
If two geometric braids are isotopic in $D^2 \times [0,1]$, then there exists an isotopy through the family of braids bringing one to the other. ("Isotopy and s-isotopy imply each other")

Continuing from the last time: we saw two definitions of the braid group. Now we see that they coincide.

THEOREM (Fox - Neuwirth, '62)

$$B_n(\Sigma) \cong B^{\text{geom}}_n(\Sigma)$$

**Sketch of proof**

Let $\ell$ be a closed path in $F_n(\Sigma)$ based at $x$.

We can send it to a geometric braid $\beta(\ell)$ defined by:

- $k \in \{1, \ldots, n\}$
  $$\beta_k(t) : = (k\text{-th coord. of } \ell(t), t)$$
- $t \in [0,1]$

This defines a map

$$[\ell] \quad \mapsto \quad [\beta(\ell)]$$

The map:
- is well defined;
- respects multiplication;
- is bijective.
Then $PB_n(\Sigma) \cong PB_n^{geom}(\Sigma)$. Consider the diagram with exact rows:

$$
\begin{array}{c}
1 \rightarrow PB_n(\Sigma) \rightarrow B_n(\Sigma) \rightarrow S_n \rightarrow 1 \\
\downarrow \quad \quad \quad \downarrow \\
1 \rightarrow PB_n^{geom}(\Sigma) \rightarrow B_n^{geom}(\Sigma) \rightarrow S_n \rightarrow 1
\end{array}
$$

Five-Lemma $\Rightarrow B_n(\Sigma) \cong B_n^{geom}(\Sigma)$. □

One of the most useful tools we have when dealing with braid groups are: finite presentations!

Here we will focus on the case $\Sigma = D^2$, the 2-disc. For general oriented surfaces, see: “On presentations of surface braid groups by Bellinoeri. For non-orientable surfaces: “The lower central and derived series of the braid groups of compact surfaces” by Guaschi and De Miranda e Pereiro.

Before getting to the point, let us review the following method, which is a basic ingredient in finding presentations of braid groups. A very clear exposition can be found in Chapter 10 of “Presentations of groups” by Johnson.

**LEMMA** Consider a short exact sequence of groups:

$$
\begin{array}{c}
1 \rightarrow S \xrightarrow{i} G \xrightarrow{p} Q \rightarrow 1
\end{array}
$$

where $S = \langle A \mid B \rangle$ and $Q = \langle X \mid Y \rangle$.

Let $F(X)$ be the free group generated by the set $X$, and $t: F(X) \rightarrow G$ a homomorphism such that $pt(x) = x \in Q, \forall x \in X$.

For every $y$, let $w_y$ be a word in $A$ s.t. $i(w_y) = t(y) \in G$.

Then $G$ admits a presentation given by:

$$
\langle A \cup X \mid B \cup \{w_yy^{-1} | y \in Y\} \cup \{v_{x,a}xa^{-1}x^{-1} | a \in A, x \in X\} \rangle.
$$

Remark that when the sequence is split, you can take $t$ to be a right section $s$ ($p \circ s = id_Q$), and $w_y$ can be taken to be the empty word $\varepsilon_Y$.

**THEOREM** (Artin, 1925) $\Sigma = D^2$

The braid group admits the following presentation

$$
\langle \sigma_1, \ldots, \sigma_{n-1}, \sigma_n | \sigma_i \sigma_j = \sigma_j \sigma_i, \quad |i-j| > 2 \rangle.
$$
Many proofs can be found in the literature. We sketch here one that relies on the short exact sequence
\[ 1 \to PB_n \to B_n \to S_n \to 1 \]
merging a presentation of \( PB_n \) with a presentation of \( S_n \).

**Remark** For another finite presentation of \( B_n \), see:
"A new approach to the word and conjugacy problems in the braid groups" by Birman- Ko- Lee.

**Idea of the proof**

- Define a "forgetting homomorphism
  \[ p: PB_{n+1} \to PB_n \]
  forgetting the last strand,
and a homomorphism
  \[ i: \pi_1 \left( D^2 \setminus \{x_1, \ldots, x_n\} \right) \to PB_{n+1} \]
sending the homotopy class of a closed path \( \alpha \) to the isotopy class of a braid by
  \[
  \begin{align*}
  (k, t) &\mapsto (x_k, t) \quad \text{for } k \leq n \\
  (n+1, t) &\mapsto (\alpha(t), t)
  \end{align*}
  \]

\[ \text{SPLIT S.E.S.} \]

The sequence
\[ 1 \to \pi_1 \left( D^2 \setminus \{x_1, \ldots, x_n\} \right) \to PB_{n+1} \overset{p}{\to} PB_n \to 1 \]
is exact and split.

A proof of this consists in:
- observing that \( p \) is the homom. induced by
  \[ F_{n+1}(D^2) \to F_n(D^2) \]
  \[ (z_1, \ldots, z_{n+1}) \to (z_1, \ldots, z_n) \]
and that this has a right inverse \( s: F_n(D^2) \to F_{n+1}(D^2) \)
  \[ (x_1, \ldots, x_n, z) \to (x_1, \ldots, x_n, \sqrt{\max(|z_1|^2, |z_2|^2)}) \]
- observe that \( i \) is induced by
  \[ D^2 \setminus \{x_1, \ldots, x_n\} \to F_{n+1}(D^2) \]
  \[ (x_1, \ldots, x_n, z) \to (x_1, \ldots, x_n, z) \]
- prove that \( p \) is a fibre bundle with fibre
  \[ D^2 \setminus \{x_1, \ldots, x_n\} \].
• The symmetric groups \( S_n \) admit presentations:
\[
\left\langle \rho_1, \ldots, \rho_{n-1} \mid \rho_i^2 = 1, \rho_i \rho_j = \rho_j \rho_i, \rho_i \rho_{i+1} \rho_i = \rho_{i+1} \rho_i \rho_{i+1}, \rho_i \rho_{j+1} \rho_i = \rho_{j+1} \rho_i \rho_{j+1} \right\rangle
\]
(Moore, 1897)

• \( \text{PB}_2 \cong \mathbb{Z} \) (\( \mathbb{P}_2(\mathbb{S}^2) \cong \mathbb{Z} \)) \( \pi_1(\mathbb{P}_2(\mathbb{S}^2), x) \cong \pi_1(\mathbb{S}^2, x) \cong \mathbb{Z} \).

• Using the short exact sequence * to merge presentations + induction on \( n \), obtain presentations for groups \( \text{PB}_n \).

• Merge presentations of \( \text{PB}_n \) and \( S_n \) through the s.e.s.
\[
1 \rightarrow \text{PB}_n \rightarrow B_n \rightarrow S_n \rightarrow 1
\]
(\( \text{attached to these notes, Johnson's Chapter 10} \))

1.3 Braids as mapping classes an Artin's representation

\( \Sigma \) connected, orientable, compact surface with \( x_1, \ldots, x_n \) marked pts.
Fix an orientation on \( \Sigma \).

\[
\text{Homeo}^+(\Sigma, \{x\}) = \begin{cases} f : \Sigma \rightarrow \Sigma \text{ orientation preserving homeos s. that:} & \\
1. \forall p \in \Sigma, f(p) = p ; \\
2. f(\{x\}) = \{x\} . & 
\end{cases}
\]

\[
\text{Homeo}^+(\Sigma, x) = \begin{cases} f : \Sigma \rightarrow \Sigma \text{ orientation preserving homeos s. that:} & \\
1. \forall p \in \Sigma, f(p) = p ; \\
2. \forall i \in \{1, \ldots, n\}, f(x_i) = x_i . & 
\end{cases}
\]

With the usual composition of homeos, these sets admit group structures. Moreover, equipped with the compact-open
they are topological groups.

\[ V(K,U) = \{ f \in \text{Homeo}^+(\Sigma) : f(K) \subset U \} \]

**Def.** The mapping class group of \( \Sigma \) with marked points \( x_1, \ldots, x_n \) is

\[ \text{Mod} \left( \Sigma, \{x_1\} \right) = \pi_0 \left( \text{Homeo}^+ \left( \Sigma, \{x_1\} \right) \right) \]

and

the pure mapping class group of \( \Sigma \) with marked points \( x_1, \ldots, x_n \) is

\[ \text{PMod} \left( \Sigma, \{x_1\} \right) = \pi_0 \left( \text{Homeo}^+ \left( \Sigma, \{x_1\} \right) \right) \]

**Remark:** The definition of mapping class groups admits several variations.

- Let \( \text{Homeo}_0^+ \left( \Sigma, \{x_1\} \right) \) be the connected component of \( \text{id}_\Sigma \) in \( \text{Homeo}^+ \left( \Sigma, \{x_1\} \right) \).

  Then

  \[ \text{Mod} \left( \Sigma, \{x_1\} \right) \cong \frac{\text{Homeo}^+ \left( \Sigma, \{x_1\} \right)}{\text{Homeo}_0^+ \left( \Sigma, \{x_1\} \right)} \]

- A continuous map \( \rho : [0,1] \to \text{Homeo}^+ \left( \Sigma, \{x_1\} \right) \) (with compact-open topology) is the same as an isotopy relative to \( \partial \Sigma \) between \( \rho(0) \) and \( \rho(1) \).

Recall that two homeomorphisms \( f, f' : \Sigma \to \Sigma \) are isotopic if there is a homotopy

\[ H : \Sigma \times [0,1] \to \Sigma \]

such that

\[ H(-, t) \] is a homeo \( \forall t \in [0,1] \).

Two homeos \( f, f' : \Sigma \to \Sigma \) that \( f \times \partial \Sigma \) are isotopic relative to \( \partial \Sigma \) if they are related by an isotopy

\[ H : \Sigma \times [0,1] \to \Sigma \]

such that

\[ H(-, t) \] fixes \( \partial \Sigma \) \( \forall t \in [0,1] \).
Then \( \text{Mod} \left( \Sigma, \{x\} \right) \cong \text{Homeo}^+ \left( \Sigma, \{x\} \right) \) 
\(_{\text{isotopy rel } \partial \Sigma} \)

- A result of Baer (1928) and Epstein (1966) states that: two orientation preserving homeomorphisms \( \Sigma \to \Sigma \) are homotopic (rel \( \partial \Sigma \)) if and only if they are isotopic (rel \( \partial \Sigma \)).

So we can consider homeos up to homotopy instead of isotopy.

- It is sometimes convenient to work with homeos and sometimes with diffeos. The following theorem allows us to go back and forth:

  \[ \text{THEOREM } \Sigma \text{ compact surface. Then every homeomorphism of } \Sigma \text{ is isotopic to a homeomorphism of } \Sigma. \]

This was proved independently by Munkres, Smale, and Whitehead in the '50.

So we have

\[
\text{Mod} \left( \Sigma, \{x\} \right) \cong \pi_0 \left( \text{Diff}^+ \left( \Sigma, \{x\} \right) \right) \\
\cong \text{Diff}^+ \left( \Sigma, \{x\} \right) \\
\cong \text{Diff}^\circ \left( \Sigma, \{x\} \right) \\
\cong \text{Diff} \left( \Sigma, \{x\} \right) \\
\cong \text{Diff}^\circ \left( \Sigma, \{x\} \right) \\
\]

This remark concerns general mapping class groups of surfaces. More details in Chapter 1.4, "A primer on mapping class groups".

For any \( [f] \in \text{Mod} \left( \Sigma, \{x\} \right) \) denote by \( s([f]) \in S_n \) the unique permutation such that

\[ f(x_i) = x_{s([f])(i)} \text{ for all } i \in \{1, \ldots, n\}. \]

Then, we have the following short exact sequence:

\[ \mathbb{1} \to \text{PMod} \left( \Sigma, \{x\} \right) \to \text{Mod} \left( \Sigma, \{x\} \right) \to S_n \to \mathbb{1} \]

This is a brick in a result that relates braid groups to mapping class groups.
Theorem (Birman, Corollary 14 "Mapping class groups and their relationship to Braid Groups", 1969)

The following diagram is commutative with exact rows and columns:

\[
\begin{array}{cccccc}
\pi_1(\text{Homeo}^+(\Sigma)) & \longrightarrow & \text{PB}_n(\Sigma) & \longrightarrow & \text{PMod}(\Sigma, x) & \longrightarrow & \text{Mod}(\Sigma) & \longrightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
\pi_1(\text{Homeo}^0(\Sigma)) & \longrightarrow & \text{B}_n(\Sigma) & \longrightarrow & \text{Mod}(\Sigma, \{x\}) & \longrightarrow & \text{Mod}(\Sigma) & \longrightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
\text{S}_n & & \text{S}_n & & \text{S}_n & & \text{S}_n & & \text{S}_n \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & & 1 & & 1 & & 1 & & 1 \\
\end{array}
\]

Exercise: Show that, when $\Sigma = D^2$,

\[
\text{B}_n \cong \text{Mod}(D^2, \{x, 1\})
\]

(Hint: look up "Alexander's trick")
1. Basic concepts

Definition 1. An extension of a group \( G \) by a group \( A \) is a group \( \tilde{G} \) having a normal subgroup \( N \) such that

\[
A \trianglelefteq N, \quad \tilde{G}/N \cong G.
\]

1. (i) given a normal embedding

\[
i : A \rightarrow \tilde{G},
\]

that is, \( i \) is a monomorphism with \( \text{Im} i \trianglelefteq \tilde{G} \), \( \tilde{G} \) is an extension of \( \tilde{G}/\text{Im} i \) by \( A \);

(ii) given an epimorphism

\[
v : \tilde{G} \twoheadrightarrow G,
\]

\( \tilde{G} \) is an extension of \( G \) by \( \text{Ker} v \).

For our purposes, the best way to picture a group extension is as follows. Name the isomorphisms (1) \( \alpha, \beta \), respectively, and let \( i, v \) denote the composites

\[
\begin{align*}
A & \rightarrow N \rightarrow \tilde{G}, \\
\tilde{G} & \rightarrow \tilde{G}/N \rightarrow G,
\end{align*}
\]

respectively. Then we have a diagram

\[
A \overset{i}{\rightarrow} \tilde{G} \overset{v}{\rightarrow} G,
\]

(2)
where the maps satisfy:

\[ \text{Ker } \tau = E, \quad \text{Im } \tau = \text{Ker } \nu, \quad \text{Im } \nu = G. \quad (3) \]

This prompts the following definition, which will be useful later in another setting.

**Definition 2.** A sequence

\[ A_0 \xrightarrow{\alpha_0} A_1 \xrightarrow{\alpha_1} A_2 \xrightarrow{} \ldots \xrightarrow{} A_{n-1} \xrightarrow{\alpha_{n-1}} A_n \quad (4) \]

of groups and homomorphisms is called **exact** if

\[ \text{Im } \alpha_{i-1} = \text{Ker } \alpha_i, \quad 1 \leq i \leq n - 1. \]

In the case when \( A_0 \) and \( A_n \) are both trivial and \( n = 4 \), (4) is called a **short exact sequence** (of groups).

In deference to tradition, we denote the trivial group by \( 1 \), rather than \( E \), in this context, and so write a short exact sequence in the form

\[ 1 \xrightarrow{\alpha_1} A_1 \xrightarrow{\alpha_2} A_2 \xrightarrow{} A_3 \xrightarrow{} 1, \]

where \( \alpha_0 \) and \( \alpha_3 \), being trivial, have been suppressed. The conditions of exactness at \( A_1 \), \( A_2 \), \( A_3 \) respectively assert that

\[ \text{Ker } \alpha_1 = 1, \quad \text{Im } \alpha_1 = \text{Ker } \alpha_2, \quad \text{Im } \alpha_2 = A_3, \]

which is a restatement of (3). The notions of group extension and short exact sequence of groups are thus **the same**, and we think of an extension as an exact sequence

\[ 1 \to A \xrightarrow{\iota} \widetilde{G} \xrightarrow{\nu} G \to 1. \]

The above ideas form the starting point for (algebraic) homology theory. While we shall not develop this further than we need it (which is not very far), it involves one other simple notion. This we now define (cf. Fig. 1.1) and illustrate by a pretty little lemma.

**Definition 3.** A **diagram** is a directed graph whose vertices are groups and whose edges are homomorphisms between their endpoints. Such a diagram is called **commutative** if, given any two vertices and any two paths between them, the corresponding composite homomorphisms are equal.
Lemma 1 (The five-lemma). Let

\[
\begin{array}{cccccc}
A_0 & \xrightarrow{\alpha_0} & A_1 & \xrightarrow{\alpha_1} & A_2 & \xrightarrow{\alpha_2} & A_3 & \xrightarrow{\alpha_3} & A_4 \\
\downarrow{\phi_0} & & \downarrow{\phi_1} & & \downarrow{\phi_2} & & \downarrow{\phi_3} & & \downarrow{\phi_4} \\
B_0 & \xrightarrow{\beta_0} & B_1 & \xrightarrow{\beta_1} & B_2 & \xrightarrow{\beta_2} & B_3 & \xrightarrow{\beta_3} & B_4
\end{array}
\]

be a commutative diagram with exact rows. If \(\phi_0, \phi_1, \phi_3, \phi_4\) are isomorphisms, then so is \(\phi_2\).

Proof. The proof is by "diagram-chasing", and is easier to see than to write down. We merely give the justification of the successive steps, abbreviating the hypotheses to statements like \(EA_2\) (exactness at \(A_2\)) and \(C3\) (commutativity of the third square from the left).

First, let \(a \in \text{Ker} \phi_2\), so that \(a\phi_2\beta_2 = 1\). Then apply

\[
C3, \phi_3 1 - 1, EA_2, C2, EB_1, \phi_0 \text{ onto, } C1, \phi_1 1 - 1, EA_1
\]

in turn to deduce that \(a = 1\). Hence, \(\phi_2\) is one-to-one. Next, let \(b \in B_2\), so that \(b\beta_2 \in B_3\).

Then use \(\phi_3\) onto, \(EB_3, C4, \phi_4 1 - 1, EA_3, C3, EB_2, \phi_1 \text{ onto, } C2\) in turn to deduce that \(b \in \text{Im} \phi_2\). Hence, \(\phi_2\) is onto.

2. The main theorem

Suppose we are given an extension

\[
1 \to A \overset{\iota}{\to} \tilde{G} \overset{\nu}{\to} G \to 1
\]

and presentations

\[
G = \langle X \mid R \rangle, \ A = \langle Y \mid S \rangle
\]

for \(G\) and \(A\). Our aim is to put together a presentation for \(\tilde{G}\).

First, let

\[
\tilde{Y} = \{\tilde{y} = y \mid y \in Y\}
\]

and let

\[
\tilde{S} = \{\tilde{s} \mid s \in S\}
\]
be the set of words in \( \bar{Y} \) obtained from \( S \) by replacing each \( y \) by \( \bar{y} \) wherever it appears.

Next, let

\[ \bar{X} = \{ \bar{x} \mid x \in X \} \]

be members of a transversal for \( \text{Im } t \) in \( \bar{G} \) such that \( \bar{x}v = x \) for all \( x \in X \). Furthermore, for each \( r \in R \), let \( \bar{r} \) be the word in \( \bar{X} \) obtained from \( r \) by replacing each \( x \) by \( \bar{x} \). Now \( v \) annihilates each \( \bar{r} \), and so for all \( r \in R, \bar{r} \in \text{Ker } v = \text{Im } t \) and since \( \text{Im } t \) is generated by the set \( \bar{Y} \), each \( \bar{r} \) can be written as a word - say \( v_r \) - in the \( \bar{y} \). We put

\[ \bar{R} = \{ \bar{r}v_r^{-1} \mid r \in R \} \]

Finally, since \( \text{Im } t \triangleleft G \), each conjugate \( \bar{x}^{-1} \bar{y} \bar{x}, \bar{x} \in \bar{X}, \bar{y} \in \bar{Y} \), belongs to \( \text{Im } t \), and so is a word - \( w_{x,y} \) say - in the \( \bar{y} \). Putting

\[ \bar{T} = \{ \bar{x}^{-1} \bar{y} \bar{x} w_{x,y}^{-1} \mid x \in X, y \in Y \} \]

we have the following result.

**Proposition 1.** With the above notation, the group \( \bar{G} \) has a presentation

\[ <\bar{X}, \bar{Y} \mid \bar{R}, \bar{S}, \bar{T}> \] \hspace{1cm} (7)

**Proof.** Letting \( D \) be the group presented by (7), it follows from the fact that all the relations in (7) hold in \( \bar{G} \) that there is a homomorphism

\[
\begin{align*}
\theta : D & \rightarrow \bar{G} \\
\bar{x} & \mapsto \bar{x} \\
\bar{y} & \mapsto \bar{y}
\end{align*}
\]

by the substitution test. The restriction of \( \theta \) to the subgroup \( <\bar{Y}> \) of \( D \) gives rise to a homomorphism

\[
\begin{align*}
\theta_1 : <\bar{Y}> & \rightarrow \text{Im } t \cong A \\
\bar{y} & \mapsto y
\end{align*}
\]

and since the defining relations \( S \) of \( A \) (with each \( y \) replaced by \( \bar{y} \)) all hold in \( <\bar{Y}> \leq D, \theta_1 \) must be a bijection. Now the presence of the relations \( \bar{T} \) in (7) means that \( <\bar{Y}> \) is a normal
subgroup of \( D \), and since \( \langle \tilde{Y} \rangle \) induces a homomorphism

\[
\begin{align*}
\theta_2 : D / \langle \tilde{Y} \rangle & \rightarrow \tilde{G} / \text{Im} \ t \cong G \\
\langle \tilde{Y} \rangle \tilde{x} & \mapsto x
\end{align*}
\]

Now the relations \( R \) defining \( G \) all hold (with \( x \) replaced by \( \langle \tilde{Y} \rangle \tilde{x} \)) in \( D / \langle \tilde{Y} \rangle \), so \( \theta_2 \) must be a bijection. We thus have a commutative diagram

\[
\begin{array}{cccccc}
1 & \rightarrow & A & \xrightarrow{\imath} & \tilde{G} & \xrightarrow{\nu} & G & \rightarrow & 1 \\
\theta_1 & \uparrow & \theta & \uparrow & \theta_2 & \uparrow \\
1 & \rightarrow & \langle \tilde{Y} \rangle & \xrightarrow{\text{inc}} & D & \xrightarrow{\text{nat}} & D / \langle \tilde{Y} \rangle & \rightarrow & 1
\end{array}
\]

with exact rows. Since \( \theta_1 \) and \( \theta_2 \) are isomorphisms, it follows from Lemma 1 that \( \theta \) also is an isomorphism. This proves the theorem.

**Corollary 1.** Let \( G = \langle X \mid R \rangle \) and \( A = \langle Y \mid S \rangle \) be groups, and \( \alpha : G \rightarrow \text{Aut} \ A \) a homomorphism such that \( y(x\alpha) = w_{x,y} \), a word in \( Y^k \) (\( x \in X, y \in Y \)). Then the semi-direct product \( A \rtimes G \) has the presentation

\[
A \rtimes G = \langle X, Y \mid R, S, \{ x^{-1} y x w_{x,y}^{-1} \mid x \in X, y \in Y \} \rangle.
\]

**Proof.** Merely apply the theorem to the group \( K = A \rtimes G \) of Definition (5.1), taking \( \tilde{y} = (e,y), \tilde{x} = (x,e) \). Then the \( \nu_r \) in (7) are all trivial, and removing all the tildas from (7) gives the result, by (5.6).

**Corollary 2.** Let \( \tilde{G} \) be an extension of \( G \) by \( A \). If \( G \) and \( A \) are finitely presented, then so is \( \tilde{G} \).

**Proof.** Let \( \tilde{G}, G, A \) be as in (5), (6) with \( |X|, |R|, |Y|, |S| \) all finite. Then (7) is a presentation of \( \tilde{G} \) having

\[
|X| + |Y|, \quad |R| + |S| + |X| \quad |Y|
\]
generators, relators, respectively. Hence, \( \tilde{G} \) is finitely presented.
10.3 Special cases

Corollary 3. Let $H$ be a subgroup of finite index in a group $G$. If $H$ is finitely presented, then so is $G$.

Proof. This is a consequence of Corollary 2 and Corollary 9.1 (of which it is the converse!) as $H$ is of finite index, it has only finitely many conjugates. Since each of these is of finite index, so is their intersection, call it $N$. Then $N$ is a subgroup of finite index in $H$, and so is finitely presented (Corollary 9.1), and $G/N$ is finite, and so is finitely presented (Proposition 4.1). Then $G$, being an extension of $G/N$ by $N$, is finitely presented (Corollary 1).

3. Special cases

As remarked above, the idea of a group extension is a very general one. There are four particularly favourable (and useful) special cases and we now discuss these in turn, all with reference to the extension (5) and its presentation (7).

(S) Semi-direct products

This is the case when $N := \text{Im} \ i$ has a complement, call it $C$, in $\tilde{G}$, that is, a subgroup $C \leq \tilde{G}$ such that

$$\tilde{G} = NC, \quad N \cap C = 1$$

(8)

(cf. formula (5.9)), so that $\tilde{G}$ is a semi-direct product $A \rtimes C$. Because of (8), the elements of $C$ form a right transversal for $N$ in $G$, and it follows that the restriction $\nu \mid_C$ is an isomorphism. There is thus a homomorphism $\sigma$

$$G \to C \to \tilde{G}$$

with the property that $\nu \sigma = 1_G$ (such a $\sigma$ is called a splitting for (5)). Conversely, if (5) is split by $\sigma : G \to \tilde{G}$ (i.e. $\sigma$ is a homomorphism such that $\sigma \nu = 1_G$), then $\text{Im} \ \sigma$ is clearly a complement for $N$ in $\tilde{G}$. It follows that a semi-direct product is nothing other than a split extension.

In the case when (5) is split, by $\sigma$ say, we can choose the generators $\tilde{X}$ in the proof of Theorem 1 to be \{x \sigma \mid x \in X\}. Then for each $r \in R$, we have $\tilde{r} = r \sigma = e$, and in $\tilde{R}$, all the $\nu_r$ are equal to $e$. Split extensions of $G$ by $A$ are thus parametrized by the $w_{x,y}$, $x \in X$, $y \in Y$, alone. The automorphism $\alpha$ defining the corresponding semi-direct product $A \rtimes G$ is then given by
\[ \alpha: G \longrightarrow \text{Aut } A \]
\[ x \longmapsto \begin{cases} A \longrightarrow A \\ y \mapsto w_{x,y} \end{cases} \] \tag{9}

N.B. Starting from presentations (6) and a homomorphism (9), the presentation (7), with every \( v_r = e \), always defines an extension of \( G \) by \( A \) (see Corollary 1). Unfortunately, there appears to be no satisfactory analogue of this in the non-split case.

(A) Extensions with abelian kernel

\( A \) is often called the kernel of the extension (5). Since \( A \triangleleft \tilde{G} \), there is a homomorphism

\[ \gamma: \tilde{G} \rightarrow \text{Aut } A \] \tag{10}

induced by conjugation. Thus the map \( \gamma: A \rightarrow \text{Aut } A \) is that induced by conjugation within \( A \), and so is trivial if and only if \( A \) is abelian. In this case, \( \gamma \) induces (in the sense of Lemma 4.1) a homomorphism \( \alpha: G \rightarrow \text{Aut } A \), as in §5.4. Because of (5.7), this makes \( A \) into a \( G \)-module in the following sense.

Definition 4. Given a (multiplicatively-written) group \( G \), a (right) \( G \)-module is an (additively-written) abelian group \( A \) together with an action of \( G \) on \( A \) (on the right) such that the following axioms hold:

\[ \begin{aligned}
(a + b)g &= a + bg \\
ag(gh) &= (ag)h \\
ae &= a
\end{aligned} \] \tag{11}

In this case, there is a satisfactory theory of extensions of \( G \) by \( A \) (in which conjugation induces the given \( G \)-action). Such extensions are classified up to equivalence by the elements of the second cohomology group \( H^2(G,A) \). Further discussion of this is beyond our scope, although the notion of \( G \)-module will be useful later.

(Z) Central extensions

This is the case when \( N = \text{Im } \iota \) is contained in the centre of \( \tilde{G} \). Thus, not only is \( A \) abelian, but the homomorphism \( \gamma \) of (10) is trivial. When this is so, the \( w_{x,y} \) appearing in the relators \( \tilde{T} \) of (7) are as simple as possible, i.e., \( w_{x,y} = x \) for all \( x \in X, y \in Y \). Central extensions are thus parametrized by the \( v_r, r \in R \), alone. In other words, \( G \) is determined
by \(|R|\) choices from a set with \(|A|\) elements, and we have the following lemma.

**Lemma 2.** The total number of central extensions of a group \(G = \langle X \mid R \rangle\) by a group \(A\) is at most \(|A| \cdot |R|\).

(D) **The direct product**

Suppose the \(v_i\) in (7) are all equal to \(e\) and the \(w_{x,y}\) to \(x\). Then (7) reduces to the presentation (4.3) of the direct product \(A \times G\). It is not hard to check that this happens if and only if there is a homomorphism \(\tau: \tilde{G} \to A\) such that \(\tau \tau = 1_A\) (cf. the situation with \(\sigma\) in case (S)).

4. **Finite \(p\)-groups**

**Definition 5.** A \(p\)-group is a group whose every element has order a power of \(p\), where \(p\) is understood to be a prime. Let \(G\) be a non-trivial finite \(p\)-group. Then it follows from our present purpose, which is to apply the above ideas to finite \(p\)-groups to give rather crude estimates for a) their deficiency, and b) their number.

**Lemma 3.** Every non-trivial finite \(p\)-group has a central subgroup of order \(p\).

Further properties of finite \(p\)-groups will be developed later, but this is all we need for the moment, which is to apply the above ideas to finite \(p\)-groups to give rather crude estimates for a) their deficiency, and b) their number.

**Proposition 2.** Let \(G\) be a group of order \(p^n\), \(p \in \mathbb{P}, n \in \mathbb{N}\). Then \(G\) has a presentation on \(n\) generators with \(n(n + 1)/2\) defining relations.

**Proof.** The proof is by induction on \(n\). When \(n = 1\),

\[ G \cong Z_p = \langle x \mid x^p \rangle, \]

and the result is obvious. Let \(n > 1\) and assume the result for groups of order \(p^{n-1}\). By Lemma 3, \(G\) has a central subgroup, \(N\) say, of order \(p\), and is thus a central extension

\[ 1 \to N \to G \to G/N \to 1. \tag{12} \]