = K \rtimes Q$ the *internal* semidirect product, extending the notion of internal and external direct products.

Theorem 1.1.11 (Rotman 7.23)**.** *If $G = K \rtimes Q$ and $\theta : Q \to \operatorname{Aut} K$ is defined by $\theta_x(a) = xax^{-1}$ then $G \cong K \rtimes_\theta Q$ (via an isomorphism that identifies K with K_1 and Q with Q_1).*

Hence any two semidirect products that realize θ are isomorphic. This resolves the issue that the notation $\rtimes$ does not carry complete information about the semidirect product. On the other hand, it is usual to write just $\rtimes$ instead of $\rtimes_\theta$.

Proof. We define a mapping

$$K \rtimes_\theta Q \to K \rtimes Q$$
$$(a, x) \mapsto ax$$

We check that $(a, x)(b, y) = (a\theta_x(b), xy) \mapsto a\theta_x(b)xy = axbx^{-1}xy = (ax)(by)$. Thus the mapping is a homomorphism. We check that it is bijective. □

Exercise 1.1.12. Let $\theta, \psi : Q \to \operatorname{Aut} K$ be two homomorphisms and let $\beta \in \operatorname{Aut} K$ and $\gamma \in \operatorname{Aut} Q$ be automorphisms. Which, if any, of the following always imply that $K \rtimes_\theta Q \cong K \rtimes_\psi Q$?

1. $\psi = \beta\theta$
2. $\psi = \theta\gamma$
3. $\psi = \beta\theta$ where $\beta \in \operatorname{Inn} K$
4. $\psi = \theta\gamma$ where $\gamma \in \operatorname{Inn} Q$
5. for all $x \in Q$, $\theta(x) = \beta\psi(x)\beta^{-1}$

1.1.1 Small p-groups

Semidirect products are important because many groups that arise in practice can be constructed this way. We describe the non-abelian groups of order p^3 when p is a prime.

Example 1.1.13 (Example 7.15 of Rotman)**.** Consider the groups of the form $(C_p \times C_p) \rtimes C_p$ where p is a prime. First we consider the possible actions of C_p on $C_p \times C_p$. The automorphism group $\operatorname{Aut}(C_p \times C_p) = GL(2, p)$ has size $(p^2-1)(p^2-p) = p(p-1)^2(p+1)$, so that Sylow p-subgroups are copies of C_p and they are all conjugate to the subgroup generated by the matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. This means that all non-identity actions of C_p on

$C_p \times C_p$ will give isomorphic semidirect products. We may take a generator of $C_p = \langle c \rangle$ to act on $C_p \times C_p = \langle a, b \rangle$ in additive notation via the matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, and in multiplicative notation as ${}^c a = a$, ${}^c b = ab$.

Class Activity. In the last paragraph, is the sentence that ends, 'will give isomorphic semidirect products' obvious?

1. $(C_p \times C_p) \rtimes C_p$ is isomorphic to the subgroup of $SL(3, p)$

$$\{ \begin{bmatrix} 1 & u & v \\ 0 & 1 & w \\ 0 & 0 & 1 \end{bmatrix} \mid u, v, w \in \mathbb{F}_p \}.$$

   Class Activity. Why?

2. $(C_p \times C_p) \rtimes C_p$ has a presentation

$$\langle a, b, c \mid a^p = b^p = c^p = [a, b] = [c, a] = 1,\ [c, b] = a \rangle.$$

3. If p is odd then every non-identity element of $(C_2 \times C_p) \rtimes C_p$ has order p. This provides an example of two non-identity groups whose lists of orders of elements are the same, but which are non-isomorphic.

Proof. 2. Let G be the group with the presentation in 2. Then $\langle a, b \rangle \lhd G$ and $|\langle a, b \rangle| \le p^2$, $|\langle c \rangle| \le p$ so $|G| \le p^3$. On the other hand, the semidirect product is an image of G and has order p^3, so the two groups must be isomorphic.

3. From the relation $[c, b] = a$ we deduce $cbc^{-1} = ab$. Every element in this group can be written $a^r b^s c^t$. To simplify the notation slightly, consider an element $a^r b^s c$. By induction, $(a^r b^s c)^d = a^{dr + s + 2s + \cdots (d-1)s} b^{ds} c^d$. Putting $d = p$ and using the fact that $1 + 2 + \cdots (p - 1)$ is divisible by p, we see that the pth power of this element is 1. $\square$

Class Activity. Where does the argument in proving 3 go wrong when $p = 2$. What is the name of the group $(C_2 \times C_2) \rtimes C_2$, where we have taken $p = 2$? Which of the properties listed above hold when $p = 2$?

Example 1.1.14. Consider groups of the form $C_{p^2} \rtimes C_p$ where p is a prime. Here $\operatorname{Aut} C_{p^2} \cong C_{p(p-1)}$ is cyclic (why?) and any two non-identity actions of $C_p = \langle c \rangle$ on $C_{p^2} = \langle a \rangle$ will give isomorphic groups (why?). We may take c to act on $\langle a \rangle$ as ${}^c a = a^{p+1}$ and now $C_{p^2} \rtimes C_p$ has a presentation

$$\langle a, c \mid a^{p^2} = c^p = 1,\ cac^{-1} = a^{1+p} \rangle.$$

Theorem 1.1.15. *1. Let p be an odd prime. Every non-abelian group of order p^3 is isomorphic to one of the two just described.*

2. Every non-abelian group of order 8 is isomorphic to D_8 or Q_8.

Proof. We sketch the proof of 1. There is a theorem as follows:

Theorem 1.1.16 (Rotman 5.46)**.** *Let G be a p-group with a unique subgroup of order p. Then G is cyclic or $p = 2$ and $G \cong Q_{2^n}$ where*

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

is the generalized quaternion group of order 2^n.

Assuming this, if $|G| = p^3$ is non-abelian with p odd, choose a non-central subgroup C_p. There is a normal subgroup of order p^2 not containing it. We obtain G as a semidirect product. Now classify the possible semidirect products as the ones we have considered. □

Class Activity. Each sentence in the last paragraph could be discussed.

Exercise 1.1.17. Compute the structure of the center $Z(G)$, the derived subgroup G' and the abelianization G/G' for each of the above groups G.

Example 1.1.18. We describe the semidihedral groups. A theorem states that

$$\operatorname{Aut} C_{2^n} \cong C_{2^{n-2}} \times C_2$$

when $n \geq 3$, but we do not need to know this theorem to see that $C_2 \times C_2$ acts on $C_{2^n} = \langle x \rangle$ as the set of four automorphisms determined by the following:

$$\begin{aligned} x &\mapsto x \\ x &\mapsto x^{-1} \\ x &\mapsto x^{2^{n-1}-1} \\ x &\mapsto x^{2^{n-1}+1} \end{aligned}$$

Letting $C_2 = \langle y \rangle$ act on C_{2^n} as $x \mapsto x^{-1}$ gives the dihedral group $D_{2^{n+1}} = C_{2^n} \rtimes C_2$. Letting $C_2 = \langle y \rangle$ act on C_{2^n} as $x \mapsto x^{2^{n-1}-1}$ gives the semidihedral group

$$SD_{2^{n+1}} = C_{2^n} \rtimes C_2 = \langle x, y \mid x^{2^n} = y^2 = 1,\ yxy = x^{2^{n-1}-1} \rangle.$$

The third group $C_{2^n} \rtimes C_2$ that is not a direct product is less important.

The semidihedral group $SD_{2^{n+1}}$ has three subgroups of order 2^n, and they are copies of C_{2^n}, D_{2^n} and Q_{2^n}. The group $GL(2, 3)$ of 2×2 invertible matrices over $\mathbb{F}_3$ of order 48 has SD_{16} as its Sylow 2-subgroup. The three classes of dihedral, semidihedral and generalized quaternion groups share the property that they are the 2-groups of maximal class, as well as being the non-abelian 2-groups of 2-rank at most 2.

1.1.2 Wreath products

We follow Rotman between Theorems 7.24 and 7.27.

Let Q and D be groups and let Q permute a set Ω. We may identify the full direct product $\prod_{\omega\in\Omega} D$ as the set of functions D^Ω from Ω to D, and inside that there is the *restricted* direct product K, consisting of functions that take the value 1 on all except finitely many ω. Given $d \in D$ and $\omega \in \Omega$ let $d_\omega : \Omega \to D$ be the function

$$d_\omega(\psi) = \begin{cases} 1 & \omega \neq \psi \\ d & \omega = \psi \end{cases}$$

Thus K is the subgroup of the direct product generated by the elements d_ω. Now Q acts on D^Ω as $({}^q f)(\psi) = f(q^{-1}\psi)$ and we calculate that ${}^q(d_\omega) = d_{q\omega}$.

Class Activity. Does ${}^q(d_\omega)$ equal $d_{q\omega}$ or $d_{q^{-1}\omega}$?

We see that Q also acts as automorphisms of the restricted direct product K. We define the (permutational) *wreath product* of D and Q to be $D \wr Q := K \rtimes Q$. The subgroup K is called the *base group* of the wreath product. If Ω is not specified we take it to be the regular representation of Q.

If, now, D also acts on a set Λ we can make both Q and K act on the product $\Lambda \times \Omega$ as follows:

$$d_\omega(\lambda, \psi) = \begin{cases} (d\lambda, \psi) & \text{if } \omega = \psi \\ (\lambda, \psi) & \text{if } \omega \neq \psi \end{cases}$$
$$q(\lambda, \psi) = (\lambda, \psi).$$

Picture:

$$\Lambda \times \Omega = \overbrace{\begin{array}{ccc} | & & | \\ \Lambda & \cdots & \Lambda \\ | & & | \end{array}}^{\Omega}$$

Theorem 1.1.19 (Rotman 7.24-26)**.**

1. *The wreath product $D \wr Q$ permutes $\Lambda \times \Omega$ via the above action.*
2. *If D and Q are both faithful in their actions, so is $D \wr Q$ on $\Lambda \times \Omega$.*
3. *If D and Q both act transitively then $D \wr Q$ is transitive on $\Lambda \times \Omega$.*
4. *$T \wr (D \wr Q) \cong (T \wr D) \wr Q$.*

Note that the proof Rotman gives makes the assumption that D and Q act faithfully.

Proof. 2. Let G be the subgroup of the group of permutations of $\Lambda \times \Omega$ generated by the permutations given by the d_ω and the q as above. The d_ω generate a subgroup isomorphic to the product of the copies of D. The permutations given by the $q \in Q$

generate a copy of Q. These two subgroups generate G and intersect in 1. We check that the conjugation of Q on $\prod_{\omega\in\Omega} D$ is correct for the wreath product. We calculate

$$\begin{aligned}
qd_\omega q^{-1}(\lambda,\psi) &= qd_\omega(\lambda, q^{-1}\psi) \\
&= q\begin{cases}(d\lambda, q^{-1}\psi) & \text{if } \omega = q^{-1}\psi \\ (\lambda, q^{-1}\psi) & \text{if } \omega \neq q^{-1}\psi\end{cases} \\
&= \begin{cases}(d\lambda, \psi) & \text{if } \omega = q^{-1}\psi \\ (\lambda, \psi) & \text{if } \omega \neq q^{-1}\psi\end{cases} \\
&= d_{q\omega}(\lambda,\psi).
\end{aligned}$$

This shows that $qd_\omega q^{-1} = d_{q\omega}$ so that the subgroup of G generated by the d_ω is normal. Since the conjugation action is correct for the wreath product we have $G \cong D \wr Q$. $\square$

Class Activity. Is the group $\langle(1,2,3),(4,5,6),(1,4)(2,5)(3,6)\rangle$ isomorphic to either $C_3 \wr C_2$ or $C_2 \wr C_3$?

Example 1.1.20. The group of rigid motions of the pattern

$$\begin{array}{ccccccccc}
\vdash & & \vdash & & \vdash & & \vdash & & \\
 & \vdash & & \vdash & & \vdash & & \vdash \\
\vdash & & \vdash & & \vdash & & \vdash & & \\
 & \vdash & & \vdash & & \vdash & & \vdash
\end{array}$$

is $\mathbb{Z} \wr C_2$.

Example 1.1.21. Groups of the form $D \wr \mathbb{Z}$ are sometimes called *lamplighter* groups.

Example 1.1.22. In his book Rotman describes a graph whose automorphism group is $C_2 \wr S_5$.

Rotman now presents Theorem 7.27 of Kaloujnine describing the Sylow subgroups of symmetric groups.

Class Activity. How many orbits does the Sylow 3-subgroup of S_{35} have on $\{1,\ldots,35\}$?

1.2 G-sets

We introduce a part of the theory of G-sets, suitable for understanding the approach GAP uses to compute with permutation groups, using stabilizer chains. Rotman's book describes other results about G-sets, such as the Cauchy-Frobenius lemma, often known as 'Burnside's Lemma'.

Let G be a group. A *G-set* is a set Ω with an action of G by permutations. There are right and left G-sets and by an action of G on Ω from the right we mean a mapping $\Omega \times G \to \Omega$ so that $\omega(gh) = (\omega g)h$ and $\omega \cdot 1 = \omega$ hold for all $\omega \in \Omega$ and $g, h \in G$. With the convention that functions are applied from the right, the specification of a right

G-set is equivalent to the specification of a homomorphism $G \to S_\Omega$, the symmetric group on Ω. Similarly a left G-set is equivalent to the specification of a homomorphism $G \to S_\Omega$ provided we adopt the convention that mappings are applied from the left. Because GAP applies mappings from the right, we will work with right G-sets.

For each $\omega \in \Omega$ the set $\omega G = \{\omega g \mid g \in G\}$ is the *orbit* of Ω that contains ω. We say that G acts *transitively* on Ω if there is only one orbit. We put

$$\mathrm{Stab}_G(\omega) = G_\omega = \{g \in G \mid \omega g = \omega\}$$

and this is the *stabilizer* of ω in G. For example:

- if G permutes the set of its subgroups by conjugation then $\mathrm{Stab}_G(H) = N_G(H)$,
- if G permutes the set of its elements by conjugation then $\mathrm{Stab}_G(x) = C_G(x)$,
- if G permutes the right cosets $H\backslash G = \{Hg \mid g \in G\}$ by right multiplication then $\mathrm{Stab}_G(Hg) = H^g = g^{-1}Hg$. This is part 3. of the result below.

A *homomorphism* $f : \Omega \to \Psi$ of G-sets is a mapping with $f(\omega g) = (f(\omega))g$ always, and if this condition is satisfied we say that the mapping f is *equivariant* for the action of G. Such a homomorphism of G-sets is an isomorphism if and only if it is bijective, if and only if there is a G-set homomorphism $f_1 : \Psi \to \Omega$ with $1_\Psi = ff_1$ and $1_\Omega = f_1 f$.

Class Activity. Is this obvious?

We probably already know the 'orbit-stabilizer' theorem. Part 2 of the next proposition is a more sophisticated version of this result, applying to infinite G-sets and containing more information.

Proposition 1.2.1.

1. *Every G-set Ω has a unique decomposition $\Omega = \bigcup_{i \in I} \Omega_i$ where I is some indexing set and the Ω_i are orbits of Ω.*
2. *If Ω is a transitive G-set and $\omega \in \Omega$ then $\Omega \cong \mathrm{Stab}_G(\omega)\backslash G$ as G-sets. Thus if Ω is finite then $|\Omega| = |G : \mathrm{Stab}_G(\omega)|$.*
3. *When $H \leq G$, the stabilizer of the element Hg in the space of right cosets $H\backslash G$ is $H^g = g^{-1}Hg$.*
4. *If $H, K \leq G$, there is a G-set homomorphism $f : H\backslash G \to K\backslash G$ with $f(H) = Kg$ if and only if $H \subseteq K^g$.*
5. *If $H, K \leq G$ then $H\backslash G \cong K\backslash G$ as G-sets if and only if K and H are conjugate subgroups of G.*
6. *Every equivariant map between transitive G-sets is an epimorphism.*
7. $\mathrm{Aut}_{G-\mathrm{set}}(H\backslash G) \cong N_G(H)/H$.

We see from 4. that every homomorphism $H\backslash G \to K\backslash G$ is the composite of a homomorphism $H\backslash G \to K^g\backslash G$ specified by $H \mapsto K^g$ where $H \leq K^g$, followed by an isomorphism $K^g\backslash G \to K\backslash G$ specified by $K^g \mapsto Kg$.

Proof. 2. Given $\omega \in \Omega$, define a mapping $G \to \Omega$ by $g \mapsto \omega g$. This is a map of G-sets. We check that the set of elements of G mapped to ωg is $\mathrm{Stab}_G(\omega)g$, so that there is induced a G-equivariant bijection between the two sets as claimed.

4. We first observe that if $f : \Omega \to \Psi$ is a map of G sets then $\mathrm{Stab}_G(\omega) \subseteq \mathrm{Stab}_G(f(\omega))$. From this, the implication '$\Rightarrow$' follows. Conversely, if $H \subseteq K^g$ we show that the specification $f : H\backslash G \to K\backslash G$ by $f(Hx) = Kgx$ is well defined. This is because if $Hx = Hy$ the $xy^{-1} \in H$ so $xy^{-1} \in K^g$ and $x = g^{-1}kgy$ for some $k \in K$. Thus $Kgx = Kgg^{-1}kgy = Kgy$. The mapping f is G-equivariant, so we have a homomorphism as claimed.

7. The mapping $N_G(H) \to \mathrm{Aut}_{G-\mathrm{set}}(H\backslash G)$ given by $g \mapsto (H \mapsto Hg)$ is a surjective homomorphism of groups. Its kernel is H. □

Let H be a subgroup of a group G. A *right transversal* to H in G is the same thing as a set of right coset representatives for H in G, that is: a set of elements $g_1, \ldots, g_t$ of G so that $G = Hg_1 \cup \cdots \cup Hg_t$.

Proposition 1.2.2. *Let G act transitively on a set Ω and let $\omega \in \Omega$ be an element with stabilizer G_ω. Then elements $\{g_i \mid i \in I\}$ of G form a right transversal to G_ω in G if and only if $\Omega = \{\omega g_i \mid i \in I\}$ and the ωg_i are all distinct.*

Proof. This comes from the isomorphism of G-sets $\Omega \cong G_\omega\backslash G$ under which $\omega g \leftrightarrow G_\omega g$. □

Algorithm 1.2.3. This observation provides a way to compute a transversal for $\mathrm{Stab}_G(\omega)$ in G. Take the generators of G and repeatedly apply them to ω, obtaining various elements of the form $\omega g_{i_1} g_{i_2} \cdots g_{i_r}$ where the g_{i_j} are generators of G. Each time we get an element we have seen previously, we discard it. Eventually we obtain the orbit ωG, and the various elements $g_{i_1} g_{i_2} \cdots g_{i_r}$ are a right transversal to $\mathrm{Stab}_G(\omega)$ in G.

There is an example below with a group of permutations of six points.

The elements of this transversal come expressed as words in the generators of G. It is what GAP does, except that it does the above with the inverses of the generators of G. If an inverse generator g^{-1} sends an already-computed element u to a new element v, the generator g is stored in position v in a list. This means that applying g to v gives u. By repeating this we eventually get back to the first element of the orbit. It is this list of generators that GAP stores in the field '`transversal`' of a stabilizer chain. Elements of a right transversal are obtained by multiplying the inverses of the generators in reverse sequence.

1.2.1 Stabilizer chains

Computing chains of stabilizers is the most important technique available in computations with permutation groups. The idea of doing this in the context of computational group theory is due to Charles Sims. The following theorem of Schreier allows us to compute generators for stabilizer subgroups and the whole approach is known as the *Schreier-Sims algorithm.*

Theorem 1.2.4 (Schreier)**.** *Let X be a set of generators for a group G, $H \leq G$ a subgroup, and T a right transversal for H in G such that the identity element of G represents the coset H. For each $g \in G$ let $\overline{g} \in T$ be such that $H\overline{g} = Hg$. Then*

$$\{tg(\overline{tg})^{-1} \mid t \in T, g \in X\}$$

is a set of generators for H.

Note that since $Htg = H\overline{tg}$, the elements $tg(\overline{tg})^{-1}$ lie in H always. Also $\overline{\overline{a}} = \overline{a}$ and $\overline{\overline{a}b} = \overline{ab}$. The generators in the set are called *Schreier generators.* Not only do they generate H but, if the elements of the transversal are expressed as words in the generators of G, then the generators of H are also expressed as words in the generators of G.

Proof. Suppose that $g_1 \cdots g_n \in H$ where the g_i lie in X. Then

$$g_1 \cdots g_n = (g_1\overline{g_1}^{-1})(\overline{g_1}g_2\overline{g_1g_2}^{-1})(\overline{g_1g_2}g_3\overline{g_1g_2g_3}^{-1}) \cdots (\overline{g_1 \cdots g_{n-1}}g_n)$$

is a product of the Schreier generators. Note that $g_1 \cdots g_n \in H$ so that $\overline{g_1 \cdots g_n} = 1$. □

If G permutes Ω, a *base* for G on Ω is a list of elements $\omega_1, \omega_2, \ldots, \omega_s$ of Ω so that the stabilizer $G_{\omega_1,\omega_2,\ldots,\omega_s}$ equals 1. Here $G_{\omega_1,\omega_2,\ldots,\omega_r}$ is the stabilizer inside the subgroup $G_{\omega_1,\omega_2,\ldots,\omega_{r-1}}$ of ω_r, for each r. Let us write G_r instead of $G_{\omega_1,\omega_2,\ldots,\omega_r}$ and $G_0 = G$. In this situation the chain of subgroups

$$G = G_0 \geq G_1 \geq \cdots \geq G_s = 1$$

is called a *stabilizer chain* (for G, with respect to the given base). We will consider for each r the subset Ω_r of Ω which is defined to be the G_r-orbit containing ω_{r+1}. Thus $\Omega_0 = \omega_1 G$, $\Omega_1 = \omega_2 G_1$ etc. A *strong generating set* for G (with respect to the base) is a set of generators for G which includes generators for each of the subgroups G_r. Thus in a strong generating set, G_r is generated by those generators that happen to fix each of $\omega_1, \ldots, \omega_r$.

Proposition 1.2.5. *Each Ω_i is acted on transitively by G_i. As G_i-sets, $\Omega_i \cong G_{i+1}\backslash G_i$. Hence $|G| = |\Omega_0| \cdots |\Omega_{s-1}|$.*

Proof. We have $\omega_{i+1} \in \Omega_i$ and $\mathrm{Stab}_{G_i}(\omega_{i+1}) = G_{i+1}$. □

Given a set of generators $G = \langle g_1, \dots, g_d\rangle$ and a subgroup $H \le G$ a *right Schreier transversal* for H in G is a right transversal with elements expressed as words in the generators, as suggested by the following $1, g_{i_1}, g_{i_1}g_{i_2}, g_{i_3}, \dots$ so that each initial segment of a word appears (earlier) in the list. Schreier transversals correspond to rooted trees.

Example 1.2.6. Let $G = \langle(1,5)(2,6),(1,3)(4,6),(2,3)(4,5)\rangle$ and write these generators as $a = (1,5)(2,6)$, $b = (1,3)(4,6)$, $c = (2,3)(4,5)$. Find a set of coset representatives for $\mathrm{Stab}_G(1)$.

Solution: We construct a Schreier tree:

$$\begin{tikzcd}
1 \arrow[r, "a"] \arrow[d, "b"'] & 5 \arrow[r, "c"] & 4 \\
3 \arrow[r, "c"] & 2 \arrow[r, "a"] & 6
\end{tikzcd}$$

giving coset representatives $1, a, b, ac, bc, bca$. These form a Schreier transversal: every initial segment of a word is in the transversal. These generators have order 2, and GAP stores their inverses in the list $[1, c, b, c, a, a]$.

Class Activity. Given that the element $abc = (1,4,6,3)(2,5) = x$ lies in G, find the coset representative that represents $\mathrm{Stab}_G(1)x$.

Table of $\overline{tg}$:

1	a	b	ac	bc	bca	
a	1	b	ac	bca	bc	a
b	a	1	bca	bc	ac	b
1	ac	bc	a	b	bca	c

Table of $tg\overline{tg}^{-1}$:

1	a	b	ac	bc	bca	
1	a^2	bab^{-1}	$acac^{-1}a^{-1}$	1	$bca^2c^{-1}b^{-1}$	a
1	aba^{-1}	b^2	$acba^{-1}c^{-1}b^{-1}$	$bcbc^{-1}b^{-1}$	$bcabc^{-1}a^{-1}$	b
c	1	1	ac^2a^{-1}	bc^2b^{-1}	$bcaca^{-1}c^{-1}b^{-1}$	c

Observe that 5 of these entries are necessarily 1. Upon evaluation of these expressions in G the last table becomes the following:

1	a	b	ac	bc	bca	
1	1	$(2,4)(3,5)$	$(2,3)(4,5)$	1	1	a
1	$(2,4)(3,5)$	1	$(2,5)(3,4)$	$(2,3)(4,5)$	$(2,5)(3,4)$	b
$(2,3)(4,5)$	1	1	1	1	$(2,4)(3,5)$	c

We see that, in the stabilizer chain, G_0 acts on Ω of size 6, $G_1 = \langle(2,3)(4,5),(2,4)(3,5)\rangle$ acts on $\{2,3,4,5\}$ of size 4, and $G_{12} = 1$, so that $|G| = 4\cdot 6 = 24$. The fact that $G_{12} = 1$ we can see by inspection, because the group is so small, but to continue the algorithm properly we go through Schreier's theorem.

Theorem 1.2.7 (Schreier)**.** *Let G have d generators and let $H \le G$ have finite index. Then H can be generated by $|G : H|(d-1)+1$ elements.*

Proof. Consider the generators $tg(\overline{tg})^{-1}$ for H, and write $n = |G : H|$. The number of edges in the Schreier tree is $n-1$. Each gives an entry 1 in the table of generators. The number of table entries which are not 1 is at most $dn - n + 1 = n(d-1)+1$. □

Write $d(G)$ for the smallest size of a set of generators of G. The last result can be written $d(H) - 1 \le |G : H|(d(G) - 1)$. When G is a free group it turns out that we always get equality in this bound. We will see this when we come to the section on free groups and, more generally, groups acting on trees. In the example, there were 5 edges in the Schreier tree, and these accounted for the 5 identity elements in the first table.

Algorithm 1.2.8. Given a stabilizer chain with a transversal for each stabilizer group in the next, we can test whether a permutation belongs to a group. If it does, and the transversal elements are words in the generators, we can express the permutation as a word in the generators. This algorithm solves problems such as restoring Rubik's cube to its initial position, given a random permutation of its faces.

Given a permutation π find the coset representative x_1 of the coset $G_1\pi$ by computing the action of π on Ω. We compute $(\omega_1)\pi$. If $\pi \in G$ this must equal $(\omega_1)g$ for some unique g in a right transversal for G_1 in G_0 and so $\pi g^{-1} \in G_1$. In fact, $\pi \in G$ if and only if $(\omega_1)\pi = (\omega_1)g$ for some g in the transversal and $\pi g^{-1} \in G_1$. We now continue to test whether $\pi g^{-1} \in G_1$ by repeating the algorithm.

Example 1.2.9. Continuing the previous example: is $(1,2,3)$ in G? Since $(1,2,3)c^{-1}b^{-1} = (4,5,6) \notin G_1$, the answer is No.

Class Activity. Is $(1,3,5)(2,6,4)$ in G? If it is, write this permutation as a word in the given generators of G.

Algorithm 1.2.10. We give an algorithm for listing the elements of G. We start by listing elements in the subgroups at the small end of the stabilizer chain, at each stage listing them by cosets in the next biggest stabilizer. Thus, if the elements of G_{i+1} have been listed and $t_1, \ldots, t_s$ is a transversal for G_{i+1} in G_i then $G_i = G_{i+1}t_1 \cup \cdots \cup G_{i+1}t_s$. In the example we get

$$[(), (3,5)(2,4), (2,3)(4,5), (3,4)2,5), a, (3,5)(2,4)a, (2,3)(4,5)a, \ldots,$$

starting with the 4 elements of G_1, and continuing with the cosets of G_1 put in the order given by the Schreier transversal. This puts an ordering on the elements of G. GAP orders everything.

Class Activity. Examine the list of elements of some groups, such as S_4 to see the coset structure in the list.

Other algorithms, such as computing generators for a Sylow p-subgroup of a group, or for the normalizer of a subgroup, depend on computing a stabilizer chain. This approach to computation within permutation groups is due to Charles Sims.

1.3 Nilpotent groups

As background material, we probably already know the following results.

Proposition 1.3.1. *Let p be a prime, G a finite p-group, and let $1 \neq H \triangleleft G$ be a non-identity normal subgroup. Then $1 \neq H \cap Z(G)$.*

Proof. G permutes the elements of H by conjugation with orbits whose lengths are powers of p. Thus the number of orbits of length 1 is divisible by p. The identity element lies in an orbit of length 1, so there is some other element also in an orbit of length 1. $\square$

Corollary 1.3.2. *Let p be a prime and G a finite p-group with $|G| \neq 1$. Then $Z(G) \neq 1$.*

Proof. Take $H = G$ in the previous result. $\square$

Corollary 1.3.3. *Let p be a prime and G a non-abelian group of order p^3. Then $|Z(G)| = p$.*

Proof. If $|Z(G)| = p^2$ then $G/Z(G)$ is cyclic and $G = Z(G)$. $\square$

The rest of this section is to be filled in later.

Chapter 2

Free constructions with groups

2.1 Construction of free groups

We follow the start of Chapter 11 of Rotman's book, specifically 11.1-11.6. As far as the construction of free groups is concerned, we already know the definition of a free group, have some idea that they consist of reduced words in their generators and inverses, and have seen their role in presentations of groups. The trouble is that we might not know for sure that any free groups (of rank bigger than 1) exist. We describe an algebraic construction of free groups. There is also a topological construction as the fundamental group of a graph. This might be thought to be more immediate, but it relies on first knowing what the fundamental group is, and then we must verify that it satisfies the free property. It is more direct to take an algebraic approach.

Definition 2.1.1. Let X be a subset of a group F. We say that F is *free* on X (or the *free group generated by* X etc.) if and only if for every group G and mapping $f : X \to G$ there exists a unique group homomorphism $\tilde{f} : F \to G$ extending f. We say that X is a *free set of generators* for F, or a *basis* for F. The size of X is called the *rank* of F.

Intuitively, if $X = \{x, y\}$ then $F = F(X)$ is the set of words such as $x^2yxy^{-1}x^{-5}$ etc, and such elements of F expressed as *reduced* words are distinct elements of F if and only if the words look distinct; but this needs to be proved. The free group $F(X)$ may have many bases, such as $\{x, y\}$, $\{x, xy\}$, $\{x^2y, xy\}$ and so on. We already probably know that if F is free with basis X then its abelianization is free abelian with basis the image of X, and since any two bases of a free abelian group must have the same size, any two bases of F must also have the same size. From the same considerations we see that the minimum number of generators $d(F)$ equals the size of X. It is true, but not obvious (and we will not prove it), that any set of generators of $F(X)$, with the same size as X, is a basis of $F(X)$. We also know already that any two free groups on generating sets of the same size are isomorphic (and the possible isomorphism biject with the bijections between the two sets of the same size).

Theorem 2.1.2 (Rotman's Theorem 11.1)**.** *If X is a set, there exists a group F that is free on X.*

To prove this we introduce some terminology. A *word* in X is a string $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ of finite length where $\epsilon_i = \pm 1$ for each i and $x_i \in X$. We write $x^1 = x$. A word is *reduced* if and only if symbols x and x^{-1} are never adjacent. Two reduced words are distinct if and only if they appear to be distinct. It is tempting to try to define F to be the set of reduced words in X and define multiplication of words by juxtaposition, followed by reduction, but the combinatorics of proving that the associative law holds in this fashion are not elegant. For example, consider the product $(y^{-1}x^{-1})(xyz)(z^{-1}y^{-1}x^{-1})$. This equals $y^{-1}x^{-1}$, but if we do the multiplication in one order these terms appear at the left end of the word, and if we do it in the other order they appear at the right end. Somehow the argument that shows associativity must cope with this phenomenon. Instead, we realize $F(X)$ as a set of permutations of the set of reduced words. Permutations automatically satisfy associativity.

Proof. For each $x \in X$ define

$$|x^\epsilon| x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} = \begin{cases} x^\epsilon x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} & \text{if } x^\epsilon \neq x_1^{-\epsilon_1} \\ x_2^{\epsilon_2} \cdots x_n^{\epsilon_n} & \text{otherwise} \end{cases}$$

Then both $|x||x^{-1}|$ and $|x^{-1}||x|$ act as the identity mapping on the set W of reduced words on X. It follows that $|x|$ and $|x^{-1}|$ are inverse permutations of W. Let F_0 be the subgroup of S_W generated by $\{|x| \mid x \in X\} = X_0$. Every element of F_0 can be written as a product $|x_1^{\epsilon_1}| \cdots |x_n^{\epsilon_n}|$ where $|x^\epsilon|$ and $|x^{-\epsilon}|$ are never adjacent. This expression is unique, because for any element $\alpha \in F_0$, if $\alpha(1) = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ then $\alpha = |x_1^{\epsilon_1}| \cdots |x_n^{\epsilon_n}|$.

We verify that F_0 is free on the generating set X_0. If G is any group and $f : X_0 \to G$ is a mapping, define $\tilde{f} : F_0 \to G$ by $\tilde{f}(|x_1^{\epsilon_1}| \cdots |x_n^{\epsilon_n}|) = f(|x_1|)^{\epsilon_1} \cdots f(|x_n|)^{\epsilon_n}$. This is well-defined, by the property of uniqueness. We observe, finally, that $\tilde{F}$ is a homomorphism and it is uniquely determined by f. □

Corollary 2.1.3. *Every group is a quotient of a free group.*

As a consequence, every group can be specified by a presentation $G = \langle X \mid R \rangle$.

Corollary 2.1.4. *Let X be a subset of a group G. Then G is freely generated by X if and only if each element of G is uniquely expressible as a reduced word in X.*

Proof. We have seen the implication '⇒' in the construction of $F(X)$. Conversely, suppose that each element of G is uniquely expressible as a reduced word in X, and let $F(X)$ be a free group generated by X. Consider the homomorphism $F(X) \to G$ that uniquely extends the identity mapping on X. It is surjective since X generates G. It is injective since each element of $F(X)$ is sent to a different element of G. Thus it is an isomorphism. □

2.2 Coset enumeration

We continue to follow 11.7 and 11.8 of Rotman's book and also the book by Johnson. These describe the Todd-Coxeter algorithm from 1936, implemented on computer from the 1950s onwards. For each relator of length n in a presentation we set up a table with $n+1$ columns; etc.

Theorem 2.2.1. *Suppose that the Todd-Coxeter algorithm for the presentation $G = \langle X \mid R\rangle$ terminates. Then G is finite, and the rows of the coset tables determine a permutation representation of G. This permutation representation is the regular representation.*

Proof. The rows give permutations, by construction. The permutations satisfy the relations in R. The group H generated by these permutations is an image of G. We have constructed a finite transitive permutation representation of G, and it has every other transitive permutation representation of G as an image, since the only restriction on it is that the relations in R hold. The fact that coset collapse may have occurred introduces some delicacy into justifying this last statement. From this it follows by Proposition 1.2.1 part 4 that G is finite and the permutation representation is the regular representation. □

Examples 2.2.2. $G = \langle a, b \mid b^2,\ bab^{-1}a^{-2}\rangle$ has order 6, no extra symbols are needed.

We eliminate c from the 'Fibonacci' group $F(2,3) = \langle a, b, c \mid ab = c,\ bc = a,\ ca = b\rangle$ to get $F(2,3) = \langle a, b \mid baba^{-1},\ abab^{-1}\rangle$. This has order 8 and no extra symbols are needed.

$G = \langle a, b \mid a^2,\ ababa\rangle$ has order 4, no extra symbols are needed.

$G = \langle a, b \mid a^2,\ b^2,\ (ab)^3\rangle$ has order 6, no extra symbols are needed.

$G = \langle a, b \mid aba^{-1} = b^2,\ bab^{-1} = a^2\rangle$ has order 1, at least 6 symbols are needed.

$G = \langle a, b, c \mid abc = b,\ bca = c,\ cab = a\rangle$ has order 48 and is not suitable for hand computation.

Coxeter presentations of D_6 and D_8 can be done by hand and need no extra symbols.

Class Activity. Find the order of the group with presentation $\langle x, y \mid xy^2,\ x^2y^3\rangle$. How many symbols did you introduce in doing the calculation?

Proposition 2.2.3. *The presentation $T_n = \langle x, y \mid x^n y^{n+1},\ x^{n+1}y^{n+2}\rangle$ of the identity group needs at least $2n+1$ symbols to complete the Todd-Coxeter algorithm.*

Proof. Consider the tables for these relators. We can only stop introducing new symbols by completing rows, and the first row to be completed will require $2n+1$ new symbols. □

I believe it is the case, for a finite presentation of a finite group, that there is always a way to choose new symbols so that the algorithm terminates, but I do not know where to find this result in the literature (if it is true). In view of the previous result, the time taken for the algorithm to terminate is not bounded by a function of the group order. Whether or not it is true that there is always a way for the algorithm to terminate, given a presentation of a finite group, it is the case that if an implementation of the algorithm does not terminate after some time, for some presentation, we cannot deduce that the group is infinite. If we do not know that the group presented is finite in advance, it is algorithmically undecidable to determine whether the group is finite or, indeed, if it is the identity group.

2.3 Cayley graphs

These are often introduced as a pictorial way to view the way multiplication works inside a group. We will use them as a tool to characterize free groups and other related groups. Sometimes the Cayley graph of G is taken to have the elements of G as its vertices, but we make the definition more general than this.

Let G act on a set Ω (from the right) and let X be a set of generators of G. The *Cayley graph* $\Gamma(\Omega, X)$ is the graph whose vertex set is Ω and where there is an edge $\omega_1 \to \omega_2$ labeled by $x \in X$ if and only if $\omega_2 = \omega_1 x$.

Example 2.3.1. The Cayley graph of S_3 acting on $\Omega = G$ in the regular representation looks like a triangular prism. When $\Omega = \{1, 2, 3\}$ the graph has three vertices joined in a triangle with some extra edges. Also do the Cayley graph of $C_2 \times C_2$ using two generators.

Example 2.3.2. Picture of the tree for the free group of rank 2.

Proposition 2.3.3. *Let F be a group with generating set X. Then F is a free group freely generated by X if and only if $\Gamma(F, X)$ is a tree.*

Given a set X of generators of a group G we define the *length* of an element $g \in G$ (with respect to X) to be the minimal length $\ell(g)$ of a word in the $x^{\pm 1}$, $x \in X$, whose evaluation in G is g. In the case of a free group with free generators X this length is the length of the reduced word that represents the element g. In this situation, if $x \in X$ then $|\ell(gx^{\pm 1}) - \ell(g)| = 1$.

Proof. Suppose that F is freely generated by X. Each non-identity vertex $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ of $\Gamma(F, X)$ has one adjacent vertex of shorter length, namely $x_1^{\epsilon_1} \cdots x_{n-1}^{\epsilon_{n-1}}$, and all other adjacent vertices are strictly longer. If there were a circuit in the graph, consider a minimal circuit and a vertex in it of maximal length: it must have two distinct adjacent vertices of shorter length. But such adjacent vertices must be equal, which is a contradiction.

Conversely, suppose that $\Gamma(F, X)$ is a tree. Words in the generators and their inverse are in bijection with paths in the tree from the identity to vertices in the tree, and reduced words correspond to reduced paths. Since there is a unique reduced path from the identity to each vertex, each element of F has a unique expression as a reduced word and so F is freely generated by X, by Corollary 2.1.4 □

If $\Omega = G$ is the regular G-set then G acts on $\Gamma(G, X)$ from the *left* as a group of graph automorphisms, with an element $g \in G$ sending an edge $y \to yx$ to $gy \to gyx$.

Lemma 2.3.4. *Let G be a group with generating set X and let H be a subgroup of G. Then*

$$H\backslash\Gamma(G, X) \cong \Gamma(H\backslash G, X).$$

Proof. The vertices of $H\backslash\Gamma(G, X)$ are the orbits Hg of elements $g \in G$, and these are the right cosets of H. There is an edge $Hg \to Hgx$ in $\Gamma(H\backslash G, X)$ for each $x \in X$, and this corresponds to the H orbit of the edge $g \to gx$ of $\Gamma(G, X)$. □

Example 2.3.5. Let G be free of rank 2 on generators x, y and let $H = \langle x \rangle$. Draw $G\backslash\Gamma(G, X)$ and $H\backslash\Gamma(G, X)$.

Proposition 2.3.6. *Let G be a group with generating set X and let H be a subgroup of G. Schreier transversals for H in G biject with maximal rooted trees in the Cayley graph $\Gamma(H\backslash G, X)$, rooted at the subgroup H.*

Proof. This is a question of examining what these things mean. □

2.4 Covering spaces and free groups acting on trees

At this point we can borrow the theory of covering spaces from topology, for which a suitable reference is the book by J.R. Munkres: *Elements of Algebraic Topology*, Addison-Wesley 1984. For our application the topological spaces we study are all graphs (with loops and multiple edges), and so it is possible to apply this theory without the topological terms that apply generally.

Let K and $\tilde{K}$ be topological spaces. We say $p : \tilde{K} \to K$ is a *covering* if and only if each x in K has an open neighborhood U such that $p^{-1}U$ is a disjoint union of open subsets of $\tilde{K}$ each mapped homeomorphically onto U by p.

In the full topological situation, if K is connected and locally path connected, pick any base point x_0 in K. We say $p : \tilde{K} \to K$ is a *universal covering* if and only if $\pi_1(\tilde{K}, \tilde{x}_0) = 1$, where $p(\tilde{x}_0) = x_0$. When K and $\tilde{K}$ are graphs they are automatically locally path connected, and it is equivalent to require that $\tilde{K}$ be a tree.

Topologically, we say that an action of a group G on a space $\tilde{K}$ is *properly discontinuous* if and only if for all $x \in \tilde{K}$ there exists a neighborhood V of x such that $gV \cap V = \emptyset$ for all non-identity $g \in G$. When $\tilde{K}$ is a graph and G is acting by graph automorphisms, it is equivalent to require that the action be *free*, meaning that the stabilizer of every point in the tree is 1. In what follows, when G acts on a graph we will always mean that G acts via graph automorphisms. We will also require that G act *without inversions*, meaning that the setwise stabilizer of each edge fixes that edge pointwise. This condition is implied by a free action (on both vertices and edges).

Proposition 2.4.1. *Let G act freely on a graph Γ. Then the map $\Gamma \to G\backslash\Gamma$ is a covering.*

Corollary 2.4.2. *Let X be a set of generators for a group G. The action of G on the Cayley graph $\Gamma(G,X)$ is free. Hence the quotient map $p:\Gamma(G,X)\to G\backslash\Gamma(G,X)$ is a covering. If G is freely generated by X, it is a universal covering.*

Given a vertex v_0 in a graph Γ we may define the fundamental group $\pi_1(\Gamma,v_0)$ to be the set of equivalence classes of paths in Γ that start and end at v_0. Topologically, equivalence means that the paths are based homotopy equivalent, but in the case of graphs we can express the condition combinatorially: two such paths are equivalent if one can be obtained from the other by inserting and deleting a succession of paths consisting of an edge, followed by the same edge in the opposite direction. Multiplication in this group is determined by concatenation of paths. We follow the convention that the path on the left is the first path followed and the path on the right is the second. There may be the same issue ensuring associativity as with free groups.

Lemma 2.4.3. *If G acts freely on a tree Γ then $\pi_1(G\backslash\Gamma,v_0)\cong G$, where v_0 is a distinguished vertex of $G\backslash\Gamma$.*

Proof. Let $\hat{v}_0$ be a vertex in Γ with $p(\hat{v}_0)=v_0$. We obtain a mapping $G\to\pi_1(G\backslash\Gamma,v_0)$ as follows: for each $g\in G$ there is a unique (shortest) path α_g from $\hat{v}_0$ to $g\hat{v}_0$ and we send g to the homotopy class $[p(\alpha_g)]$. Given a circuit in $(G\backslash\Gamma,v_0)$ based at v_0 it has a unique lift to a path in Γ starting at $\hat{v}_0$. The end point of the path has the form $g\hat{v}_0$ for some g, and depends only on the equivalence class of the path. We send the circuit to g, and this defines a mapping $\pi_1(G\backslash\Gamma,v_0)\to G$. These two mappings are inverse and are group homomorphisms. □

We deduce the following:

Corollary 2.4.4. *Let Y be a graph with a single vertex y_0 and n loops. Then $\pi_1(Y,y_0)$ is a free group of rank n, freely generated by the paths that consist of a single edge.*

The graph in the last result is called a *wedge* of circles or, more florally, a *bouquet* of circles.

Lemma 2.4.5. *Let Y be a graph with a distinguished vertex y_0, and let T be a subtree of Y that contains every vertex. Let $\overline{Y}$ be the graph with y_0 as its only vertex, and whose edges are the edges of Y that do not lie in T. Then $\pi_1(Y,y_0)\cong\pi_1(\overline{Y},y_0)$.*

Proof. For each vertex $y\in Y$ let α_y be the geodesic from y_0 to y in T, and let α_y^{-1} denote the geodesic from y to y_0 in the opposite direction. We define a homomorphism $\pi_1(Y,y_0)\to\pi_1(\overline{Y},y_0)$ by sending each path to the same path with the edges in T omitted. In the opposite direction we define a homomorphism $\pi_1(\overline{Y},y_0)\to\pi_1(Y,y_0)$ as follows. If e is an edge of Y not in T, going from vertex x to vertex y, we replace it by the path $\alpha_x e\alpha_y^{-1}$. These homomorphisms are inverse on both sides, and hence are isomorphisms. □

Corollary 2.4.6. *Let Y be a graph with a distinguished vertex y_0.*

1. *Then $\pi_1(Y, y_0)$ is a free group of rank $-\tilde{\chi}(Y) = E - V + 1$ where E is the number of edges of Y and V is the number of vertices of Y.*

2. *Let T be a maximal subtree of Y and for each vertex y let α_y be the geodesic from y_0 to y in T. Then the elements $\alpha_v e \alpha_w^{-1}$ ranging over edges e (from v to w) that are not in T freely generate $\pi_1(Y, y_0)$.*

Proof. We know that $\pi_1(Y, y_0) \cong \pi_1(\overline{Y}, y_0)$ is free, and the rank of this free group is the number of edges of Y not in T. This number is $E - V + 1$ and the elements of $\pi_1(Y, y_0)$ that correspond to the single edges in Y_0 are free generators. These elements are the ones listed. □

Theorem 2.4.7. 1. *Let G be a group. Then G is a free group if and only if G can act freely on a tree.*

2. *Subgroups of free groups are free.*

Proof. 1. We have seen that if G is a free group then it does act freely on a tree, namely its Cayley graph. On the other hand, if G is a group that acts freely on a tree Γ then $G \cong \pi_1(G\backslash\Gamma, v_0$, which is a free group.

2. If $H \leq G$ where G is a free group, then G acts freely on a tree Γ, hence so does H. Therefore H is free, by part 1. □

We now take the last basic result and look more carefully at the generators of the subgroup H. From the theory of groups acting on trees we obtain a result that does not mention trees.

Theorem 2.4.8 (Nielsen-Schreier)**.** *Let H be a subgroup of finite index in a free group F of finite rank $d(F)$. Then $d(H) - 1 = |F : H|(d(F) - 1)$. Furthermore, H is freely generated by the non-identity elements of the form $tx\overline{tx}^{-1}$ where t ranges over the elements of a right Schreier transversal to H in F, x ranges over the generators of F, and $\overline{tx}$ is the transversal element representing the same coset as tx.*

Proof. Let $F = F(X)$ act on its Cayley graph $\Gamma(F, X)$, so that $H\backslash\Gamma(F, X)$ is the Cayley graph $\Gamma(H\backslash G, X)$, by Lemma 2.3.4. By Proposition 2.3.6 a maximal tree in $\Gamma(H\backslash G, X)$ corresponds to a Schreier transversal for H in G. The free generators for $H \cong \pi_1(\Gamma(H\backslash G, X), v_0)$ specified as $\alpha_v e \alpha_w^{-1}$ in Corollary 2.4.6 exactly correspond to elements $tx\overline{tx}^{-1}$, and such an element equals 1 if and only if the edge e lies in T. We have seen before when considering stabilizer chains that the number of these elements is as claimed, and we can now interpret this as an Euler characteristic. If E_H, V_H are the numbers of edges and vertices in the Cayley graph $H\backslash\Gamma(F, X)$ and E_F, V_F are the corresponding numbers for $F\backslash\Gamma(F, X)$ then because these are orbit graphs under a free action we have $E_H = |F : H|E_F$ and $V_H = |F : H|V_F$. Thus the Euler characteristics behave multiplicatively: $\chi(H\backslash\Gamma(F, X)) = |F : H|\chi(\backslash\Gamma(F, X))$ and this gives the subgroup rank formula by Corollary 2.4.6. □

In the above proof, one way to see which elements of G correspond to the paths $\alpha_v e \alpha_w^{-1}$ is to consider their image in $\Gamma(G\backslash G, X)$ which is a bouquet of circles corresponding to the generators of G, but we do not have to do this, because the edges of $\Gamma(H\backslash G, X)$ are labeled with elements of X.

Example 2.4.9. The normal subgroup N of $F(a,b)$ generated by $[a,b], a^2, b^2$ has quotient $C_2 \times C_2$ and the quotient $N\backslash\Gamma(F(a,b)$ is the Cayley graph $\Gamma(C_2 \times C_2, \{\bar{a}, \bar{b}\})$, which looks like (picture). We may take a Schreier transversal $\{1, a, ab, b\}$ corresponding to a maximal tree

$$\begin{tikzcd} b & ab \\ 1 \arrow[u, "b"] \arrow[r, "a"] & a \arrow[u, "b"] \end{tikzcd}.$$

Table of tg:

1	a	ab	b	
a	a^2	aba	ba	a
b	ab	ab^2	b^2	b

Table of $tg\overline{tg}^{-1}$:

1	a	ab	b	
1	a^2	$abab^{-1}$	$bab^{-1}a$	a
1	1	ab^2a^{-1}	b^2	b

The five non-identity elements in the last table freely generate N, which has rank $d(N) = 4(d(F) - 1) + 1 = 5$.

Example 2.4.10. Similar with $S_3 = \langle a, b \mid a^3, b^2, baba \rangle$.

Example 2.4.11. Similar with $Q_8 = \langle a, b \mid a^4, b^4, a^2b^{-2}, bab^3a^{-3} \rangle$.

2.5 The tree on which $SL(2,\mathbb{Z})$ acts.

Proposition 2.5.1. *$SL(2,\mathbb{Z})$ acts on $\mathbb{C}$ by Moebius transformations. The center of $SL(2,\mathbb{Z})$ is generated by $-I_2$ and acts trivially. Thus we obtain an action of $PSL(2,\mathbb{Z}) = SL(2,\mathbb{Z})/\{\pm I_2\}$ which sends circles and straight lines to circles and straight lines, preserving orthogonality. It preserves the real axis and also the upper half plane $\{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$.*

Proposition 2.5.2. *$SL(2,\mathbb{Z})$ is generated by elements*

$$\alpha = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad \beta = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$$

of orders 4 and 6 with square equal to $-I_2$.

Proposition 2.5.3. *Let e be the arc of the unit circle between i and $\omega = \frac{1+i\sqrt{3}}{2}$. Then $\mathrm{Stab}_{SL(2,\mathbb{Z})}(i) = \langle \alpha \rangle$, $\mathrm{Stab}_{SL(2,\mathbb{Z})}(\omega) = \langle \beta \rangle$ and $\mathrm{Stab}_{SL(2,\mathbb{Z})}(e) = \langle -I_2 \rangle$. The union of the images of e under the elements of $SL(2,\mathbb{Z})$ is a tree whose vertices are the images of i and ω. $SL(2,\mathbb{Z})$ acts simplicially on this tree, with fundamental domain e.*

2.6 Free products with amalgamation and $SL(2,\mathbb{Z})$

Definition 2.6.1. If $G = \langle x_i \mid r_j \rangle$ and $H = \langle y_k \mid s_l \rangle$ the *free product* of G and H is the group with presentation $G * H = \langle x_i, y_k \mid r_j, s_l \rangle$. There are group homomorphisms $\theta : G \to G * H$ and $\phi : H \to G * H$. Every element of $G * H$ can be written as a product $\theta(g_1)\phi(h_1)\cdots\theta(g_n)\phi(h_n)$ for some n, where the g_i lie in G and the h_j lie in H. If K is identified as a subgroup of G and also of H (via some injective homomorphism $\alpha : K \to H$) we define the *free product with amalgamation* $G *_K H = (G * H)/N$ where N is the normal subgroup generated by elements $\theta(y)\phi(\alpha(y))^{-1}$ as y ranges through elements of K.

Proposition 2.6.2. *There are surjective homomorphisms $C_4 *_{C_2} C_6 \to SL(2,\mathbb{Z})$ and $C_2 * C_3 \to PSL(2,\mathbb{Z})$.*

We will show that these two homomorphisms are isomorphisms.

Each element of $C_2 * C_3$ is the evaluation of a word $(g_1, h_1, g_2, h_2., \ldots)$ where $g_i \in C_2$ and $h_i \in C_3$ are non-identity elements (except that possibly $g_1 = 1$ and the identity element is the evaluation of the empty word). Define the length of such a word to be the number of non-identity elements in it. Each such word defines a simplicial automorphism of the tree, namely the automorphism given by the action of the evaluation $g_1h_1g_2h_2\ldots$.

Proposition 2.6.3. *Each word of length n in the non-identity elements of C_2 and C_3 sends e to an edge distant n from e.*

Proof. We proceed by induction on n. When $n = 0$ the result is true. Also when $n = 1$ the word sends e to an adjacent edge, joined to e at the vertex stabilized by the group element. In general, supposing that the path in the tree from e to $h_1g_2h_2\ldots(e)$ has length $n-1$ and that it starts by passing through the vertex stabilized by h_1, we see that the path in the tree from e to $g_1h_1g_2h_2\ldots(e)$ has length n and that it starts by passing through the vertex stabilized by g_1. The argument is similar whether the left term at the left of the word is in C_2 or C_3. This completes the induction step. □

Corollary 2.6.4. *The empty word is the only word whose evaluation in $PSL(2,\mathbb{Z})$ (and hence in $C_2 * C_3$) is 1. Distinct reduced words represent distinct elements of $PSL(2,\mathbb{Z})$ and of $C_2 * C_3$. The homomorphisms $C_2 * C_3 \to PSL(2,\mathbb{Z})$ and $C_4 *_{C_2} C_6 \to SL(2,\mathbb{Z})$ are isomorphisms. Each element of $SL(2,\mathbb{Z})$ can be written uniquely as plus or minus a word in α and β or β^2.*

Proof. A word which has evaluation equal to 1 must fix e and hence have length 0. If w_1 and w_2 are words of positive length which have the same evaluation in $PSL(2,\mathbb{Z})$ then the word obtained by concatenating w_1 with the inverses of terms in w_2 in the reverse order has evaluation 1 and so the terms must cancel in pairs to give the empty word. Thus $w_1 = w_2$. It follows that the surjective maps

$$\text{words} \to C_2 * C_3 \to PSL(2,\mathbb{Z})$$

are also injective and hence are isomorphisms. □

Lemma 2.6.5. *Let G be a finite group acting on a tree without exchanging the end vertices of any edge. Then G stabilizes a vertex.*

Proof. Let v be a vertex of the tree. The orbit Gv is finite, as is the smallest subtree containing all the vertices Gv. This subtree is preserved by G. If it has at most one edge, G stabilizes the subtree and hence fixes a vertex. Otherwise it has at least 2 edges. Delete all vertices of valence 1 and the incident edges. We find a smaller subtree, also stabilized by G. Repeating this procedure we eventually arrive at a subtree fixed by G. $\square$

Theorem 2.6.6. *Every torsion-free subgroup of $SL(2,\mathbb{Z})$ is free. Every finite subgroup of $SL(2,\mathbb{Z})$ is contained in a conjugate of either $\langle\alpha\rangle$ or $\langle\beta\rangle$.*

There is a surjective group homomorphism $C_4 *_{C_2} C_6 \to C_{12}$ which sends the generators of C_4 and C_6 to elements of orders 4 and 6 in C_{12}. It follows that there is also a surjective homomorphism $SL(2,\mathbb{Z}) \to C_{12}$.

Proposition 2.6.7. *The kernel K of the surjective homomorphism $SL(2,\mathbb{Z}) \to C_{12}$ acts freely on the tree of $SL(2,\mathbb{Z})$ and hence is a free group. It is free of rank 2.*

Proof. The stabilizers of vertices of the tree are the conjugates of $\langle\alpha\rangle$ and $\langle\beta\rangle$. Under the homomorphism they are mapped to the conjugates of the subgroups C_4 and C_6 of C_{12}, namely those subgroups. Thus all vertex stabilizers inject into C_{12} and hence no non-identity element of K can stabilize any vertex (or edge) of the tree. Thus K acts freely on the tree, and so is free. $\square$

2.6.1 Overview of Bass-Serre theory

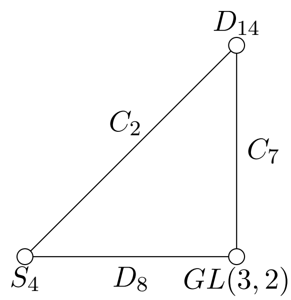
Bass-Serre theory has to do with identifying when groups have a decomposition as iterated free products with amalgamation or HNN-extensions, as well as describing the subgroup and conjugacy structure of such groups. The main theory says that a group with such a decomposition with finitely many factors can act on a tree (without inverting edges) so that stabilizers are the groups which appear in the free product or HNN extension; and, conversely, any group which acts on a tree with compact fundamental domain is an iterated free product with amalgamation or HNN extension constructed from the stabilizer groups.

Many consequences, such as the injectivity of the factors into a free product with amalgamation and the description of subgroups of a free product (the 'Kurosh subgroup theorem') were known prior to Bass-Serre theory, proved by arguments using manipulation of elements, at a time when the subject was known as 'combinatorial group theory'. A significant achievement of Bass-Serre theory was the use of group actions on trees to prove these, and other, results. As a consequence of the later contributions of Gromov in the 1980s this subject area has become part of what is known as 'geometric group theory'.

Theorem 2.6.8 (Main theorem of Bass-Serre theory)**.** *The following are equivalent for a group G.*

1. *G can act simplicially on a tree without inversions of edges, and with compact orbit space.*
2. *G is the fundamental group of a graph of groups with finitely many edges.*

A *graph of groups* is a diagram such as



where an edge $G \circ -_H \circ K$ means there are specified homomorphisms $G \leftarrow H \rightarrow K$. To construct the corresponding graph of groups we form $S_4 *_{D_8} GL(3,2) *_{C_7} *D_{14}*_{C_2}$ where the final construction is the HNN extension

$$G*_{H,\phi} = \langle G, t \mid {}^t h = \phi(h) \text{ for all } h \in H \rangle.$$