# Contents

1 Basic structures in group theory 1  
   1.1 Semidirect Products .............................. 1  
   1.1.1 Small $p$-groups ............................. 3  
   1.1.2 Wreath products .............................. 5  
   1.2 $G$-sets ........................................ 5  
   1.2.1 Stabilizer chains ............................. 7  
   1.3 Nilpotent groups ................................. 10  

2 Groups acting on trees 11
Chapter 1

Basic structures in group theory

1.1 Semidirect Products

We already know about direct products. We write \( G = K \times Q \) 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 \textit{semidirect product} of \( K \) by \( Q \), and \( Q \) is a \textit{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.
• \( S_n = A_n \rtimes C_2 \)
• \( D_{2n} = C_{2n-1} \rtimes C_2 \)
• \( C_4 \) is not a semidirect product.
• \( Q_8 \) is not a semidirect product.
• The crystallographic group of the infinite pattern

\[
\begin{align*}
&\downarrow \quad \downarrow \quad \downarrow \\
&\downarrow \quad \downarrow \quad \downarrow \\
&\downarrow \quad \downarrow \quad \downarrow 
\end{align*}
\]

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

\[
\begin{align*}
&\mid \quad \mid \quad \mid \\
&\mid \quad \mid \quad \mid \\
&\mid \quad \mid \quad \mid 
\end{align*}
\]

is not a semidirect product. The term \textit{crystallographic group} means the group of \textit{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 \(\phi\) is split epi if and only if \(G = K \times Q_1\) where \(K = \text{Ker}\ \phi\), for some subgroup \(Q_1 \leq G\) mapped isomorphically to \(Q\) by \(\phi\), if and only if \(\text{Ker}\ \phi\) 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 \(G = \text{Ker}\ \phi \times sQ\).

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

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

**Class Activity.** When \(G = S_n\) and \(K = A_n\), does \(G\) have image in \(\text{Inn} \ A_n\)?

When \(G = K \times Q\) the restriction of \(\theta\) to \(Q\) gives a mapping \(\theta : Q \to \text{Aut} \ K\). We will say that \(G\) realizes \(\theta\) in this situation.

**Example 1.1.6.** 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 1.1.7.** Let \(Q\) and \(K\) be groups and suppose we are given a homomorphism \(\theta : Q \to \text{Aut} \ K\). 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 1.1.8** (Rotman 7.22). \(K \rtimes_{\theta} Q\) is a semidirect product that realizes \(\theta\). Better: \(K \rtimes_{\theta} Q\) has subgroups \(K_1 \cong K\) and \(Q_1 \cong Q\) so that it realizes the homomorphism \(Q_1 \to Q \overset{\theta}{\to} \text{Aut} \ K \to \text{Aut} \ K_1\).

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 1.1.9 (Rotman 7.23). If \( G = K \rtimes Q \) and \( \theta : Q \to \text{Aut} K \) 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 \( \theta \) 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. \( \square \)

Exercise 1.1.10. Let \( \theta, \psi : Q \to \text{Aut} K \) be two homomorphisms and let \( \beta \in \text{Aut} K \) and \( \gamma \in \text{Aut} Q \) be automorphisms. The group \( \text{Inn} K \) of inner automorphisms of \( K \) is the group of automorphisms of the form \( \alpha(a) = bab^{-1} \) for some \( b \in K \). 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 \( \beta \in \text{Inn} K \)
4. \( \psi = \theta\gamma \) where \( \gamma \in \text{Inn} Q \)
5. for all \( x \in Q \), \( \theta(x) = \gamma\psi(x)\gamma^{-1} \)

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 1.1.11 (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 \( \text{Aut}(C_p \times C_p) = GL(2, p) \) 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 \( ^ca = a, ^cb = ab \).
1. \((C_p \times C_p) \rtimes C_p\) is isomorphic to the subgroup of \(SL(3, p)\)
\[
\begin{bmatrix}
1 & u & v \\
0 & 1 & w \\
0 & 0 & 1
\end{bmatrix} \mid u, v, w \in \mathbb{F}_p
\].

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.** Let \(G\) be the group with the presentation in 2. Then \(\langle a, b \rangle \triangleleft G\) and \(|\langle a, b \rangle| \leq p^2\), \(|\langle c \rangle| \leq p\) so \(|G| \leq p^3\). On the other hand, the semidirect product is an image of \(G\) and has order \(p^3\), so the two groups must be isomorphic. \(\square\)

**Class Activity.** 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 1.1.12.** Consider groups of the form \(C_{p^2} \rtimes C_p\) where \(p\) is a prime. Here \(\text{Aut } C_{p^2} \cong C_{p(p-1)}\) 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 \(c^2 = a^{p+1}\) 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 1.1.13.**

1. Let \(p\) be an odd prime. Every non-abelian group of order \(p^2\) 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 1.1.14 (Rotman 5.46).** Let \(G\) be a \(p\)-groups with a unique subgroup of order \(p\). Then \(G\) is cyclic or \(p = 2\) and \(G \cong Q_{2^n}\) where
\[
Q_{2^n} = \langle x, y \mid x^{2^{n-1}} = y^4 = 1, yxy^{-1} = x^{-1}, x^2 = y^2 \rangle
\]
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 subgroup of order \(p^2\) not containing it. This subgroup is normal and we obtain \(G\) as a semidirect product. Now classify the possible semidirect products as the ones we have considered. \(\square\)

**Exercise 1.1.15.** 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 1.1.16. We describe the semidihedral groups. A theorem states that
\[ \text{Aut } C_{2^n} \cong C_{2^{n-2}} \times C_2 \]
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 automorphisms
\[
\begin{align*}
x &\mapsto x \\
x &\mapsto x^{-1} \\
x &\mapsto x^{2^{n-1}-1} \\
x &\mapsto x^{2^{n-1}+1}
\end{align*}
\]
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 \( 2 \times 2 \) 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.

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 \( \Omega \) with an action of \( G \) by permutations. There are right and left G-sets and by an action of \( G \) on \( \Omega \) 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 \( \Omega \). 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 applied 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 \( \Omega \) that contains \( \omega \). We say that \( G \) acts transitively on \( \Omega \) if there is only one orbit. We put
\[
\text{Stab}_G(\omega) = G_\omega = \{ g \in G \mid \omega g = \omega \}
\]
and this is the stabilizer of \( \omega \) in \( G \). For example:

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

A homomorphism \( f : \Omega \to \Psi \) of \( G \)-sets is a mapping with \( f(\omega g) = (f(\omega))g \) always. Such a homomorphism 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 \( 1_\Psi = f f_1 \) 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.

**Proposition 1.2.1.**

1. Every \( G \)-set \( \Omega \) has a unique decomposition \( \Omega = \bigcup_{i \in I} \Omega_i \) where \( I \) is some indexing set and the \( \Omega_i \) are orbits of \( \Omega \).

2. If \( \Omega \) is a transitive \( G \)-set and \( \omega \in \Omega \) then \( \Omega \cong \text{Stab}_G(\omega) \backslash G \) as \( G \)-sets. Consequently, if \( \Omega \) is finite then \( |\Omega| = |G : \text{Stab}_G(\omega)| \).

3. 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 \( G \).

**Proposition 1.2.2.**

1. Every map between transitive \( G \)-sets is an epimorphism.

2. \( \text{Aut}_{G \text{-set}}(H \backslash G) \cong N_G(H)/H \).

3. Every homomorphism \( H \backslash G \to K \backslash G \) has the form \( H \backslash G \to J \backslash G \to K \backslash G \) where \( H \leq J \), \( H \backslash G \to J \backslash G \) is the morphism \( Hx \mapsto Jx \), and \( J \) is conjugate to \( K \).

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 1.2.3.** Let \( G \) act transitively on a set \( \Omega \) and let \( \omega \in \Omega \) be an element with stabilizer \( G_\omega \). Then elements \( \{ g_i \mid i \in I \} \) of \( G \) form a right transversal to \( G_\omega \) in \( G \) if and only if \( \Omega = \{ \omega g_i \mid i \in I \} \) and the \( \omega g_i \) 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 1.2.4. This observation provides a way to compute a transversal for \( \text{Stab}_G(\omega) \) in \( G \). Take the generators of \( G \) and repeatedly apply them to \( \omega \), obtaining various elements of the form \( \omega g_1 g_2 \cdots g_r \), where the \( g_i \) are generators of \( G \). Each time we get an element we have seen previously, we discard it. Eventually we obtain the orbit \( \omega G \), and the various elements \( g_1 g_2 \cdots g_r \) are a right transversal to \( \text{Stab}_G(\omega) \) in \( G \).

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. It is necessary to compute generators for stabilizer subgroups and this is done by the following theorem.

**Theorem 1.2.5** (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 \( \bar{g} \in T \) be such that \( Hg = H\bar{g} \). Then

\[
\{tg(\bar{g})^{-1} \mid t \in T, g \in X\}
\]

is a set of generators for \( H \).

Note that since \( Htg = H\bar{g} \), the elements \( tg(\bar{g})^{-1} \) lie in \( H \) always. Also \( \bar{a} = a \) and \( \bar{ab} = \bar{a}\bar{b} \). 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

\[
g_1 \cdots g_n = (g_1\bar{g}_1^{-1})(g_1g_2\bar{g}_2^{-1})(g_1g_2g_3\bar{g}_3^{-1})\cdots(g_1\cdots g_{n-1}\bar{g}_n^{-1})
\]

is a product of the Schreier generators. Note that \( g_1 \cdots g_n \in H \) so that \( g_1 \cdots g_n \bar{g}_n = 1 \).

If \( G \) permutes \( \Omega \), a base for \( G \) on \( \Omega \) is a list of elements \( \omega_1, \omega_2, \ldots, \omega_s \) of \( \Omega \) so that the stabilizer \( G_{\omega_1 \omega_2 \cdots \omega_s} \) equals 1. Here \( G_{\omega_1 \omega_2 \cdots \omega_r} \) is the stabilizer inside the subgroup \( G_{\omega_1 \omega_2 \cdots \omega_{r-1}} \) of \( \omega_r \), for each \( r \). Let us write \( G_r \) instead of \( G_{\omega_1 \omega_2 \cdots \omega_r} \) 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 \( \Omega_r \) of \( \Omega \) which is defined to be the \( G_r \)-orbit containing \( \omega_{r+1} \). Thus \( \Omega_0 = \omega_1G \), \( \Omega_1 = \omega_2G \) 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 1.2.6.** Each \( \Omega_i \) is acted on transitively by \( G_i \). As \( G_i \)-sets, \( \Omega_i \cong G_{i+1}\backslash G_i \).

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

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

\[
\begin{array}{cccc|c}
1 & a & b & ac & bc & bca \\
\hline
a & 1 & b & ac & bca & bc \\
b & a & 1 & bca & bc & ac \\
1 & ac & bc & a & b & bca \\
\end{array}
\]

\[
\begin{array}{cccc|c}
1 & a & b & ac & bc & bca \\
\hline
a2 & bab^{-1} & acac^{-1}a^{-1} & bc & bca^2c^{-1}b^{-1} & a \\
aba^{-1} & b^2 & acba^{-1}c^{-1}b^{-1} & bcbc & bcabc^{-1}a^{-1} & b \\
c^{-1} & 1 & ac^2a^{-1} & bc^2b^{-1} & bcaca^{-1}c^{-1}b^{-1} & c \\
\end{array}
\]
Observe that 5 of these entries are necessarily 1. Upon evaluation of these expressions in $G$ the last table becomes the following:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>a</th>
<th>b</th>
<th>ac</th>
<th>bc</th>
<th>bca</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>(2,4)(3,5)</td>
<td>(2,3)(4,5)</td>
<td>1</td>
<td>1</td>
<td>a</td>
</tr>
<tr>
<td>1</td>
<td>(2,4)(3,5)</td>
<td>1</td>
<td>acba$^{-1}c^{-1}b^{-1}$</td>
<td>(2,3)(4,5)</td>
<td>bcabc$^{-1}a^{-1}$</td>
<td>b</td>
</tr>
<tr>
<td>(2,3)(4,5)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>(2,4)(3,5)</td>
<td>c</td>
<td></td>
</tr>
</tbody>
</table>

**Class Activity.** Evaluate the remaining entries.

We see that in the stabilizer chain, $G_0$ acts on $\Omega$ 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 $|G| = 4 \cdot 6 = 24$.

**Theorem 1.2.8 (Schreier).** Let $G$ have $d$ generators and let $H \leq G$ have finite index. Then $H$ can be generated by $e$ elements, where $(e - 1) \leq |G : H|(d - 1)$.

**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 $dn - n + 1 = n(d - 1) + 1$.  

When $G$ is a free group the bound on $d(H)$ is always achieved. We will see this when we come to the section of 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 1.2.9.** 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 $\pi$ find the coset representative $x_1$ of the coset $G_1\pi$ by computing the action of $\pi$ on $\Omega$. 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 1.2.10.** Is $(1,2,3)$ in $G$? Since $(1,2,3)c^{-1}b^{-1} = (4,5,6) \not\in G_1$, the answer is No.

**Class Activity.** Is $(1,3,5)(2,6,4)$ in $G$?

**Algorithm 1.2.11.** 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

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

Groups acting on trees