# Notes on Group Theory

Mark Reeder

August 20, 2019

## Contents

# 1 Notation for sets and functions

For any set $S$, we write $|S|$ for the number of elements in $S$ if $S$ is finite, and put $|S| = \infty$ if $S$ is infinite. The empty set is denoted $S = \varnothing$.

If $f : S \to T$ is a function, we write $f(s)$ or $f_s$ for the value of $f$ at an element $s \in S$. The set $\operatorname{im} f = f(S) = \{f(s) : s \in S\}$ of these values is the image of $f$ and $f^{-1}(t) = \{s \in S : f(s) = t\}$ is the fiber of $f$ over an element $t \in T$. Thus, $\operatorname{im} f = \{t \in T : f^{-1}(t) \neq \varnothing\}$. For any subset $T' \subset T$, the set $f^{-1}(T') = \{s \in S : f(s) \in T'\}$ is the union of the fibers $f^{-1}(t)$ for $t \in T'$.

A function $f : S \to T$ is injective if $|f^{-1}(t)| \leq 1$ for all $t \in T$, in this case we sometimes write

$f : S \hookrightarrow T$ to emphasize injectivity, and to indicate that we may identify $S$ with its image in $T$.

A function $f : S \to T$ is surjective if $|f^{-1}(t)| \geq 1$ for all $t \in T$, in this case we sometimes write $f : S \twoheadrightarrow T$ to emphasize surjectivity.

Finally, $f$ is bijective if it is both injective and surjective, that is, if $|f^{-1}(t)| = 1$ for all $t \in T$. When this holds, we have $|S| = |T|$. We sometimes write $f : S \xrightarrow{\sim} T$ to indicate a bijection, or $S \leftrightarrow T$ to mean that there exists a bijection between $S$ and $T$.

# 2 Basic group theory

## 2.1 The definition of a group

A **group** is a set $G$ together with a function $* : G \times G \to G$, assigning to each pair $(a, b)$ of elements of $G$ another element $a * b \in G$, satisfying the following three axioms:

G1 (*associativity*) We have $a * (b * c) = (a * b) * c$, for all $a, b, c \in G$.

G2 (*existence of identity*) There exists an element $e \in G$ such that $e * a = a * e = a$ for all $a \in G$.

G3 (*existence of inverses*) For all $a \in G$ there exists an element $a' \in G$ such that $a * a' = a' * a = e$, where $e$ is an identity element as in axiom G2.

There is no requirement that $a * b = b * a$ for all $a, b \in G$. If this property does hold, we say that $G$ is *abelian*.

The element $e$ of axiom G2 is unique: for if $e'$ is another identity element, then $e' = e' * e = e$ by applying axiom G2 first to $e$, then to $e'$. For each $a \in G$, the inverse element $a'$ in axiom G3 is unique: for if $a''$ is another inverse element, we have

$$a'' = a'' * e = a'' * (a * a') = (a'' * a) * a' = e * a' = a',$$

by applying successively axioms G2, G3 (for $a'$), G1, G3 (for $a''$) and finally G2 again.

We usually use multiplicative notation and abbreviate $a * b$ as $ab$ or $a \cdot b$, and write $1$ or $1_G$ instead of $e$ for the identity element of $G$, and $a^{-1}$ instead of $a'$ for the inverse element of $a$. For any positive integer $n$, we write $a^n$ for the product of $a$ with itself $n$ times, and $a^{-n}$ for the product of $a^{-1}$ with itself $n$ times. Finally, we put $a^0 = 1$.

If $G$ is abelian, and only in this case, we sometimes use additive notation, writing $a*b = a+b$, denoting the identity element by $0$, and the inverse element of $a$ by $-a$.

The **order of** $G$ is the cardinality $|G|$, either a positive integer or $\infty$. Any group $G$ of order one consists of the identity element only and is called the *trivial group*.

We can extend the product of elements in $G$ to subsets: If $S$ and $T$ are subsets of a group $G$, we define

$$ST = \{st : \ s \in S, t \in T\}.$$

## 2.2 Group homomorphisms

The structure of a group $G$ is revealed by its subgroups and homomorphisms into other groups.

A **homomorphism** of groups $G, G'$ is a function $f : G \to G'$ satisfying

$$f(ab) = f(a)f(b) \qquad \forall\, a, b \in G.$$

This implies that $f(1_G) = 1_{G'}$ and that $f(g^{-1}) = f(g)^{-1}$ for all $g \in G$.

The **kernel** of a homomorphism $f : G \to G'$ is the subset of $G$ defined by

$$\ker f := \{g \in G :\ f(g) = 1_{G'}\}.$$

For all $a, b \in G$ we have $f(a) = f(b)$ if and only if $ab^{-1} \in \ker f$. Hence $f$ is injective iff $\ker f = \{1_G\}$. The **image** of $f$ is the set theoretic image, defined as above by

$$\operatorname{im} f := f(G) = \{g' \in G :\ f^{-1}(g') \neq \varnothing\}.$$

There may be many homomorphisms between two given groups. We set

$$\operatorname{Hom}(G, G') = \{\text{homomorphisms } f : G \to G'\}.$$

An **isomorphism** $f : G \to G'$ is a bijective group homomorphism. Thus $f$ is an isomorphism if and only if $\ker f = \{1_G\}$ and $\operatorname{im} f = G'$. We sometimes write $f : G \xrightarrow{\sim} G'$ to indicate that $f$ is an isomorphism. Two groups $G, G'$ are **isomorphic** if there exists an isomorphism $f : G \xrightarrow{\sim} G'$. We write $G \simeq G'$ to indicate that $G$ and $G'$ are isomorphic, without specifying any particular isomorphism between them.

We sometimes abuse terminology and say that $G$ *is* or *is a copy of* $G'$, when we really mean only that $G \simeq G'$. For example, any two trivial groups are isomorphic, so we allow ourselves to say that *the* trivial group is the unique group with one element.

Continuing in this vein, we say that a homomorphism $f : G \to G'$ is **trivial** if $\operatorname{im} f = \{1_{G'}\}$. This is equivalent to having $\ker f = G$, so being a trivial homomorphism is the opposite of being an isomorphism. Hence trivial homomorphisms are just as important as isomorphisms.

An isomorphism from a group to itself is called an **automorphism**. We set

$$\operatorname{Aut}(G) = \{\text{automorphisms of } G\}.$$

The set $\operatorname{Aut}(G)$ forms a group under composition, whose identity element is the identity automorphism, which sends $g \mapsto g$ for all $g \in G$.

Many automorphisms arise from within the group itself as follows. For each element $g$ in a group $G$, the map

$$c_g : G \to G \qquad \text{given by} \qquad c_g(x) = gxg^{-1}\ \forall x \in G$$

is an automorphism of $G$, called **conjugation by** $g$. Automorphisms of this form are called **inner automorphisms**. The function $c : G \to \operatorname{Aut}(G)$ sending $g \mapsto c_g$ is a homomorphism.

## 2.3 Subgroups

A **subgroup** of $G$ is a subset $H \subseteq G$ with the following three properties:

SG1 (*closure*) $ab \in H$ for all $a, b \in H$.

SG2 (*identity*) The identity element of $G$ is contained in $H$.

SG3 (*inverses*) For all $a \in H$ we have $a^{-1} \in H$.

The subsets $\{1\}$ and $G$ are subgroups of $G$. All other subgroups of $G$, if any, are called **proper subgroups**. We write $H \leq G$ to indicate that $H$ is a subgroup of $G$ which is possibly equal to $G$ itself. We write $H < G$ for a subgroup which is not equal to $G$.

**Lemma 2.1** *Let $G$ be a group and let $H$ be a nonempty* finite *subset of $G$. Then $H \leq G$ if and only if SG1 holds.*

**Proof:** Let $h$ be an element of the nonempty set $H$. Since $H$ is finite, the powers $h, h^2, h^3, \ldots$ must eventually repeat, so we have $h^i = h^j$ for some positive integers $i < j$. It follows that $h^{j-i} = 1$, so SG2 holds, and $h \cdot h^{j-i-1}$, so SG3 holds. Hence $H$ is a subgroup of $G$. ■

This proof moved from $H$ to a particular kind of subgroup of $G$. A group $C$ is **cyclic** if there exists an element $c \in C$ such that $C = \{c^n : n \in \mathbb{Z}\}$. In this case we write $C = \langle c \rangle$.

In an arbitrary group $G$, any element $g \in G$ is contained in the cyclic subgroup

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$

The **order** of $g$ is the order of the group $\langle g \rangle$. The order of $g$ is the smallest positive power $m$ such that $g^m = 1$, if such an $m$ exists. In this case, the order can be characterized by the useful property that for any integer $d$, we have $g^d = 1$ iff $m \mid d$. If $g^d \neq 1$ for any nonzero integer $d$, we say the order of $g$ is infinite.

More generally, if $S$ is any subset of $G$, the **subgroup generated by** $S$ is the smallest subgroup $\langle S \rangle$ of $G$ containing $S$. That is,

$$\langle S \rangle = \bigcap_{S \subseteq H \leq G} H$$

is the intersection of all subgroups $H$ of $G$ which contain the subset $S$.

## 2.4 Cosets and quotient spaces

A **left coset** of a subgroup $H < G$ is a subset of $G$ of the form $gH = \{gh : h \in H\}$. Two left cosets are either equal or disjoint; we have

$$gH = g'H \qquad \Leftrightarrow g^{-1}g' \in H.$$

In particular, we have $gH = H$ if and only if $g \in H$. The set of left cosets of $H$ in $G$ is denoted $G/H$, and is called the **quotient** of $G$ by $H$.

A **right coset** of $H$ in $G$ is a subset of the form $Hg = \{hg : h \in H\}$. Two right cosets are either equal or disjoint; we have

$$Hg = Hg' \qquad \Leftrightarrow g'g^{-1} \in H.$$

In particular, we have $Hg = H$ if and only if $g \in H$. The set of right cosets of $H$ in $G$ is denoted $H\backslash G$.

A **coset** is a left or right coset. Any element of a coset is called a *representative* of that coset. We have canonical bijections $H \to gH$ and $H \to Hg$, sending $h \mapsto gh$ and $h \mapsto hg$, respectively. Hence if $H$ is finite, all cosets have cardinality $|H|$.

There are an equal number (including infinity) of left and right cosets in $G$. We denote this number by

$$[G : H] = |G/H| = |H\backslash G|,$$

and call it the *index* of $H$ in $G$. If $G$ is finite, then $G$ is partitioned into $[G : H]$ cosets, each of cardinality $|H|$. It follows that $[G : H] = |G|/|H|$. In particular we have

**Lagrange's Theorem:** If $H$ is a subgroup of a finite group $G$, then $|H|$ divides $|G|$.

**Example 1:** If $|G| = p$ a prime, then $G$ has no proper subgroups. Hence for any nonidentity element $g \in G$ we have $G = \langle g \rangle$, so $G$ is cyclic.

**Example 2:** The order of any element in a finite group $G$ divides $|G|$. in particular, we have $g^{|G|} = 1$ for all $g \in G$. The smallest positive integer $e$ such that $g^e = 1$ for all $g \in G$ is called the **exponent of** $G$. If $g \in G$ has order $m$, then $m$ divides $e$, which in turn divides $|G|$.

The converse of Lagrange's theorem is false. The smallest counterexample is the group $A_4$ of order $12$, which has no subgroup of order $6$. However, the converse of Lagrange's theorem is true for subgroups $H$ of prime power order. This is part of the Sylow theorems, which we will prove later. However, one special case is easy:

**Proposition 2.2** *Any group of even order contains an element of order two.*

**Proof:** Suppose $G$ has even order $|G| = 2m$. Pair the nonidentity elements with their inverses. Since there are $2m - 1$ such elements, at least one of them is paired with itself. This is a nonidentity element $g \in G$ such that $g = g^{-1}$. Thus, $g$ is an element of $G$ of order two. ■

## 2.5 Normal subgroups and quotient groups

Let $G$ be a group and let $H \leq G$ be a subgroup. One attempts to define a group structure on the set $G/H$ by the rule:

$$gH * g'H = gg'H, \qquad \forall g, g' \in G. \tag{1}$$

However, this rule is only well-defined when every left coset of $H$ in $G$ is also a right coset of $H$ in $G$. The subgroup $H$ is said to be **normal** in $G$ if $gH = Hg$ for all $g \in H$. On the level of elements, this means that $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$. If $G$ is abelian, then $ghg^{-1} = h$, so every subgroup is normal in $G$. Thus, being normal in $G$ is a weakening, with respect to $H$, of the abelian condition. We write $H \triangleleft G$ or $H \trianglelefteq G$ to indicate that $H$ is a normal subgroup of $G$.

When, and only when $H \trianglelefteq G$, the set $G/H = H\backslash G$ becomes a group under the operation given by (1). We call $G/H$ the **quotient** of $G$ by $H$. It is a group of order equal to the index of $H$ in $G$:

$$|G/H| = [G : H].$$

**Example:** The **center** of a group $G$ is the subgroup

$$Z(G) = \{z \in G : \ zg = gz \quad \forall g \in G\}.$$

This is clearly a normal subgroup of $G$. We will see the quotient group $G/Z(G)$ appearing in several contexts. One useful fact is

**Proposition 2.3** *If $G/Z(G)$ is cyclic then $G$ is abelian.*

**Proof:** Exercise. ■

## 2.6 The first isomorphism theorem

Any group homomorphism $f : G \to G'$ induces an isomorphism from a quotient of $G$ to a subgroup of $G'$. More precisely, we have the following.

**Theorem 2.4 (First isomorphism theorem)** *Let $f : G \to G'$ be a group homomorphism with kernel $K = \ker f$. Then $K$ is a normal subgroup of $G$, and there is an isomorphism*

$$\bar{f} : G/K \xrightarrow{\sim} \operatorname{im} f, \qquad \textit{given by} \quad \bar{f}(gK) = f(g). \tag{2}$$

**Proof:** It is a good exercise to check that $\bar{f}$ is well-defined and bijective. ■

It is useful to have this result in slightly more general form:

**Theorem 2.5** *Let $f : G \to G'$ be a group homomorphism with kernel $K = \ker f$. Let $H$ be a normal subgroup of $G$ contained in $K$. Then there is a surjective homomorphism*

$$\bar{f} : G/H \twoheadrightarrow \operatorname{im} f, \qquad \textit{given by} \quad \bar{f}(gH) = f(g), \tag{3}$$

*with* $\ker \bar{f} = K/H$.

**Proof:** Again, this is a good exercise. ■

We often say that $\bar{f}$ is *induced* by $f$ or that $f$ *factors through* $G/H$.

Conversely, every normal subgroup $H \trianglelefteq G$ is the kernel of a surjective homomorphism from $G$ into another group. Namely, the **canonical homomorphism**

$$\pi_H : G \longrightarrow G/H, \qquad \text{given by} \quad \pi_H(g) = gH$$

is surjective with $\ker \pi_H = H$.

**Example:** If $x, y$ are two elements of $G$, the **commutator**

$$[x, y] = xyx^{-1}y^{-1}$$

is an element of $G$ that measures the failure of $x, y$ to commute. The **Commutator Subgroup**

$$[G, G] = \langle [x, y] : \ x, y \in G \rangle$$

is the subgroup generated by all commutators. For $g \in G$ we have $g[x, y]g^{-1} = [gxg^{-1}, gxg^{-1}]$. It follows that $[G, G] \trianglelefteq G$. The quotient $G/[G, G]$ is called the **abelianization of** $G$, and is often denoted $G_{ab}$, because of the following result.

**Proposition 2.6** *The quotient $G/[G, G]$ of a group $G$ by its commutator subgroup is abelian. Moreover, $G/[G, G]$ is the largest abelian quotient of $G$, in the following sense: If $f : G \to A$ is a homomorphism from $G$ to an abelian group $A$, then $[G, G] < \ker f$, so $f$ factors through a homomorphism*

$$\bar{f} : G/[G, G] \longrightarrow A.$$

**Proof:** Exercise. ■

### 2.6.1 Exact sequences

A composition of group homomorphisms

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3$$

is **exact at** $G_2$ if $\operatorname{im} f_1 = \ker f_2$. A sequence of group homomorphisms

$$\ldots \longrightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \longrightarrow \ldots$$

is an **exact sequence** if it is exact at $G_i$ for all $i$. A **short exact sequence** is a sequence

$$1 \longrightarrow G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \longrightarrow 1$$

with

$$\ker f_1 = \{1\}, \quad \operatorname{im} f_1 = \ker f_2 \simeq G_1, \quad \operatorname{im} f_2 = G_3 \simeq G_2/G_1.$$

## 2.7 The second isomorphism theorem (correspondence theorem)

The subgroups of a quotient group $G/H$ are related to subgroups of $G$ as follows.

**Theorem 2.7** *Let $G$ be a group with normal subgroup $H \trianglelefteq G$, and let $\pi_H : G \to G/H$ be the canonical homomorphism.*

1. *If $K$ is any subgroup of $G$ containing $H$, then $H \trianglelefteq K$ and $K/H = \pi_H(K)$ is a subgroup of $G/H$.*
2. *Conversely, if $J$ is any subgroup of $G/H$, then $\pi_H^{-1}(J)$ is a subgroup of $G$ containing $H$ as a normal subgroup and $J = \pi_H^{-1}(J)/H$.*
3. *$K/H \trianglelefteq G/H$ if and only if $K \trianglelefteq G$, in which case $(G/H)/(K/H) \simeq G/K$.*

Thus, we have a one-to-one correspondence

$$\begin{array}{ccc} \{\text{subgroups of } G \text{ containing } H\} & \leftrightarrow & \{\text{subgroups of } G/H\} \\ K & \to & K/H \\ \pi_H^{-1}(J) & \leftarrow & J, \end{array}$$

and this correspondence preserves normal subgroups.

There is also a correspondence theorem for homomorphisms, the first part of which is just Thm. 2.5 above.

**Theorem 2.8** *Let $G$ be a group with normal subgroup $H \trianglelefteq G$.*

1. *If $f : G \to G'$ is a group homomorphism with $H \leq \ker f$ then $f$ induces a well-defined homomorphism $\bar{f} : G/H \to G'$, given by $\bar{f}(gH) = f(g)$.*
2. *If $\varphi : G/H \to G'$ is any homomorphism, then $\varphi \circ \pi_H : G \to G'$ is a homomorphism whose kernel contains $H$.*

Thus, we have a one-to-one correspondence

$$\begin{array}{ccc} \mathrm{Hom}(G/H, G') & \leftrightarrow & \{f \in \mathrm{Hom}(G, G') : \ H \leq \ker f\} \\ \varphi & \to & \varphi \circ \pi_H \\ \bar{f} & \leftarrow & f \end{array}$$

## 2.8 The third isomorphism theorem

The final isomorphism theorem concerns products of subgroups. If $H$ and $K$ are subgroups of a group $G$, the product $HK = \{hk : \ h \in H, \ k \in K\}$ contains the identity, but it need not be closed under

the operation in $G$, hence $HK$ need not be a subgroup of $G$. However, it will be so under an additional condition.

The **normalizer** of $H$ in $G$ is the subgroup

$$N_G(H) = \{g \in G : \ gHg^{-1} = H\}.$$

We have $N_G(H) = G$ if and only if $H \trianglelefteq G$. In general, $N_G(H)$ is the largest subgroup of $G$ containing $H$ as a normal subgroup.

Returning to our two subgroups $H, K$ in $G$, let us assume that

$$K \leq N_G(H).$$

(This assumption holds automatically if $H \trianglelefteq G$.) Then, for $h, h' \in H$ and $k, k' \in K$, we have

$$(hk)(h'k') = h(kh'k^{-1}) \cdot kk'$$

(where we insert $()$ and $\cdot$ to help parse the product), and $kh'k^{-1}$ belongs to $H$ since $k \in N_G(H)$, so $(hk)(h'k') \in HK$. Similarly, $(hk)^{-1} = k^{-1}h^{-1} = (k^{-1}h^{-1}k) \cdot k^{-1} \in HK$. Hence $HK$ is a subgroup of $G$. Since both $H$ and $K$ are contained in $N_G(H)$, it follows that $HK$ is also contained in $N_G(H)$. In other words, $H$ is normal in $HK$.

This proves the first part of the following

**Theorem 2.9 (Third Isomorphism Theorem)** *Let $H$ and $K$ be subgroups of a group $G$ and assume that $K \leq N_G(H)$. Then*

1. *$HK$ is a subgroup of $G$ and $H$ is a normal subgroup of $HK$.*
2. *$H \cap K$ is a normal subgroup of $K$.*
3. *We have a group isomorphism $K/(K \cap H) \simeq HK/H$, induced by the map $f : K \to HK/H$ given by $k \mapsto kH$.*

**Proof:** We have already proved the first part, and the second part is easy. As for the third part, it is clear that $f$ is surjective, so it remains to determine $\ker f$. Let $k \in K$. Then $f(k) = 1$ in $HK/H$ iff $\iota(k) \in H$, which means that $k \in H$. But $k \in K$, so we have $f(k) = 1$ iff $k \in H \cap K$, as claimed. ■

## 2.9 Direct products

Let $H$ and $K$ be groups with identity elements $1_H$ and $1_K$. Then the direct product

$$H \times K = \{(h, k) : \ h \in H, k \in K\}$$

is a group under the operation

$$(h, k)(h', k') = (hh', kk')$$

and identity element $(1_H, 1_K)$. The direct product of finitely many groups $G_1, \ldots, G_n$ is defined similarly; we confine our discussion to the case $n = 2$.

Let $G = H \times K$, and write $1 = (1_H, 1_K)$. The maps $\phi : H \to G$ and $\psi : K \to G$ given by $\phi(h) = (h, 1_K)$ and $\psi(k) = (1_H, k)$ are injective homomorphisms. Their images $H' = \phi(H) \simeq H$ and $K' = \psi(K) \simeq K$ are normal subgroups of $G$ such that

$$H' \cap K' = \{1\} \qquad \text{and} \qquad H'K' = G.$$

Conversely, this can be used to *recognize* direct products as follows.

**Proposition 2.10** *Let $G$ be a group with subgroups $H$ and $K$. Assume that*

1. *$H$ and $K$ are both normal in $G$;*
2. *$H \cap K = \{1\}$;*
3. *$G = HK$.*

*Then $G \simeq H \times K$, via the map $f : H \times K \to G$ given by $f(h, k) = hk$.*

**Proof:** Let $h \in H$, $k \in K$ and parse the commutator $[h, k] = hkh^{-1}k^{-1}$ in two ways. On the one hand, $[h, k] = (hkh^{-1})k^{-1} \in K$ since $K \trianglelefteq G$. On the other hand, $[h, k] = h(kh^{-1}k^{-1}) \in H$, since $H \trianglelefteq G$. But $H \cap K$ is trivial, so $[h, k] = 1$. Hence $h$ and $k$ commute for all $h \in H$ and $k \in K$. It is now immediate that $f$ is a homomorphism, which is surjective by assumption 3. Finally, if $f(h, k) = 1$, we have $h = k^{-1} \in H \cap K = \{1\}$, so $h = k = 1$. Therefore $f$ is an isomorphism, as claimed. ■

If $H$ and $K$ are abelian groups then we often write $H \oplus K$ instead of $H \times K$, in accordance with our use of additive notation for abelian groups.

## 2.10 Semidirect products (internal view)

Recall that a group $G$ with two normal subgroups $H, K \trianglelefteq G$ is the direct product $G = H \times K$ iff $HK = G$ and $H \cap K = \{1\}$. This situation often occurs with the variation that only one of the subgroups is normal.

**Definition 2.11** *A group $G$ is a* **semidirect product** *of two subgroups $H, K \leq G$ if the following conditions hold.*

1. *One of the subgroups $H$ and/or $K$ is normal in $G$.*
2. *$H \cap K = \{1\}$.*
3. *$HK = G$.*

Suppose $G$ is the semidirect product of $H$ and $K$ and (say) $H$ is normal in $G$. On the set $H \times K$, define a group law as follows:

$$(h,k)(h',k') = (hkh'k^{-1}, kk').$$

Let $H \rtimes K$ denote the set $H \times K$ with this group law.

**Proposition 2.12** *If $G$ is a semidirect product of two subgroups $H$ and $K$ with $H \trianglelefteq G$, then the map $(h,k) \mapsto hk$ is a group isomorphism*

$$H \rtimes K \xrightarrow{\sim} G.$$

**Proof:** exercise. ■

## 2.11 Conjugacy

For $g, x \in G$, let us set

$$^g x = gxg^{-1}.$$

Two elements $x, y \in G$ are **conjugate** in $G$ if $y = {}^g x$ for some $g \in G$. Conjugacy is an equivalence relation on $G$, whose equivalence classes are the **conjugacy classes** of $G$. Thus any group is partitioned into conjugacy classes. We write

$$^G x = \{^g x : \ g \in G\}$$

for the conjugacy class of $x$ in $G$.

Some of our earlier notions can be expressed in terms of conjugacy. For example, we have $x \in Z(G)$ if and only if $^G x = \{x\}$. And $H \trianglelefteq G$ if and only if $H$ is a union of conjugacy classes in $G$.

The **centralizer** of a given element $x \in G$ is the subgroup $C_G(x) = \{h \in G : \ ^h x = x\}$ consisting of all elements in $G$ which commute with $x$. This is generally not a normal subgroup of $G$, so the quotient space $G/C_G(x)$ is not a group. However, we have

**Proposition 2.13** *For every $x \in G$, the map $g \mapsto {}^g x$ induces a well-defined bijection*

$$G/C_G(x) \xrightarrow{\sim} {}^G x.$$

*In particular, if $G$ is finite, we have*

$$|^G x| = [G : C_G(x)] = \frac{|G|}{|C_G(x)|}.$$

**Proof:** Exercise ■

The last formula in Prop. 2.13 is very useful for computing the sizes of conjugacy classes and centralizers in finite groups. It implies for example that $|^G x|$ divides $|G|$. Since $G$ is the disjoint union of its conjugacy classes, we have

**Corollary 2.14 (The class equation)** *Let $G$ be a finite group, let $X_1, \ldots, X_k$ be its conjugacy classes, choose $x_i \in X_i$ for $1 \leq i \leq k$, and let $G_i = C_G(x_i)$. Then we have*

$$\sum_{i=1}^{k} [G : G_i] = |G|.$$

*Alternatively,*

$$\frac{1}{|G_1|} + \frac{1}{|G_2|} + \cdots + \frac{1}{|G_k|} = 1.$$

**Corollary 2.15** *If $|G|$ is a power of a prime $p$ then $G$ has nontrivial center.*

**Proof:** We have $G$ partitioned as $G = Z(G) \cup \{\text{noncentral elements}\}$. Every conjugacy class has size a power of $p$. This power is zero precisely for those classes consisting of a single element in $Z(G)$ and every conjugacy class of noncentral elements has size a positive power of $p$. Hence $|\{\text{noncentral elements}\}|$ is divisible by $p$. As $|G|$ is also divisible by $p$, it follows that $p$ divides $|Z(G)|$. Since $|Z(G)| \geq 1$, it follows that a positive power of $p$ divides $|Z(G)|$. ■

# 3 The Symmetric Group

Groups usually arise as symmetries of mathematical structure. The most basic structure is just a set.

For any set $X$, the **symmetric group** on $X$ is the group $S_X$ of bijections $\sigma : X \to X$ from $X$ to itself, where the group operation is composition of functions: $(\sigma\tau)(x) = \sigma(\tau(x))$. The identity element is the identity function $e(x) \equiv x$. The elements of $S_X$ are usually called **permutations**.

If $\beta : X \to Y$ is a bijection between two sets $X$ and $Y$, then we get a group isomorphism $S_\beta : S_X \xrightarrow{\sim} S_Y$, defined by

$$S_\beta(\sigma) = \beta \circ \sigma \circ \beta^{-1}.$$

If $X = Y$ then $\beta \in S_X$ and $S_\beta$ is conjugation by $\beta$.

## 3.1 Cycle decomposition and conjugacy classes

Assume now that $X$ is finite, say $|X| = n$. Then $S_X$ is finite and one checks that

$$|S_X| = n! = n(n-1)\cdots 2 \cdot 1.$$

Given $\sigma \in S_X$, define an equivalence relation $\underset{\sigma}{\sim}$ on $X$ by the rule:

$$x \underset{\sigma}{\sim} y \quad \Leftrightarrow \quad y = \sigma^j(x) \quad \text{for some } j \in \mathbb{Z}.$$

The equivalence classes are called $\sigma$**-orbits**. If $\mathcal{O}$ is a $\sigma$-orbit and $x \in \mathcal{O}$, the distinct elements of $\mathcal{O}$ are

$$x,\ \sigma(x),\ \sigma^2(x),\ \ldots,\ \sigma^{\lambda-1}(x),$$

where $\lambda = |\mathcal{O}|$. We note that $\sigma^\lambda(x) = x$.

Number the $\sigma$-orbits in $X$ as $\mathcal{O}_1, \ldots \mathcal{O}_q$, where $|\mathcal{O}_1| \geq |\mathcal{O}_2| \geq \cdots \geq |\mathcal{O}_q|$, and set $\lambda_i = |\mathcal{O}_i|$ for each $i$. Thus, we have a set partition

$$X = \bigsqcup_{i=1}^{q} \mathcal{O}_i$$

and a corresponding numerical partition

$$|X| = \sum_{i=1}^{q} \lambda_i.$$

Let us choose $x_i \in \mathcal{O}_i$, for each $\sigma$-orbit $\mathcal{O}_i$, and set $x_i^j = \sigma^{j-1}(x_i)$, so that

$$\mathcal{O}_i = \{x_i^j :\ 1 \leq \lambda_i\}.$$

Let $\sigma_i \in S_X$ be the permutation sending

$$x_i = x_i^1 \mapsto x_i^2 \mapsto \cdots \mapsto x_i^{\lambda_i} \mapsto x_i,$$

and acting as the identity on $\mathcal{O}_k$ for $k \neq i$. We express $\sigma_i$ by the symbol

$$\sigma_i = (x_i^1\ x_i^2\ \cdots\ x_i^{\lambda_i}).$$

Then $\sigma_i\sigma_j = \sigma_j\sigma_i$ for $i \neq j$ and

$$\sigma = \sigma_1\sigma_2\cdots\sigma_q, \tag{4}$$

where the product may be taken in any order. This is the **disjoint cycle decomposition** of $\sigma$. The partition

$$\lambda(\sigma) := [\lambda_1, \lambda_2, \ldots, \lambda_q]$$

is called the **cycle type** of $\sigma$. The cycle type determines the conjugacy class, as follows.

**Proposition 3.1** *Two elements $\sigma, \sigma' \in S_X$ are conjugate if and only if $\lambda(\sigma) = \lambda(\sigma')$.*

**Proof:** Let $\mathcal{O}_1, \ldots, \mathcal{O}_q$ be the $\sigma$-orbits in $X$. If $\sigma' = \tau\sigma\tau^{-1}$ for some $\tau \in S_X$, one checks that $\tau(\mathcal{O}_1), \ldots, \tau(\mathcal{O}_q)$ are the $\sigma'$-orbits in $X$. Since $\tau$ is a permutatation, we have $|\tau(\mathcal{O}_i)| = |\mathcal{O}_i|$ for each $i$, which implies that $\lambda(\sigma') = \lambda(\sigma)$.

Conversely, suppose $\lambda(\sigma') = \lambda(\sigma)$. Let $\mathcal{O}_1, \ldots, \mathcal{O}_q$ be the $\sigma$-orbits and let $\mathcal{O}'_1, \ldots, \mathcal{O}'_{q'}$ be the $\sigma'$-orbits. Since $\lambda(\sigma) = \lambda(\sigma')$ we have $q = q'$ and $|\mathcal{O}_i| = |\mathcal{O}'_i|$ for each $i$. Since the orbits are disjoint there exists a permutation $\tau \in S_X$ such that $\tau(\mathcal{O}_i) = \mathcal{O}'_i$ for each $i$. Replacing $\sigma$ by $\tau\sigma\tau^{-1}$, we may assume that $\mathcal{O}'_i = \mathcal{O}_i$ for each $i$.

Choose $x_i \in \mathcal{O}_i$, and set $x_i^j = \sigma^{j-1}(x_i)$, $y_i^j = (\sigma')^{j-1}(x_i)$, so that $x_i^1 = y_i^1 = x_i$ and

$$\mathcal{O}_i = \{x_i^1, x_i^2, \ldots, x_i^{\lambda_i}\} = \{y_i^1, y_i^2, \ldots, y_i^{\lambda_i}\}.$$

Every element of $X$ may be uniquely expressed in the form $x_i^j$ or in the form $y_i^j$, where $1 \leq i \leq q$ and $1 \leq j \leq \lambda_i$. Let $\pi \in S_X$ be the permutation sending $x_i^j \mapsto y_i^j$ for each such $i, j$. For $x = x_i^j$, we have

$$\pi\sigma\pi^{-1}(x) = \pi\sigma\sigma^j(x_i) = \pi\sigma^{j+1}(x_i) = (\sigma')^{j+1}(x_i) = \sigma'(x).$$

It follows that $\pi\sigma\pi^{-1} = \sigma'$, so $\sigma$ and $\sigma'$ are conjugate. ■

## 3.2 The group $S_n$

When $X = \{1, 2, \ldots, n\}$ we write $S_n = S_X$. If $X$ is any set with $|X| = n$ then by labelling the elements of $X$ we obtain a bijection $f : X \to \{1, 2, \ldots, n\}$, whence a group isomorphism $S_f : S_X \xrightarrow{\sim} S_n$. This isomorphism is noncanonical, because it depends on the chosen labelling $f$. Moreover, the set $X$ need not be ordered, as $\{1, 2, \ldots, n\}$ is. The ordering gives additional structure to $S_n$ that is missing in $S_X$ when $X$ is unordered

As in (4), an element in $S_n$ is a product of cycles, but now the symbols in the cycle are numbers in $\{1, 2, \ldots, n\}$. For example, the element $\sigma \in S_6$ sending

$$1 \mapsto 4, \quad 2 \mapsto 6, \quad 3 \mapsto 1, \quad 4 \mapsto 3, \quad 5 \mapsto 5, \quad 6 \mapsto 2$$

may be written as

$$\sigma = (1\ 4\ 3)(2\ 6),$$

and has cycle type $\lambda(\sigma) = [3, 2, 1]$. Note that 5, which is fixed, is omitted in the cycle decomposition of $\sigma$, but is counted in the cycle type of $\sigma$.

We multiply using the cycle decomposition by following the path of each number, starting with the right-most cycle. For example, we have

$$(1\ 4\ 3)(2\ 6)(4\ 6\ 5) = (1\ 4\ 2\ 6\ 5\ 3).$$

Note that the cycle type of $\tau = (1\ 4\ 3)(2\ 6)(4\ 6\ 5)$ is *not* $[3, 3, 2]$, because the cycles are not disjoint. We first have to make them disjoint, as we have done above. We obtained a single 6-cycle $(1\ 4\ 2\ 6\ 5\ 3)$, so the cycle type of $\tau$ in $S_6$ is $\lambda(\tau) = [6]$.

We illustrate the cycle types for all elements of $S_3$ and $S_4$, as follows.

| $\lambda$ | $\sigma$ |
|---|---|
| $[3]$ | $(1\ 2\ 3), (3\ 2\ 1)$ |
| $[2, 1]$ | $(1\ 2), (2\ 3), (1\ 3)$ |
| $[1, 1, 1]$ | $e$ |

| $\lambda$ | $\sigma$ |
|---|---|
| $[4]$ | $(1\ 2\ 3\ 4), (1\ 3\ 2\ 4), (1\ 2\ 4\ 3), (1\ 4\ 2\ 3), (1\ 3\ 4\ 2), (1\ 4\ 3\ 2)$ |
| $[3, 1]$ | $(1\ 2\ 3), (3\ 2\ 1), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (4\ 3\ 2)$ |
| $[2, 2]$ | $(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$ |
| $[2, 1, 1]$ | $(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$ |
| $[1, 1, 1, 1]$ | $e$ |

### 3.2.1 Descending decomposition

The additional structure imparted to $S_n$ by the ordering on $\{1, 2, \ldots, n\}$ can be seen as follows: i) the transposition $(1\ 3)$ has a gap, while its conjugates $(1\ 2)$ and $(2\ 3)$ do not, and ii) the cycles $(1\ 2\ 3), (3\ 2\ 1), (2\ 1\ 3)$ denote the same element of $S_3$, but the numbers in the cycle are ascending, descending and neither, respectively. The *descending decomposition* uses the ordering to give a unique expression of each element in $S_n$ in terms of descending cycles $(k\ k-1\ k-2\ \cdots)$.

For later purposes it will be more convenient to work with $S_{n+1}$, permuting $\{0, \ldots, n\}$. Let $\mathbf{K}_n$ be the set of $n$-tuples $\mathbf{k} = (k_1, \ldots, k_n)$ of integers satisfying $i - 1 \leq k_i \leq n$ for each $i$. Given $\mathbf{k} \in K_n$ we define cycles $\pi_1, \pi_2, \ \ldots\ , \pi_n \in S_n$ by

$$\pi_i = (k_i\ k_i - 1\ \ldots\ i\ i-1)$$

if $k_i > i - 1$ and $\pi_i = e$ if $k_i = i - 1$, and we set

$$\pi_{\mathbf{k}} = \pi_1 \ldots \pi_n.$$

**Proposition 3.2** *Sending* $\mathbf{k} \mapsto \pi_{\mathbf{k}}$ *gives a bijection* $\mathbf{K}_n \xrightarrow{\sim} S_{n+1}$.

**Proof:** We construct the inverse map. Given $\sigma \in S_{n+1}$ define $\mathbf{k}$ recursively by $k_1 = \sigma(0)$, which defines $\pi_1 = (k_1\ k_1 - 1\ \ldots 1\ 0)$, and for $i > 1$ set

$$k_i = \pi_{i-1} \cdots \pi_1(i).$$

Since $\pi_i(j) = j$ for $j < i$, it follows that

$$\sigma = \pi_1 \pi_2 \cdots \pi_n = \pi_{\mathbf{k}}, \tag{5}$$

as claimed. ■

For example, the identity element $e = \pi_{\mathbf{k}}$ where each $k_i \equiv i - 1$. At the other extreme, when $k_i \equiv n$ we get the permutation

$$\tilde{\sigma} = (n\ \ldots\ 1\ 0)(n\ \ldots\ \ 2\ 1) \cdots (n\ n-1). \tag{6}$$

Clearly there is also an ascending decomposition, obtained by inverting (5). We have emphasized the descending version since it appears naturally in the Bruhat decomposition of $\mathrm{GL}_n$ for the upper-triangular Borel subgroup, as we will see in section 7.1.

### 3.2.2 Length

We continue with $S_{n+1}$ permuting $\{0, 1, \ldots, n\}$. The descending 2-cycles

$$s_i = (i\ i-1) \qquad \text{for } 1 \leq i \leq n$$

are called **simple transpositions**. A general descending cycle $(k \ \dots \ i \ i-1)$ can be expressed as a product of simple transpositions thus:

$$(k \ \dots \ i \ i-1) = s_k s_{k-1} \cdots s_i. \tag{7}$$

Combined with Prop. 3.2, this gives a recipe for expressing an arbitrary element $\sigma \in S_{n+1}$ as a product of

$$\ell(\sigma) := \sum_{i=1}^{n} (k_i - i + 1)$$

simple transpositions, where $\sigma = \pi_{\mathbf{k}}$. We call $\ell(\sigma)$ the **length** of $\sigma$. For example, we have $\ell(e) = 0$ and the element $\tilde{\sigma}$ defined in (6) has length

$$\ell(\tilde{\sigma}) = 1 + 2 + \cdots + n = n(n+1)/2.$$

Thus $\tilde{\sigma}$ is the **longest element** of $S_{n+1}$. The expression for $\tilde{\sigma}$ produced by Prop. 3.2 and (7) is

$$\tilde{\sigma} = (s_n s_{n-1} \cdots s_1) \cdot (s_n s_{n-1} \cdots s_2) \cdots (s_n).$$

Note that length is not constant on conjugacy-classes. For example, $\ell(s_1 s_2 s_1) = 3$, while $\ell(s_2) = 1$. We see again that length depends on more than the group structure of $S_{n+1}$. It turns out that $\sigma$ cannot be expressed as a product of fewer than $\ell(\sigma)$ simple transpositions, but we will not need this.

### 3.2.3 Inversions

We have defined $\ell(\sigma)$ in terms of the descending cycle decomposition. This can be interpreted as counting the inversions of $\sigma$.

Let $R$ be the set of ordered pairs pairs $(i, j)$ such that $0 \leq i, j \leq n$ and $i \neq j$. We have $R = R^+ \sqcup R^-$, where $R^+ = \{(i, j) \in R : \ i < j\}$ and $R^- = \{(i, j) \in R : \ i > j\}$. For $\sigma \in S_{n+1}$ we consider the set of **inversions**

$$N(\sigma) := R^+ \cap \sigma^{-1} R^-.$$

Thus, $N(\sigma)$ is the set of pairs $(i, j) \in R$ such that $i < j$ and $\sigma(i) > \sigma(j)$.

For a descending cycle $\sigma = [k \ k-1 \ \cdots p]$ we have

$$N(\sigma) = \{(p, j) : \ p < j \leq k\} \qquad \text{and} \qquad \sigma N(\sigma) = \{(k_p, j) : \ p \leq j < k_p\}. \tag{8}$$

We observe in this case that $|N(\sigma)| = k - p - 1 = \ell(\sigma)$. This holds true in general.

**Proposition 3.3** *For any element $\sigma \in S_{n+1}$ we have*

$$\ell(\sigma) = |N(\sigma)|.$$

**Proof:** Let $\sigma = \sigma_1 \cdots \sigma_n$ be the descending cycle decomposition. We first show that for any $1 \le p < q \le n$ that we have a disjoint union

$$N(\sigma_p \cdots \sigma_q) = N(\sigma_{p+1} \cdots \sigma_q) \sqcup (\sigma_{p+1} \cdots \sigma_q)^{-1} N(\sigma_p). \tag{9}$$

Let us abbreviate $\tau := \sigma_{p+1} \cdots \sigma_q$, and note that $\tau(i) = i$ if$i < p$.

Let $(i,j) \in N(\sigma_p \tau)$. If $\tau(i) > \tau(j)$ then $(i,j) \in N(\tau)$. If $\tau(i) < \tau(j)$ then $(i,j) \in \tau^{-1} N(\sigma_p)$. Hence $(i,j) \in N(\tau) \cup \tau^{-1} N(\sigma_p)$.

From (8) we have

$$N(\sigma_p) = \{(p-1, j) : \ p \le j \le k_p\} \qquad \text{and} \qquad \sigma_p N(\sigma_p) = \{(k_p, j) : \ p-1 \le j \le k_p - 1\}.$$

The right side of (9) is contained in $R^+$. Indeed, $N(\tau) \subset R^+$ by definition and $\tau^{-1} N(\sigma_p) \subset R^+$ since $\tau(p-1) = p-1$.

The right side of (9) is contained in $N(\sigma)$. Indeed, $\sigma \tau^{-1} N(\sigma_p) = \sigma_p N(\sigma_p) \subset R^-$ by definition. And if $(i,j) \in \tau N(\tau)$ then $i > j \ge p$ so $(j,i) \notin N(\sigma_p)$ so $\sigma_p(j) > \sigma_p(i)$. It follows that $\sigma_p \tau N(\tau) \subset R^-$.

The right side of (9) is a disjoint union. Indeed, if $(i,j) \in N(\tau)$ then $i \ge p$ and that if $(i,j) \in \tau^{-1} N(\sigma_p)$ then $i = p-1$. ■

Applying (9) to the full descending decomposition $\sigma = \sigma_1 \cdots \sigma_n$ and using induction, we obtain

$$N(\sigma) = \bigsqcup_{p=1}^{n} (\sigma_{p+1} \cdots \sigma_n)^{-1} N(\sigma_p). \tag{10}$$

Now Prop. 3.3 follows from (8). ■

We highlight an observation made in the last step of the proof; we will use later for the Bruhat decomposition in section 8.10:

$$N(\sigma_1 \cdots \sigma_q) = N(\sigma_q) \sqcup \bigsqcup_{p=1}^{q-1} (\sigma_{p+1} \cdots \sigma_q)^{-1} N(\sigma_p),$$

and that

$$N(\sigma_q) = \{(i,j) \in N(\sigma_1 \cdots \sigma_q) : \ i = q-1\}, \qquad (\sigma_{p+1} \cdots \sigma_q)^{-1} N(\sigma_p) = \{(i,j) \in N(\sigma_1 \cdots \sigma_q) : \ i = p-1\}.$$

In particular, we have

$$(i,j) \in N(\sigma_1 \cdots \sigma_q) \quad \Rightarrow i < q. \tag{11}$$

## 3.3 Sign character and alternating group

A permutation $\sigma \in S_n$ is **even** if its cycle type $\lambda(\sigma)$ contains an even number of even numbers; otherwise $\sigma$ is **odd**. This notion does not use the ordering on $\{1, \ldots, n\}$. Nevertheless, a permutation $\sigma$ is even precisely when its length is even.

Thus, $(1\ 2)(3\ 4)$ and $(1\ 2\ 3)$ are even, while $(1\ 2)$ and $(1\ 2)(3\ 4\ 5)$ are odd. We put

$$\operatorname{sgn}(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

Note that $\{\pm 1\}$ is a group under multiplication.

**Proposition 3.4** *The function* $\operatorname{sgn} : S_n \to \{\pm 1\}$ *is a surjective group homomorphism.*

We will prove this in section 5.1, using determinants.

The **Alternating Group** $A_n$ is defined as

$$A_n = \ker \operatorname{sgn} = \{\sigma \in S_n : \ \sigma \text{ is even}\}.$$

Thus, $A_n \lhd S_n$ and

$$|A_n| = \tfrac{1}{2}n! = 3 \cdot 4 \cdot \ \cdots \ \cdot n.$$

For example, $A_4$ has order 12; it is the union of the classes of type $[3],\ [2,2],\ [1,1,1,1]$ in $S_4$. However, these are not quite the conjugacy classes in $A_4$.

The conjugacy classes in $A_n$ are determined as follows. First, $A_n$ consists of the even classes in $S_n$. However, two elements of $A_n$ which are conjugate in $S_n$ need not be conjugate in $A_n$. Hence an even $S_n$-class could break up into several $A_n$-classes. To see when this happens, let $\sigma \in A_n$ and restrict the character $\operatorname{sgn}$ to the centralizer $C_{S_n}(\sigma)$ of $\sigma$ in $S_n$. We have

$$C_{A_n}(\sigma) = \ker[C_{S_n}(\sigma) \xrightarrow{\operatorname{sgn}} \{\pm 1\}],$$

so that the index

$$h_\sigma := [C_{S_n}(\sigma) : C_{A_n}(\sigma)] = \begin{cases} 2 & \text{if} \quad C_{S_n}(\sigma) \not\leq A_n \\ 1 & \text{if} \quad C_{S_n}(\sigma) \leq A_n. \end{cases}$$

Now the size of the conjugacy class $\sigma^{A_n}$ in $A_n$ is given by

$$|\sigma^{A_n}| = \frac{|A_n|}{|C_{A_n}(\sigma)|} = \frac{\frac{1}{2}|S_n|}{\frac{1}{h_\sigma}|C_{S_n}(\sigma)|} = \frac{h_\sigma}{2} \cdot |\sigma^{S_n}|.$$

It follows that if $C_{S_n}(\sigma) \not\leq A_n$ then $\sigma^{S_n}$ is a single conjugacy class in $A_n$ and if $C_{S_n}(\sigma) \leq A_n$ then $\sigma^{S_n}$ breaks up into two $A_n$-conjugacy classes:

$$\sigma^{S_n} = \sigma^{A_n} \cup \bar{\sigma}^{A_n},$$

where $\bar{\sigma}$ is conjugate to $\sigma$ in $S_n$ but not in $A_n$.

For example, in $S_4$ elements in the $[2,2]$-class contain 2-cycles in their centralizer (which is the dihedral group $D_4$, see section 8.3), so the $[2,2]-$ class is a single class in $A_4$. But elements in the $[3,1]$-class generate their own centralizer, which is therefore contained in $A_4$. So the $[3,1]$-class breaks up into two classes with four elements each. These classes are mutually inverse. If $A_4$ is viewed as rotations of the tetrahedron, then one class consists of clockwise face rotations and the other class consists of counterclockwise face rotations.

# 4 Group actions

We say that group $G$ **acts** on the set $X$ if there is a homomorphism $\varphi : G \to S_X$ from $G$ into the group $S_X$ of permutations of $X$. The pair $(X, \varphi)$ is sometimes called a $G$**-set** or a $G$**-action**. Thus, each $g \in G$ gives a permutation $\varphi_g$ of $X$, which sends any $x \in X$ to an element $\varphi(g)x$. If $\varphi$ is understood or is completely general, we usually omit it from the notation, writing $gx$ or $g \cdot x$ instead of $\varphi(g)x$.

If $(X, \varphi)$ and $(Y, \psi)$ are two $G$-sets, a function $f : X \to Y$ is called $G$**-equivariant** if $f(\varphi(g)x) = \psi(g)f(x)$ for all $g \in G$ and $x \in X$. We say that $(X, \varphi)$ and $(Y, \psi)$ are **equivalent** $G$**-sets** if there exists a $G$-equivariant bijection $f : X \to Y$.

The notion of a $G$-set generalizes the notion of a group. For we can regard the action as a map $G \times X \to X$, given by $(g, x) \mapsto g \cdot x$ such that $g \cdot (g' \cdot x) = (gg') \cdot x$ for all $g, g' \in G$ and $x \in X$.

Some standard terminology associated with group actions is as follows.

The **stabilizer** or **fixer** of a point $x \in X$ is the subgroup of $G$ given by

$$G_x = \{g \in G : \ g \cdot x = x\} \leq G.$$

The **orbit** of an element $x \in X$ is the subset of $X$ given by

$$G \cdot x = \{g \cdot x : \ g \in G\} \subseteq X.$$

Orbits are equivalence classes under the equivalence relation $x \sim y$ if $y = g \cdot x$ for some $g \in G$. Hence two orbits are either equal or disjoint; the orbits form a partition of $X$. We write $G\backslash X$ for the set of orbits.

The **fixed-point set** of $g \in G$ is the subset of $X$ given by

$$X^g = \{x \in X : \ g \cdot x = x\}$$

One can check that stabilizers and fixed-point sets behave well under conjugacy:

**Proposition 4.1** *For all $g \in G$ and $x \in X$, we have*

$$G_{g \cdot x} = gG_xg^{-1}.$$

*In particular, the stabilizers of all elements of the same orbit are conjugate. Likewise, if $g, h \in G$ then*

$$h \cdot (X^g) = X^{hgh^{-1}}.$$

The **kernel** of a group action $\varphi : G \to S_X$ is the normal subgroup of $G$ consisting of the elements acting trivially on $X$. We have

$$\ker \varphi = \bigcap_{x \in X} G_x = \{g \in G : \ X^g = X\}.$$

A $G$-action on $X$ is **faithful** or **effective** if $\ker \varphi$ is trivial. Equivalently, the action is faithful if no nontrivial element of $G$ acts trivially on $X$. In this case, $G$ is isomorphic to a subgroup of $S_X$.

Finally, a group action is **free** if $g \cdot x = x$ for some $x \in X$ implies $g = 1$. That is, a group action is free if and only if all stabilizers are trivial. Clearly free actions are faithful. An example of a free action is where a subgroup $H$ of a group $G$ acts on $G$ by left multiplication: $h \cdot x = hx$. Here, $G$ is the set and $H$ is the group which is acting. The orbits are the right cosets $Hx$.

A $G$-action on $X$ is **transitive** if for all $x, y \in X$ there exists $g \in G$ such that $g \cdot x = y$. Equivalently, the action is transitive iff $X$ consists of a single $G$-orbit. For a general group action, each orbit is a transitive $G$-set. Thus, transitive group actions are the essential ones. An example of a transitive group action is where $X = G/H$, for some subgroup $H \leq G$, and the action is $g \cdot xH = gxH$. We will see that all transitive $G$-actions are of this form. More generally, a $G$-action on $X$ is **$k$-transitive** if $G$ is transitive on $k$-tuples of distinct elements of $X$. This is a measure of the strength of transitivity.

**The Main Theorem of Group Actions**

*If a group $G$ acts on a set $X$, then for each $x \in X$ we have a $G$-equivariant bijection*

$$f : G/G_x \xrightarrow{\sim} G \cdot x, \qquad \textit{given by} \qquad f(gG_x) = g \cdot x.$$

*In particular, any transitive group action is equivalent to an action on cosets.*

**Proof:** The map $f$ is well-defined because for all $h \in G_x$ we have $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x$. The map $f$ is injective because if $g \cdot x = g' \cdot x$ then $g^{-1}g' \cdot x = x$, so $g^{-1}g' \in G_x$, which means that $gG_x = g'G_x$. The map $f$ is surjective, by the definition of the orbit $G \cdot x$. Finally, for all $g, g' \in G$ and $x \in X$ we have

$$f(g \cdot g'G_x) = f(gg'G_x) = (gg') \cdot x = g \cdot (g' \cdot x) = g \cdot f(g'G_x),$$

which shows that $f$ is $G$-equivariant. ■

As a corollary, we have one of the most useful formulas in group theory.

**The Counting Formula.** *Let $G$ be a finite group acting on a set $X$. Then the cardinality of an orbit equals the index of the stabilizer of any point in the orbit. That is, for any $x \in X$ we have*

$$\frac{|G|}{|G_x|} = |G \cdot x|. \tag{12}$$

Note that the right hand side of this equation depends only on the orbit, while the left side appears to depend on the stabilizer of a particular point in the orbit. However, by Prop. 4.1 all stabilizers $G_x$ for $x$ in a given orbit are conjugate, hence have the same order.

Let $\mathcal{O}_1, \ldots, \mathcal{O}_k$ be the orbits of $G$ in $X$, and choose $x_i \in \mathcal{O}_i$. Applying the counting formula to each orbit, we have the weaker but still useful formula

$$|X| = \sum_{i=1}^{k} |\mathcal{O}_i| = \sum_{i=1}^{k} [G : G_{x_i}]. \tag{13}$$

## 4.1 The left regular action

Any group $G$ acts on itself by left multiplication. More precisely, this action is given by the homomorphism $L : G \to S_G$ such that $L_g x = gx$ for all $g, x \in G$. This is called the **left regular action**; one easily checks that it is free and transitive. Moreover, any free transitive $G$-action on a set $X$ is isomorphic to the left regular action (Exercise ...). If $G$ is finite, say $|G| = n$, then $S_G \simeq S_n$ via a labelling of the elements of $G$. Since the left regular action is faithful, this proves:

**Proposition 4.2** *A finite group $G$ of order $n$ is isomorphic to a subgroup of $S_n$, via the left regular action $L : G \to S_n$.*

In other words, $S_n$ contains every group of order $n$ as a subgroup.

What are the cycle types of the elements of $L(G)$? For any permutation $\sigma \in S_n$, the numbers in the cycle type $\sigma$ are the sizes of the orbits of $\langle\sigma\rangle$ on $\{1, 2, \ldots, n\}$. Since $G$ acts freely on itself, the subgroup $\langle g\rangle$ also acts freely on $G$ and the orbits of $\langle g\rangle$ on $G$ are just the right cosets of $\langle g\rangle$. The order $d$ of $g$ divides $n$ and there are $n/d$ right cosets of $\langle g\rangle$ in $G$, all of size $d$. This proves

**Proposition 4.3** *Let $G$ be a finite group of order $n$, let $g \in G$, and let $d$ be the order of $g$. Then under the left regular action $L : G \to S_n$ the cycle type of $L_g$ is a product of $n/d$ cycles of length $d$.*

This has the following surprising corollary.

**Corollary 4.4** *Suppose $G$ is a group of order $n$ containing an element of order $d$ where $d$ is even and $n/d$ is odd. Then $G$ has a normal subgroup of index two. In particular, $G$ cannot be simple.*

**Proof:** If $g \in G$ has even order $d$ with $n/d$ odd, then $L_g$ is a product of an odd number of even cycles, so $\operatorname{sgn}(L_g) = -1$. Hence the homomorphism $\operatorname{sgn} \circ L : G \to \{\pm 1\}$ is nontrivial, so $\ker(\operatorname{sgn} \circ L)$ is a normal subgroup of $G$ of index two. ■

From this, we can prove another partial converse to Lagrange's theorem.

**Corollary 4.5** *Suppose $G$ is a group of order $2m$ where $m$ is odd. Then $G$ has a normal subgroup of order $m$.*

**Proof:** By Prop. 2.2 there exists $g \in G$ of order two, satisfying the conditions of Cor. 4.4. ■

Since a group $G$ also acts on itself by right multiplication, we also have the **right regular action** given by the homomorphism $R : G \to S_G$ given by $\rho_g x = xg^{-1}$. [Check that this is a group action- in so doing, you'll see why we need the inverse.] Analogues of the above results all hold for $R$ as well.

## 4.2 Group actions on coset spaces

Let $G$ be a group with identity element $e$, let $H \leq G$ be a subgroup and let $G/H$ be the set of left cosets of $H$ in $G$. Instead of $H$ acting on $G$, we can consider $G$ acting on $G/H$, via left multiplication: $g \cdot xH = gxH$. When $H = \{1\}$ we recover the left regular action. For nontrivial $H$, this action is transitive (because any $xH \in G/H$ is $x \cdot eH$) but no longer free, because the stabilizer of $eH$ is the nontrivial subgroup $H$. More generally, the stabilizer of $xH$ is $xHx^{-1}$.

Every transitive group action is isomorphic to one of this form. Indeed, if $G$ acts transitively on a set $X$, and we pick any $x \in X$, then the Main Theorem of Group Actions shows that this action is isomorphic to the action of $G$ on $G/H$, via left multiplication as just defined, where $H = G_x$. However, describing a transitive $G$-set as $G/H$ contains the additional data of a basepoint, namely $eH$.

If $G$ is finite, this gives a useful way to study subgroups of $G$, as follows.

**Proposition 4.6** *Let $G$ be a finite group having a subgroup $H \leq G$ of index $[G : H] = m$. Then there is a homomorphism $\sigma_H : G \longrightarrow S_m$ whose image is a transitive subgroup of $S_m$ and whose kernel is given by*

$$\ker \sigma_H = \bigcap_{g \in G} gHg^{-1}.$$

## 4.3 Double cosets

Suppose a group $G$ acts transitively on a set $X$ and we wish to study the action of a subgroup $K < G$ on $X$. From the Main Theorem on Group Actions, we may assume that $X = G/H$ for some subgroup $H \leq G$, possibly equal to $K$.

So let us begin with a group $G$ and arbitrary subgroups $K, H$. Let the group $K \times H$ act on the set $G$ by the rule

$$(k, h) \cdot g = kgh^{-1}.$$

The orbits of this action are called $(K, H)$**-double cosets**. Each double coset is of the form

$$KxH = \{kxh : \ k \in K, h \in H\}$$

for some $x \in G$. As with all group actions, the set $G$ is partitioned as

$$G = \bigsqcup_x KxH,$$

where $x$ runs over representatives for the $(K, H)$-double cosets.

Each double coset $KxH$ is a union of left cosets of $H$ and $KxH/H \subset G/H$ is the set of the left cosets of $H$ contained in $KxH$. In fact $KxH/H$ is exactly the $K$-orbit of $xH$ in $G/H$. By the Main Theorem of Group actions, this orbit is a $K$-set which must be equivalent to $K/J$ for some subgroup $J \leq K$.

**Proposition 4.7** *The stabilizer of $xH$ in $K$ is $K \cap xHx^{-1}$. Hence we have a $K$-equivariant bijection*

$$K/(K \cap xHx^{-1}) \xrightarrow{\sim} KxH/H,$$

*sending $k(K \cap xHx^{-1}) \mapsto kxH/H$.*

**Proof:** If $k \in K$, then

$$kxH = xH \quad \Leftrightarrow \quad x^{-1}kx \in H \quad \Leftrightarrow \quad k \in xHx^{-1} \cap K.$$

The rest of the proposition follows from the Main Theorem of Group Actions. ■

If $G$ is finite, we can use Prop. 4.7 to compute the number of elements in a given double coset $KxH$, namely

$$|KxH| = \frac{|K| \cdot |H|}{|K \cap xHx^{-1}|}.$$

We can also view $KxH$ as the $H$-orbit of $Kx$ in $K\backslash G$, and the stabilizer of $Kx$ in $H$ is $x^{-1}Kx \cap H$, so that $K\backslash KxH \simeq (x^{-1}Kx \cap H)\backslash H$, as $H$-sets.

The set of $(K, H)$-double cosets in $G$ is denoted by $K\backslash G/H$. The number $|K\backslash G/H|$ of double cosets may be thought of in three ways:

- $|K\backslash G/H|$ is the number of $K \times H$ orbits on $G$.
- $|K\backslash G/H|$ is the number of $K$-orbits on $G/H$.
- $|K\backslash G/H|$ is the number of $H$-orbits on $K\backslash G$.

In contrast to ordinary cosets, there is no simple formula for $|K\backslash G/H|$ in general, because the action of $K$ on $G/H$ (or the action of $H$ on $K\backslash G$) need not be free.

It is especially interesting to know when $|K\backslash G/H|$ is small. For example, it follows from the definitions that

$$|K\backslash G/H| = 1 \quad \Leftrightarrow \quad G = KH \quad \Leftrightarrow \quad K \quad \text{is transitive on} \quad G/H.$$

Here is a deeper situation. Let $G$ be a group acting transitively on a set $X$. To avoid trivialities we assume $X$ has more than one element. Then $G$ also acts on $X \times X$, via $g \cdot (x, y) = (g \cdot x, g \cdot y)$. This action cannot be transitive, because the diagonal $\Delta X = \{(x, x) : \ x \in X\}$ is an orbit. Hence there are at least two orbits on $X \times X$. We say that $G$ acts **doubly transitively** on $X$ if $G$ has exactly two orbits on $X \times X$. This means $G$ acts transitively on $\{(x, y) \in X \times X : \ x \neq y\}$. In other words, $G$ is doubly transitive on $X$ if for any two pairs of distinct elements $(x, y)$ and $(x', y')$ in $X \times X$, there is a single element $g \in G$ such that $g \cdot x = x'$ and $g \cdot y = y'$.

**Proposition 4.8** *Let $G$ be a group acting transitively on a set $X$, and assume $|X| > 1$. The following are equivalent.*

1. $|G_x \backslash G / G_x| = 2$ *for any* $x \in X$.

2. *For any* $x \in X$, *the stabilizer* $G_x$ *is transitive on* $X - \{x\}$.

3. $G$ *acts doubly transitively on* $X$.

**Proof:**

($1 \Leftrightarrow 2$): We have $|G_x \backslash G / G_x| = 2$ exactly when $G_x$ has exactly two orbits in $X$. One of these orbits is $\{x\}$ so $|G_x \backslash G / G_x| = 2$ exactly when $G_x$ is transitive on $X - \{x\}$.

($2 \Rightarrow 3$): Assume $G_x$ is transitive on $X - \{x\}$ for any $x \in X$. Let $(x, y)$ and $(x', y')$ be two pairs of distinct elements of $X$. Since $G$ is transitive on $X$, there is $g \in G$ such that $g \cdot x' = x$. Note that $g \cdot y' \neq x$ since $x' \neq y'$. By our assumption, there is $h \in G_x$ such that $h \cdot (g \cdot y') = y$. For the element $hg \in G$ we have $hg \cdot x' = h \cdot x = x$ and $hg \cdot y' = y$, so $hg \cdot (x', y') = (x, y)$. Hence $G$ is doubly transitive on $X$.

($3 \Rightarrow 2$): Assume $G$ is doubly transitive on $X$ and let $x \in X$. Let $y, y'$ be two elements of $X - \{x\}$. Since $G$ is doubly transitive, there exists $g \in G$ such that $g \cdot x = x$ and $g \cdot y = y'$. This shows that $G_x$ is transitive on $X - \{x\}$. ■

In other words, if $H$ is any subgroup of $G$ then $G$ acts doubly transitively on $G/H$ if and only if

$$G = H \cup HgH, \qquad \text{(disjoint)}$$

For any element $g$ outside of $H$.

**Example :** Let $G = S_n$ and let $H \simeq S_{n-1}$ be the subgroup stabilizing the number $1$. The permutations in $H$ are precisely those whose disjoint cycle expression does not involve the number $1$, and we have $S_n/H \simeq \{1, 2, \ldots, n\}$ as $S_n$-sets. Given $1 \leq i < j \leq n$ there exists $\sigma \in S_n$ sending $1, 2$ to $i, j$ respectively. It follows that $S_n$ is doubly-transitive on $\{1, 2, \ldots, n\}$ and we have

$$S_n = H \cup H\sigma H.$$

The elements of $H\sigma H$ are precisely those permutations whose disjoint cycle expression involves the number $1$.

For any positive integer $k \leq n$ the group $S_n$ acts on on the set $X_k = \{x \subset \{1, 2, \ldots, n\} : \ |x| = k\}$ of $k$-element subsets of $\{1, 2, \ldots n\}$. One such subset is $x_0 = \{1, 2, \ldots, k\}$, whose stabilizer is isomorphic to $S_k \times S_{n-k}$. The counting formula says that

$$|X_k| = \frac{|S_n|}{|S_k| \cdot |S_{n-k}|} = \frac{n!}{k!(n-k)!},$$

as it should.

## 4.4 Conjugation

Conjugation can be viewed as an action of $G$ on itself. This action is the homomorphism $c : G \to S_G$ given by $c_g(x) = gxg^{-1}$. Understanding this action is another important way to know a given group.

In this context, the orbit of an element $x \in G$ is its conjugacy class ${}^G x = \{gxg^{-1} : \ g \in G\}$ and the stabilizer of $x$ is the centralizer $C_G(x) = \{g \in G : \ gxg^{-1} = x\}$. . Finally, the kernel of the conjugation action is the center $Z(G)$ of $G$.

If $G$ is finite, the formula

$$|C_G(x)| \cdot |{}^G x| = |G|, \qquad \text{for all} \quad x \in G \tag{14}$$

is the Counting Formula for the conjugation action.

## 4.5 Burnside's Lemma

Let $G$ be a group acting on a set $X$. Consider the set

$$\widetilde{X} = \{(g, x) \in G \times X : \ g \cdot x = x\}.$$

The projections onto $G$ and $X$ give maps

$$p_1 : \widetilde{X} \to G, \qquad p_2 : \widetilde{X} \to X,$$

whose fibers are the fixed-point sets and stabilizers, respectively:

$$p_1^{-1}(g) = X^g, \qquad p_2^{-1}(x) = G_x.$$

If $G$ and $X$ are finite, we can compute $|\widetilde{X}|$ in two ways, by summing both sets of fibers:

$$\sum_{g \in G} |X^g| = |\widetilde{X}| = \sum_{x \in X} |G_x|.$$

Since $|G_x|$ is constant for $x$ in an orbit, we can partition the last sum into orbits $\mathcal{O}_1, \ldots, \mathcal{O}_k$, as in (13):

$$\sum_{x \in X} |G_x| = \sum_{i=1}^{k} |\mathcal{O}_i| \cdot |G_{x_i}| = k \cdot |G|.$$

It follows that the number of orbits is the average size of a fixed-point set:

$$|G\backslash X| = \frac{1}{|G|} \sum_{g \in G} |X^g|. \tag{15}$$

This formula is known as "Burnside's Lemma" because he seems to have given the first published proof, though it was apparently known to Cauchy, well before Burnside.

The sum in (15) can be condensed because $|X^g| = |X^h|$ if $g$ and $h$ are conjugate elements of $G$. Thus, if $\Lambda$ is a set of representatives of the conjugacy-classes in $G$ we have

$$|G\backslash X| = \sum_{g \in \Lambda} \frac{|X^g|}{|C_G(g)|}. \tag{16}$$

### 4.5.1 Application: Graph counting

Let $V$ be a set and let $V_2$ be the set of two-element subsets $\{v, v'\} \subset V$. A *graph* $(V, E)$ consists of the set $V$ of "vertices" and a subset $E \subset V_2$ of "edges". Two graphs $(V, E)$ and $(V', E')$ are *isomorphic* if there is a bijection $f : V \to V'$ such that $f_2(E) = E'$, where $f_2 : V_2 \to V_2'$ is the map induced by $f$. Now $E$ is determined by its characteristic function

$$\chi_E : V_2 :\longrightarrow \{0, 1\},$$

so the isomorphism classes of graphs with vertex set $V$ are the orbits of the symmetric group $S_V$ on the set $X$ consisting of all functions $\chi : V_2 \to \{0, 1\}$.

Fix a positive integer $n$ and let $V = \{1, \ldots, n\}$, so that $V_2 = \{\{i, j\} : \ i, j \in V, \ i \neq j\}$. The number $\gamma_n$ of isomorphism classes of graphs with $n$ vertices is given by

$$\gamma_n = |S_n \backslash X_n|,$$

where $X_n = \{\chi : V_2 \to \{0, 1\}\}$. We will use Burnside's Lemma (twice) to give an explicit formula for $\gamma_n$.

First, we have

$$\gamma_n = \frac{1}{n!} \sum_{\sigma \in S_n} |X_n^\sigma|.$$

A function $\chi \in X_n$ is fixed by $\sigma$ exactly when $\chi$ is constant on the orbits of $\langle \sigma \rangle$ in $V_2$. It follows that

$$|X_n^\sigma| = 2^{o(\sigma)},$$

where $o(\sigma)$ is the number of orbits of $\langle \sigma \rangle$ on $V_2$.

The number $o(\sigma)$ depends only on the conjugacy class of $\sigma$, which corresponds, via cycle types, to a partition $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r > 0)$ of $n$. We set $o(\lambda) = o(\sigma)$ where $\sigma$ has cycle type $\lambda$. Using the condensed formula (16) we have

$$\gamma_n = \sum_\lambda \frac{2^{o(\lambda)}}{z(\lambda)},$$

sum over all partitions $\lambda$ of $n$, where $z(\lambda)$ is the order of the centralizer in $S_n$ of a permutation with cycle type $\lambda$. In fact we have the explicit formula

$$z(\lambda) := \prod_{k=1}^{n} [e_k(\lambda)!] \cdot k^{e_k(\lambda)},$$

where $e_k(\lambda) = |\{i : \ \lambda_i = k\}|$.

Thus the problem is to compute $o(\lambda) = o(\sigma)$. For this we can use Burnside's Lemma again, this time for the cyclic group $\langle \sigma \rangle$. If $\sigma$ has order $m$, we get

$$o(\sigma) = \frac{1}{m} \sum_{d=1}^{m} |V_2^{\sigma^d}|.$$

We note that

$$|V_2^\sigma| = \binom{e_1(\lambda)}{2} + e_2(\lambda).$$

The same holds for each power $\sigma^d$, but with $\lambda$ replaced by the cycle type of $\sigma^d$. Let

$$\sigma = \sigma_1 \cdots \sigma_r$$

be the disjoint cycle decomposition of $\sigma$, so that each $\sigma_i$ is a $\lambda_i$-cycle. Then

$$\sigma^d = \sigma_1^d \cdots \sigma_r^d,$$

and $\sigma_i^d$ has cycle type

$$\left[\frac{\lambda_i}{d_i}, \ldots, \frac{\lambda_i}{d_i}\right], \tag{17}$$

where $d_i = \gcd(\lambda_i, d)$, and $d_i$ is also the number of parts in the partition (17). It follows that

$$e_1(\sigma^d) = \sum_{\substack{i \\ \lambda_i = d_i}} d_i = \sum_{\substack{i \\ \lambda_i | d}} \lambda_i.$$

When we sum over $d$, each $\lambda_i$ occurs for

$$d = \lambda_i,\ 2\lambda_i,\ \cdots,\ \frac{m}{\lambda_i}\lambda_i.$$

Hence

$$\frac{1}{m}\sum_{d=1}^{m} e_1(\sigma^d) = \frac{1}{m}\sum_{i=1}^{r} \frac{m}{\lambda_i}\lambda_i = r.$$

Likewise, one checks that

$$\frac{1}{m}\sum_{d=1}^{m} e_1(\sigma^d)^2 = n + 2(\lambda, \lambda),$$

where

$$(\lambda, \lambda) = \sum_{i<j} \gcd(\lambda_i, \lambda_j),$$

and that

$$\frac{1}{m}\sum_{d=1}^{m} e_2(\sigma^d) = \frac{r_+(\lambda)}{2},$$

where $r_+(\lambda) = \{i :\ \lambda_i \in 2\mathbb{Z}\}$ is the number of even parts of $\lambda$. Putting all this together, we find that

$$o(\lambda) = (\lambda, \lambda) + \frac{n - r_-(\lambda)}{2},$$

where $r_-(\lambda) = |i :\ \lambda_i \in 1 + 2\mathbb{Z}\}$ is the number of odd parts of $\lambda$.

For example, if $n = 4$ we find

$$o(1,1,1,1) = 6, \quad o(2,1,1) = 4, \quad o(22) = 4, \quad o(31) = 2, \quad o(4) = 2,$$

so that

$$\gamma_4 = \frac{2^6}{24} + \frac{2^4}{4} + \frac{2^4}{8} + \frac{2^2}{3} + \frac{2^2}{4} = 11.$$

# 5 Linear groups

Let $V$ be a vector space over a field $F$. The set $GL(V)$ of invertible linear transformations $T : V \to V$ forms a group under composition, called the **general linear group** of $V$, whose identity element is the transformation $I_V(v) \equiv v$.

If $V$ has finite dimension $n$ over $F$ and we choose an ordered basis $\{v_1, \ldots, v_n\}$ of $V$ then each $T \in GL(V)$ corresponds to an invertible $n \times n$ matrix $A_T$ whose $j^{th}$ column is

$$\begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{bmatrix},$$

where $T(v_j) = a_{1j}v_1 + a_{2j}v_j + \cdots + a_{nj}v_n$. Matrix multiplication is defined so that

$$A_S \cdot A_T = A_{ST}, \qquad \text{for all} \qquad S, T \in \mathrm{GL}(V).$$

It follows that sending $T \mapsto A_T$ is a group isomorphism

$$\mathrm{GL}(V) \xrightarrow{\sim} \mathrm{GL}_n(F), \tag{18}$$

where $\mathrm{GL}_n(F)$ is the group of $n \times n$ invertible matrices under matrix multiplication, whose identity element is the $n \times n$ identity matrix

$$I_n = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & & \ddots & 0 \\ 0 & 0 & \ldots & 1 \end{bmatrix}.$$

As was the case for $S_n$, the isomorphism (18) is noncanonical, because it depends on a choice of ordered basis $\{v_1, \ldots, v_n\}$ of $V$.

A $1 \times 1$ matrix is just a number, so

$$\mathrm{GL}_1(F) = F^\times$$

is the group of nonzero elements of the field $F$ under multiplication. This group $F^\times$ appears in $\mathrm{GL}_n(F)$ as both a normal subgroup and a quotient.

First, we have an injective homomorphism

$$F^\times \hookrightarrow \mathrm{GL}_n(F), \qquad \text{given by } a \mapsto a \cdot I_n = \begin{bmatrix} a & 0 & \ldots & 0 \\ 0 & a & \ldots & 0 \\ \vdots & & \ddots & 0 \\ 0 & 0 & \ldots & a \end{bmatrix}, \tag{19}$$

whose image $Z \simeq F^\times$ is the center of $\mathrm{GL}_n(F)$. The **Projective Linear Group** $PGL_n(F)$ is defined as

$$\mathrm{PGL}_n(F) = \mathrm{GL}_n(F)/Z.$$

Elements of $PGL_n(F)$ are no longer linear transformations, but they permute the lines in the vector space $F^n$. Thus, the elements of $\mathrm{PGL}_n(F)$ are transformations of the **Projective Space** $\mathbf{P}^{n-1}(F)$ which is the set of lines in $F^n$.

Next, recall that an $n \times n$ matrix $A$ is invertible if and only if its determinant $\det(A)$ is nonzero. Moreover, if $A$ and $B$ are two $n \times n$ matrices, we have $\det(AB) = \det(A) \cdot \det(B)$. Thus, $\det$ is a homomorphism

$$\det : \mathrm{GL}_n(F) \to F^\times.$$

The **Special Linear Group** $\mathrm{SL}_n(F)$ is defined as

$$\mathrm{SL}_n(F) = \ker \det = \{A \in \mathrm{GL}_n(F) : \ \det(A) = 1\}.$$

When $F = \mathbb{R}$, elements of $\mathrm{SL}_n(F)$ are the linear transformations of $\mathbb{R}^n$ which preserve volume.

Returning to general $F$, consider the restriction of $\det$ to $Z$. Since

$$\det(aI_n) = a^n, \tag{20}$$

it follows that

$$\det(Z) = F^{\times n}$$

is the subgroup of $n^{th}$ powers in $F^\times$. Hence the composition

$$\mathrm{GL}_n(F) \xrightarrow{\det} F^\times \longrightarrow F^\times/F^{\times n}$$

induces a surjective homomorphism

$$\mathrm{PGL}_n(F) \xrightarrow{\overline{\det}} F^\times/F^{\times n}.$$

The latter group depends on the field $F$. For example, we have $|\mathbb{C}^\times/\mathbb{C}^{\times n}| = 1$, while $|\mathbb{R}^\times/\mathbb{R}^{\times n}| = 1$ or 2 according as $n$ is odd or even, and $\mathbb{Q}^\times/\mathbb{Q}^{\times n}$ is infinite.

It also follows from (20) that the intersection

$$Z_1 = SL_n(F) \cap Z = \{aI_n : \ a^n = 1\} \simeq \mu_n(F),$$

where $\mu_n(F) = \{a \in F^\times : \ a^n = 1\}$ is the subgroup of $n^{th}$ roots of unity in $F^\times$. The group $Z_1$ is the center of $\mathrm{SL}_n(F)$ and the quotient

$$\mathrm{PSL}_n(F) = \mathrm{SL}_n(F)/Z_1 = \ker \overline{\det}$$

is the image of $\mathrm{SL}_n(F)$ in $\mathrm{PGL}_n(F)$. The center $Z_1 \simeq \mu_n(F)$ of $\mathrm{SL}_n(F)$ also depends on the field $F$. For example, we have $|\mu_n(\mathbb{C})| = n$, while $|\mu_n(\mathbb{R})| = 1$ or 2 according as $n$ is odd or even. For general fields $F$, $\mu_n(F)$ is always finite of order dividing $n$.

In summary, we have four closely related groups $\mathrm{GL}_n(F), \mathrm{SL}_n(F), \mathrm{PGL}_n(F), \mathrm{PSL}_n(F)$, related to each other via the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_n(F) & \longrightarrow & F^\times & \xrightarrow{n} & F^{\times n} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{SL}_n(F) & \longrightarrow & \mathrm{GL}_n(F) & \xrightarrow{\det} & F^\times & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{PSL}_n(F) & \longrightarrow & \mathrm{PGL}_n(F) & \xrightarrow{\overline{\det}} & F^\times/F^{\times n} & \longrightarrow & 1 \end{array} \tag{21}$$

If $F$ is a finite field with $|F| = q$, we write

$$\mathrm{GL}_n(q), \qquad \mathrm{SL}_n(q), \qquad \mathrm{PGL}_n(q), \qquad \mathrm{PSL}_n(q)$$

instead of

$$\mathrm{GL}_n(F), \qquad \mathrm{SL}_n(F), \qquad \mathrm{PGL}_n(F), \qquad \mathrm{PSL}_n(F).$$

Often in the literature one finds the abbreviation $L_n(q)$ for $\mathrm{PSL}_n(q)$. The orders of these groups are given as follows.

$$\begin{aligned} |\mathrm{GL}_n(q)| &= q^{n(n-1)/2}(q-1)(q^2-1)\cdots(q^n-1) \\ |\mathrm{PGL}_n(q)| = |\mathrm{SL}_n(q)| &= q^{n(n-1)/2}(q^2-1)(q^3-1)\cdots(q^n-1) \\ |\mathrm{PSL}_n(q)| &= |\mathrm{SL}_n(q)|/\gcd(n, q-1) \end{aligned} \tag{22}$$

In the last line, recall from (24) that $\gcd(n, q-1) = |\mu_n(F)|$. All of these orders then follow from the calculation of $|GL_n(q)|$, which can be done as follows. To have a matrix $A \in GL_n(q)$, we can take any of the $q^n - 1$ nonzero vectors in $F^n$ for the first column, then any of the $q^n - q$ vectors not in the line spanned by the first column, then any of the $q^n - q^2$ vectors not in the plane spanned by the first two columns, etc. This gives

$$\begin{aligned} |\mathrm{GL}_n(q)| &= (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1}) \\ &= q^{1+2+\cdots+(n-1)}(q^n-1)(q^{n-1}-1)(q^{n-2}-1)\cdots(q-1) \\ &= q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)(q^{n-2}-1)\cdots(q-1), \end{aligned}$$

as claimed above.

## 5.1 Symmetric groups and Linear groups

Let $X$ be a set and let $F$ be a field. To this data we associate an $F$-vector space $V$ with a *canonical basis* $\{v_x : x \in X\}$, as follows: $V$ is the set of all functions $v : X \to F$, and $v_x$ is the function $v_x(x') = 1$ if $x = x'$, zero otherwise.

The symmetric group $S_X$ acts on $V$ in the obvious way: If $\sigma \in S_X$ and $v = \sum_{x\in X} c_x v_x$, (with all $c_x \in F$) then $\sigma v = \sum_{x\in X} c_x v_{\sigma(x)}$. In particular we have $\sigma(v_x) = v_{\sigma(x)}$ and this latter equation determines the action of $\sigma$ on all of $V$.

Suppose $\sigma = (i_1\ i_2\ \cdots\ i_r)$ is an $r$-cycle in $S_n$. The matrix $A_\sigma$ sends $e_{i_1} \mapsto e_{i_2} \mapsto \cdots \mapsto e_{i_r} \mapsto e_{i_1}$ and fixes the remaining $e_j$'s. Since the determinant of a matrix is unchanged by simultaneous interchanges of rows and columns, we have

$$\det(A_\sigma) = \det \begin{bmatrix} A'_\sigma & 0 \\ 0 & I_{n-r} \end{bmatrix} = \det(A'_\sigma)$$

where $A'_\sigma$ is the $r \times r$ matrix

$$A'_\sigma = \begin{bmatrix} 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}.$$

Expanding along the top row, we compute

$$\det(A'_\sigma) = (-1)^{r-1}.$$

Hence $\det(A_\sigma) = +1$ or $-1$ according as $r$ is odd or even.

Now take a general $\sigma \in S_n$ and write it as a product of disjoint cycles. We have $\det(A_\sigma) = +1$ or $-1$ according as $\sigma$ has an even or odd number of even cycles. This agrees with our definition of $\mathrm{sgn}$ above, so we have shown that

$$\det(A_\sigma) = \mathrm{sgn}(\sigma).$$

Hence $\mathrm{sgn} = \det \circ f$ is a group homomorphism, as claimed in Prop. 3.4.

It will be useful to know how $S_n$ conjugates a general matrix. Let $R$ be the set of ordered pairs of distinct integers $(i, j)$ with $i, j \in \{1, \dots, n\}$. The group $S_n$ acts on $R$ via $\sigma \cdot (i, j) = (\sigma i, \sigma j)$. For any $n \times n$ matrix $A = [A_{ij}]$ let $R(A) = \{(i, j) :\ A_{ij} \neq 0\}$.

**Lemma 5.1** *If $\sigma \in S_n$ and $A$ is any $n \times n$ matrix over a field $F$ then we have*

1. $(A_\sigma A A_\sigma^{-1})_{\sigma i, \sigma j} = A_{ij}$
2. $R(A_\sigma A A_\sigma^{-1}) = \sigma \cdot R(A)$.

**Proof:** The first assertion is a straightforward computation and the second assertion follows. ■

### 5.1.1 Conjugacy classes in $\mathrm{GL}_2(F)$

We assume a bit more familiarity with fields in this section. Let $F$ be a field. Assume either that $F$ is finite or that $2 \neq 0$ in $F$. Let $\bar{F}$ be a fixed algebraic closure of $F$. We identify $F^\times$ with the center of $\mathrm{GL}_2(F)$, as in (19).

A **quadratic extension** of $F$ is a field $K$ such that $F \subset K \subset \bar{F}$ and $K$ is a two-dimensional $F$-vector space. This means $K = F \oplus F\lambda$ for some (any) $\lambda \in K - F$. The elements $1, \lambda, \lambda^2$ are then linearly

dependent over $F$ so we have a dependence relation $\lambda^2 - \mathsf{T}\lambda + \mathsf{N} = 0$, where $\mathsf{T} = \mathsf{T}(\lambda)$ and $\mathsf{N} = \mathsf{N}(\lambda)$ (the norm and trace) are elements of $F$. The roots of the polynomial $x^2 - \mathsf{T}x + \mathsf{N}$ are distinct; let $\bar{\lambda}$ be the root other than $\lambda$.

Using the basis $\{1, \lambda\}$ the action of $K^\times$ on $K$ by multiplication gives an embedding

$$\iota_\lambda : K^\times \hookrightarrow \mathrm{GL}_2(F).$$

For an arbitrary element $a + b\lambda \in K^\times$ we have $(a + b\lambda) \cdot 1 = a + b\lambda$ and

$$(a + b\lambda) \cdot \lambda = a\lambda + b\lambda^2 = a\lambda + b(\mathsf{T}\lambda - \mathsf{N}) = -b\mathsf{N} + (a + b\mathsf{T})\lambda.$$

Hence $\iota_\lambda$ is given explicitly by

$$\iota_\lambda(a + b\lambda) = \begin{bmatrix} a & -b\mathsf{N} \\ b & a + b\mathsf{T} \end{bmatrix}.$$

The eigenvalues of this matrix are $a + b\lambda$ and $a + b\bar{\lambda}$; in particular these eigenvalues lie in $K^\times$.

A different choice $\lambda'$ of $\lambda \in K - F$ gives a new basis of $K$ over $F$, and the subgroups $\iota_{\lambda'}(K^\times)$ and $\iota_\lambda(K^\times)$ are conjugate in $\mathrm{GL}_2(F)$. We denote any of these subgroups by $K^\times$, with the understanding that they are only determined up to conjugacy. If $L$ and $K$ are distinct quadratic extensions of $F$ the groups $L^\times$ and $K^\times$ are not conjugate in $\mathrm{GL}_2(F)$ and any two members in the class $L^\times$ or $K^\times$ will intersect in $F^\times$. This is because the eigenvalues of elements of $L^\times$ lie in $L$ and similarly for $K$, and $K \cap L = F$.

For $g, h \in \mathrm{GL}_2(F)$ we write $g \sim h$ to mean that $g$ and $h$ are conjugate in $\mathrm{GL}_2(F)$.

**Proposition 5.2** *Let $g \in \mathrm{GL}_2(F)$ have eigenvalues $\lambda, \mu$ in $\bar{F}$.*

1. *If $\lambda = \mu \in F^\times$, then either $g = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$ or $g \sim \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$.*
2. *If $\lambda \neq \mu \in F^\times$, then $g \sim \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix} \sim \begin{bmatrix} \mu & 0 \\ 0 & \lambda \end{bmatrix}$.*
3. *If $\lambda \neq \mu \notin F^\times$ then $\lambda$ and $\mu = \bar{\lambda}$ belong to a unique quadratic extension $K$ and $g \sim \iota_\lambda(\lambda) \sim \iota_\lambda(\bar{\lambda}) \in K^\times$.*

**Proof:** In case 1, the matrix $g - \lambda \cdot I_2$ has nonzero kernel. Choose any vector $v \in F^2$ such that the vector $u := (g - \lambda \cdot I_2)v$ is nonzero. Since $(g - \lambda \cdot I_2)^2 = 0$, the vectors $u, v$ are linearly independent. Using the basis $u, v$, we have $g \sim \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$.

In case 2, we use the basis of eigenvectors of $g$ to see that $g \sim \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}$.

In case 3, $\lambda$ and $\bar{\lambda}$ are the roots of the characteristic polynomial of $g$ so they generate a quadratic extension $K$ of $F$. The element $\iota_\lambda(\lambda) \in \iota_\lambda(K^\times)$ has the same eigenvalues. Hence $g$ and $\iota_\lambda(\lambda)$ are two

elements of $\mathrm{GL}_2(F)$ which are conjugate to $\begin{bmatrix}\lambda & 0\\ 0 & \bar{\lambda}\end{bmatrix}$ in $\mathrm{GL}_2(K)$. From the theory of rational canonical form, or Hilbert's theorem 90, it follows that $g$ and $\iota_\lambda(\lambda)$ are conjugate in $\mathrm{GL}_2(F)$.

■

If $F$ has no quadratic extensions, for example if $F = \mathbb{C}$ or if $F$ is the field of constructible numbers, then case 3 does not arise. If $F$ is finite, say $|F| = q$, then $F$ has only one quadratic extension $K$, and $|K| = q^2$. In this case there are $(q^2 - q)/2$ conjugacy classes of type 3.

# 6 Affine Groups

In space all points are the same: there is no natural origin. But the relative position of two points $P, Q$ in space can be described as a vector $v = \overrightarrow{PQ}$ indicating an arrow from $P$ to $Q$. Thus points are fixed in space, but vectors are the differences between points; another pair of points $R, S$ could be in the same relative position as $P, Q$, so that $\overrightarrow{PQ} = v = \overrightarrow{RS}$. In both cases we obtain $Q$ from $P$ and $S$ from $R$ by adding the difference $v$. Thus the group of vectors acts on the space of points.

Based on these intuitive notions from geometry and physics, we define an affine space as follows. Let $V$ be a finite dimensional vector space over a field $F$. Regard $V$ as an abelian group under addition. An *affine space under* $V$ is a set $A$ on which $V$ acts simply and transitively. We denote this action by $(v, a) \mapsto a + v$. Thus for any two points $P, Q \in A$ there is a unique vector $v$ such that $Q = v + P$. Traditionally one writes $v = \overrightarrow{PQ}$, as above. We will instead write $v = P - Q$.

For example, suppose $W$ is an $F$-vector space and $\lambda : W \to F$ is a linear functional which is not identically zero. Let $V = \ker \lambda$ and let $A = \{w \in W : \ \lambda(w) = 1\}$. Then $A$ is an affine space under $V$ via the addition of vectors in $W$.

## 6.1 Affine functions

Let $A$ and $A'$ be affine spaces under vector spaces $V$ and $V'$ respectively. A function $f : A \to A'$ is *affine* if there is a linear function, the *derivative*, $\dot{f} : V \to V'$ such that $f(a + v) = f(b) + \dot{f}(v)$ for any $a \in \mathcal{A}$ and $v \in V$.

For example, the derivative of an affine function $\psi : A \to \mathbb{R}$ is a linear functional $\dot{\psi} : V \to F$ such that

$$\psi(x + v) = \psi(x) + \dot{\psi}(v),$$

for all $x \in A$ and $v \in V$. The zero set $H_\psi = \{x \in A : \ \psi(x) = 0\}$ is an **affine hyperplane,** and $H_\psi = x_0 + \ker \dot{\psi}$, for any $x_0 \in H_\psi$. Two affine functions $\psi, \phi : A \to \mathbb{R}$ have $\dot{\psi} = \dot{\phi}$ if and only if $\psi \in \phi + \mathbb{R}$, and $H_\psi = H_\phi$ if and only if $\psi \in \mathbb{R} \cdot \phi$. Thus, an affine function $\psi$ is completely determined by its derivative $\psi$ and vanishing hyperplane $H_\psi$.

## 6.2 Affine Automorphisms

The set of affine automorphisms $g : A \to A$ forms a group under composition, denoted $\mathrm{Aff}(A)$. The given action of $V$ on $A$ is by affine automorphisms: each $v \in V$ gives an element $\tau_v \in \mathrm{Aff}(A)$ which is the translation $\tau_v(x) = x + v$. Thus we identify $V$ with the subgroup of translations in $\mathrm{Aff}(A)$.

The derivative of an affine automorphism $\gamma \in \mathrm{Aff}(A)$ is a linear automorphism $\dot{g} \in \mathrm{GL}(V)$ such that $g(x + v) = g(x) + \dot{g}(v)$ for all $x \in A$ and $v \in V$. Sending $g \mapsto \dot{g}$ gives a canonical homomorphism $\mathrm{Aff}(A) \to \mathrm{GL}(V)$. If $\dot{\gamma} = I_V$ is the identity element in $\mathrm{GL}(V)$ then $\gamma(x + v) = \gamma(x) + v$ for all $x \in A$ and $v \in V$. This implies that $\gamma$ is a translation. Indeed, choose any point $x_0 \in A$ and let $v_0 = \gamma(x_0) - x_0$. Now let $x \in A$ be arbitrary, and let $v = x - x_0$. Then $\gamma(x) = \gamma(x_0 + v) = \gamma(x_0) + v = (x_0 + v_0) + v = (x_0 + v) + v_0 = x + v_0$, so that $\gamma = t_{v_0}$. Thus, the translations form a normal subgroup of $\mathrm{Aff}(A)$ isomorphic to $V$ and we have an exact sequence

$$1 \to V \longrightarrow \mathrm{Aff}(A) \xrightarrow{g \mapsto \dot{g}} \mathrm{GL}(V).$$

The last map is surjective. To see this, we again choose a point $x_0 \in A$. Now given $g \in \mathrm{GL}(V)$, define $\gamma \in \mathrm{Aff}(A)$ by $\gamma(x) = x_0 + \gamma(x - x_0)$. We then have $\gamma(x+v) = x_0 + \gamma(x - x_0 + v) = \gamma(x) + g(v)$, so that $\dot{\gamma} = g$, as desired. Note that $\gamma$ belongs to the stabilizer $\mathrm{Aff}(A, x_0)$ of $x_0$ in $\mathrm{Aff}(A)$ and that $g \mapsto \gamma$ gives an isomorphism $\mathrm{GL}(V) \to \mathrm{Aff}(A, x_0)$, and we have a semidirect product

$$\mathrm{Aff}(A) = V \rtimes \mathrm{Aff}(A, x_0).$$

We have just seen that linear groups are contained in affine groups. On the other hand, affine groups are themselves contained in linear groups. As above, let $W$ be an $F$-vector space and let $\lambda : W \to F$ be a nonzero linear map, so that $A := \{x \in W : \ \lambda(x) = 1\}$ is an affine space under $V := \ker \lambda$. Let

$$\mathrm{GL}(W, \lambda) = \{g \in \mathrm{GL}(W) : \ \lambda(gw) = \lambda(w) \quad \forall w \in W\}.$$

Any $g \in \mathrm{GL}(W, \lambda)$ preserves both $A$ and $V$. If $x \in A$ and $v \in V$ we have $g(x + v) = g(x) + g(v)$. It follows that the restriction $g|_A$ is an affine automorphism with derivative $\dot{g} = g|_V$, the restriction of $g$ to $V$. Thus, restriction to $A$ defines a homomorphism

$$\mathrm{GL}(W, \lambda) \longrightarrow \mathrm{Aff}(A, \lambda).$$

This map is easily checked to be an *isomorphism*. That is, every affine automorphism of $A$ extends uniquely to a linear automorphism of $W$. For example, the translation $t_v(x) = x + v$ on $A$ (which is not linear on $W$) extends to the map $t_v(w) = w + \lambda(w)v$ (which is linear on $W$). Such linear maps $t_v$ are called **transvections**.

For example, let $W = \mathbb{R}^3$ with standard coordinates $x, y, z$ and let $\lambda = x+y+z$. Thus $V = \{(x, y, z) : x + y + z = 0\}$ and $A = \{(x, y, z) : \ x + y + z = 1\}$. We have $\mathrm{GL}(W) = \mathrm{GL}_3(\mathbb{R})$ and $\mathrm{GL}(W, \lambda)$ is the subgroup of matrices whose columns sum to 1.

The part of $A$ having $x, y, z \geq 0$ is an equilateral triangle in $A$ with vertices $P = (1, 0, 0)$, $Q = (0, 1, 0)$, $R = (0, 0, 1)$. In $\mathrm{Aff}(A)$ we have the reflections about the lines containing the sides of the triangle. Let $\ell$ be the line though $PQ$. Let $r_\ell \in \mathrm{Aut}(A)$ be the automorphism that moves a point to its mirror image

in $A$ on the other side of $\ell$. Then $r_\ell$ extends to a 180 degree rotation about $\ell$ in $W$. But this rotation is not linear: it moves $(0,0,0)$. The unique linear extension of $r_\ell$ has matrix

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & -1 \end{bmatrix}.$$

### 6.3 Euclidean Affine spaces

The affine space $A$ is *Euclidean* if $F = \mathbb{R}$ and $V$ has a positive definite inner product. We denote the inner product by $(u|v)$, for $u, v \in V$. The **orthogonal group** $O(V)$ is the subgroup of $\mathrm{GL}(V)$ preserving the inner product. That is,

$$\mathrm{O}(V) = \{g \in \mathrm{GL}(V) : \ (gu, gv) = (u, v) \quad \forall\, u, v \in V\}$$

An affine automorphism $f : A \to A$ is an **isometry** if $\dot{f} \in \mathrm{O}(V)$. We write $\mathrm{E}(A)$ for the group of isometries of $A$. For any $x \in A$ the stabilizer $\mathrm{E}(A, x)$ is isomorphic to $\mathrm{O}(V)$ and we have a semidirect product

$$\mathrm{E}(A) = V \rtimes \mathrm{E}(A, x).$$

## 7 Projective Groups

A set $X$ has Projective Geometry if $X$ admits a transitive action by the group $\mathrm{PGL}_{n+1}(F)$ for some integer $n \geq 1$ and some field $F$.

The first example is the projective space $\mathbb{P}^n$, whose points are lines in an $F$-vector space $V$ of dimension $n+1$. A line is determined by a nonzero vector in it, so we denote points in $\mathbb{P}^n(F)$ as $[v]$, where $v \in V$ is a nonzero vector and $[cv] = [v]$, where $c \in F^\times$.

The group $\mathrm{GL}(V)$ acts on $\mathbb{P}^n$ by $g \cdot [v] = [g \cdot v]$. Note that the center of $\mathrm{GL}(V)$ acts trivially, so this action factors through the quotient group $\mathrm{PGL}(V) \simeq \mathrm{PGL}_{n+1}(V)$. Thus, projective space has projective geometry.

There are other examples: Instead of lines we could consider the set $X_k$ of subspaces of some fixed dimension $k \in [1, n]$. Again $\mathrm{GL}(V)$ acts transitively on $X_k$ and the action factors through $\mathrm{PGL}(V)$.

Then we can refine. For example, suppose $\dim V = 3$, and let $X$ be the set of pairs $(\ell, P)$, where $\ell$ is a line in $V$, $P$ is a plane in $V$, and $\ell \subset P$. Again the group $\mathrm{PGL}(V)$ acts transitively on $X$.

Taking this to the extreme, let $\dim V = n+1$ and let $\mathbb{F}_n$ be the set of sequences of subspaces $(V_1, V_2, \ldots, V_n)$ of $V$ such that $\dim V_k = k$ and $V_k \subset V_{k+1}$ for $1 \leq k < n$. An element of $\mathbb{F}_n$ is called a **flag** in $V$, by analogy with polyhedra, where a flag is a vertex contained in an edge contained in a face, like an ordinary flag. Again the group $\mathrm{GL}(V)$ acts transitively on $\mathbb{F}_n$ and this action factors

through $\mathrm{PGL}(V)$. A **Borel subgroup** is the stabilizer in $\mathrm{GL}(V)$ or $\mathrm{PGL}(V)$ of a flag in $V$. That is, the stabilizer of $(V_1, V_2, \ldots, V_n) \in \mathbb{F}_n$ is the Borel subgroup

$$B = \{b \in G : \ bV_k = V_k \quad \forall 1 \leq k \leq n\},$$

and we have a $\mathrm{GL}(V)$-equivariant bijection

$$\mathrm{GL}(V)/B \xrightarrow{\sim} \mathbb{F}_n.$$

Each ordered basis $(e_0, \ldots, e_n)$ of $V$ determines a flag $(V_1, \ldots, V_n) \in \mathbb{F}_n$ where $V_k$ is spanned by $(e_0, \ldots, e_{k-1})$. Using this basis we may identify $\mathrm{GL}(V) = \mathrm{GL}_{n+1}(F)$, and then $B$ is identified with the subgroup of upper triangular matrices in $\mathrm{GL}_{n+1}(F)$.

## 7.1 The Bruhat decomposition

Elements in $\mathrm{GL}_n(F)$ are matrices whose determinant is nonzero. However, it is not obvious how to write down the general such matrix. That is, we have the locus, but not the parametrization of $\mathrm{GL}_n(F)$ in the space of all $n \times n$ matrices. The Bruhat decomposition remedies this by partitioning $\mathrm{GL}_n(F)$ into $B - B$ double cosets, called **Bruhat cells** which can themselves be parameterized.

This is easy to see for $n = 2$. Consider the upper triangular subgroup

$$B = \begin{bmatrix} \times & * \\ 0 & \times \end{bmatrix} \subset \mathrm{GL}_2(F).$$

One checks that if $g \in \mathrm{GL}_2(F)$ has nonzero lower left entry then there are elements $b_1, b_2 \in B$ such that $g = b_1 \sigma b_2$, where $\sigma$ is the permutation matrix

$$\sigma = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Thus $\mathrm{GL}_2(F)$ is partitioned as

$$\mathrm{GL}_2(F) = B \ \sqcup \ B\sigma B.$$

This generalizes to $\mathrm{GL}_n(F)$ as follows. We have seen that the we may identify the symmetric group $S_n$ as a subgroup of $\mathrm{GL}_n(F)$, whereby the permutation $\sigma$ becomes the matrix sending $e_i \mapsto e_{\sigma(i)}$. We also have the subgroup $B < \mathrm{GL}_n(F)$ consisting of upper triangular matrices with all diagonal entries nonzero.

**Theorem 7.1 (Bruhat Decomposition)** *The group $G = \mathrm{GL}_n(F)$ is a disjoint union*

$$G = \bigsqcup_{\tau \in S_n} B\tau B,$$

*where $B\tau B = \{b_1 \tau b_2 : \ b_i \in B\}$.*

**Proof:** The result is obvious for $n = 1$ and we have seen that it is is true for $n = 2$. We now assume the result is true for $\mathrm{GL}_n(F)$, and use induction.

Let $V$ be an $n+1$-dimensional vector space over $F$. To prove the theorem we study the action of $G = \mathrm{GL}(V)$ on the projective space $\mathbb{P}^n$ of lines in $V$ through the origin. See section 4 for background on group actions.

A typical point in $\mathbb{P}^n$ is a line $[v]$ through a nonzero vector $v \in V$ and $[cv] = [v]$ if $c \in F^\times$. The group $G$ acts on $V$ via $g \cdot [v] = [gv]$. This action is transitive: if $v \in V$ is nonzero then $v$ is contained in a basis of $V$ so there is an element $g \in G$ such that $ge_0 = v$, hence $g \cdot \ell_0 = [v]$.

We choose an ordered basis $e_0, e_1, \ldots, e_n$ of $V$, and will often regard elements of $G$ as matrices with respect to this basis. We also write $[v] = [x_0, x_1, \ldots, x_n]$ for the line through $v = \sum x_k e_k$. Our choice of basis also determines particular lines $\ell_k = [e_k] \in \mathbb{P}^n$ which play a key role in what follows. The ordering of the basis determines subspaces $V_k = \ell_0 + \cdots + \ell_{k-1}$, the span of the first $k$ lines. In turn these subspaces determine the subgroup preserving each $V_k$:

$$B = \{b \in G : \ bV_k = V_k \ \forall k\}.$$

The elements of $B$ are precisely those whose matrices with respect to the ordered basis $\{e_k\}$ are upper triangular.

The transitive action of $G$ on $\mathbb{P}^n$ restricts to an action of $B$ which is no longer transitive: each $B$-orbit contains a unique line $\ell_k$ and the $B$-orbit of $\ell_k$ is the subset

$$\mathcal{O}_k := B \cdot \ell_k = \{[v + e_k] : \ v \in V_k\}.$$

Thus $\mathcal{O}_0 = \ell_0$ is a single point in $\mathbb{P}^n$ and in general $\mathcal{O}_k$ is an affine space of dimension $k$. The whole projective space is partitioned into $B$-orbits as

$$\mathbb{P}^n = \bigsqcup_{k=0}^{n} \mathcal{O}_k.$$

We have a parallel partition of the symmetric group $S_{n+1}$ on $\{0, 1, \ldots, n\}$, as follows. For each $1 \leq k \leq n$ we have a descending cycle $\sigma_k = (k \ k-1 \ \cdots \ 2 \ 1 \ 0)$. Since $\sigma_k(0) = k$, it follows that

$$S_{n+1} = \bigsqcup_{k=0}^{n} \sigma_k S_n, \tag{23}$$

where $S_n$ is the symmetric group on $\{1, 2, \ldots, n\}$, regarded as the stabilizer of $0$ in $S_{n+1}$.

Regarding $S_{n+1} < G$, we also have $\sigma_k \cdot \ell_0 = \ell_k$. It follows that

$$G = \bigsqcup_{k=0}^{n} B\sigma_k P,$$

where $P$ is the stabilizer in $G$ of the line $\ell_0$. We note that $P = G_1 \ltimes Q$, where $G_1 \simeq \mathrm{GL}_n(F)$ is the subgroup of $G$ fixing $e_0$ and preserving the span of $\{e_1, \ldots, e_n\}$ and $Q = \{g \in G : \ (g-1)V \subset \ell_0\}$. By induction we have

$$G_1 = \bigsqcup_{\sigma \in S_n} B_1 \sigma B_1,$$

where $B_1 = B \cap G_1$. Note also that $B_1 Q = B$. It follows that

$$G = \bigsqcup_{k=0}^{n} B\sigma_k G_1 Q = \bigsqcup_{k=0}^{n} \bigsqcup_{\sigma \in S_n} B\sigma_k B_1 \sigma B.$$

Now for $1 \leq i$ we have

$$\sigma_k(i) = \begin{cases} i-1 & \text{if } 1 \leq i \leq k \\ i & \text{if } k < i \leq n \end{cases}$$

so if $1 \leq i < j$ then $\sigma_k(i) < \sigma_k(j)$. By Lemma 5.1 we have that $\sigma_k B_1 \sigma_k^{-1} \subset B$. It follows that

$$G = \bigsqcup_{k=0}^{n} \bigsqcup_{\sigma \in S_n} B\sigma_k \sigma B = \bigsqcup_{\sigma \in S_{n+1}} B\sigma B,$$

by (23), as desired. ■

Thus $G$ is partitioned into **Bruhat cells** $B\sigma B$, in each of which one can write down every element. However, in a given cell $B\sigma B$ it is possible to have $b_1 \sigma b_2 = b_1' \sigma b_2'$ for $b_i \neq b_i'$.

We can sharpen the Bruhat decompositon to obtain uniqueness of expression. We continue with $V$ of dimension $n+1$ and our choice of ordered basis $\{e_0, \ldots, e_n\}$, as in the proof of Thm. 8.10. Recall that $V_k = \ell_0 + \cdots + \ell_{k-1}$ is the span of the first $k$ basis elements. As a first step, we note that $B = UT = TU$, where

$$T = \{t \in G : \ t \cdot \ell_k = \ell_k \quad \forall\, k\} \qquad \text{and} \qquad U = \{u \in G : \ u \cdot e_k \in e_k + V_k \quad \forall\, k\}$$

and that $S_{n+1}$ normalizes $T$. Hence

$$B\sigma B = UT\sigma B = U\sigma T B = U\sigma B.$$

However it is still possible to have $u\sigma b = u'\sigma b'$ for distinct $u, u'$ and $b, b'$, so we must refine further.

For each $k \in [0, n]$ let

$$U_k = \{u \in B : \ ue_k \in e_k + V_k \quad \text{and} \quad ue_j = e_j \ \forall j \neq k\}.$$

If $u \in U_k$ then $ue_k = e_k + v$ for a unique $v \in V_k$. One checks that $U_k$ is a subgroup of $B$ and that the assignment $u \mapsto v$ is an isomorphism $U_k \xrightarrow{\sim} V_k$, where $V_k$ is regarded as an abelian group (under vector addition). We see that $U_k$ acts *simply and transitively* on the $B$-orbit $\mathcal{O}_k$ in $\mathbb{P}^n$. With this observation we now re-examine the proof of Thm. 8.10 to obtain the following sharper form of the Bruhat decomposition.

For each $k \in [0, n]$ let $V^k$ be the span of the $e_j$ for $k \leq j \leq n$, so that $V = V_k \oplus V^k$, and let

$$G_k = \{g \in G : \ gv = v \ \ \forall v \in V_k \quad \text{and } gV^k = V^k\}.$$

Thus, we have $G = G_0 > G_1 > \cdots > G_n$ and $G_k \simeq \mathrm{GL}(V^k)$. Noting that $\ell_k \subset V^k$, let $P_k$ be the stabilizer of $\ell_k$ in $G_k$ and let $Q_k = \{q \in G_k : \ (q-1)V^k \subset \ell_k\}$. We have $P_k = G_{k+1} \ltimes Q_k$.

**Theorem 7.2** *Let $\sigma$ in $S_{n+1}$ have descending decomposition $\sigma = \sigma_1 \cdots \sigma_n$, corresponding to the $n$-tuple of integers $(k_1, \ldots, k_n)$ as in Prop. 3.2. Then for each $g \in B\sigma B$ there exist unique elements $u_i \in U_{k_i} \cap G_{i-1}$ and an element $b \in B$ such that*

$$g = u_1\sigma_1 \cdot u_2\sigma_2 \cdots u_n\sigma_n \cdot b.$$

**Proof:**

The following algorithm gives a constructive proof of the theorem.

1. Let $k_1 \in [0, n]$ be the unique index such that $g \cdot \ell_0 \in \mathcal{O}_{k_1}$.

2. Let $u_1 \in U_{k_1}$ be the unique element such that $g \cdot \ell_0 = u_1 \cdot \ell_{k_1}$.

3. Let $\sigma_1 = (k_1 \ \ldots 2\ 1\ 0) \in S_{n+1}$. This is the unique descending cycle such that $\sigma_1 \cdot \ell_0 = \ell_{k_1}$. We now have

$$g \cdot \ell_0 = u_1\sigma_1 \cdot \ell_0,$$

so $g = u_1\sigma_1 \cdot p_0$ for a unique element $p_0 \in P_0$.

4. Let $g_1 \in G_1$ and $q_0 \in Q_0$ be the unique elements such that $p_0 = g_1q_0$. We now have

$$g = u_1\sigma_1 \cdot g_1q_0.$$

5. Repeat steps 1-4 with $g$ replaced by $g_1$ and $\ell_0$ replaced by $\ell_1$. This gives a unique index $k_2 \in [1, n]$ and element $u_2 \in U_{k_2} \cap G_1$ such that $g_1 \cdot \ell_1 = u_2 \cdot \ell_1 \in \mathcal{O}_{k_2}$, and the decending cycle $\sigma_2 = (k_2 \ \ldots 2\ 1)$ such that $\sigma_2 \cdot \ell_1 = \ell_{k_2}$, so that $g_1 = u_2\sigma_2 \cdot p_1$ for a unique element $p_1 \in P_1$. Writing $p_1 = g_2q_1$ for unique $g_2 \in G_2$ and $q_1 \in Q_1$ we have

$$g = u_1\sigma_1 \cdot u_2\sigma_2 \cdot g_2q_1q_2.$$

We eventually get

$$g = u_1\sigma_1 \cdot u_2\sigma_2 \cdots u_n\sigma_n \cdot b,$$

where $u_i \in U_{k_i} \cap G_{i-1}$ and $b = q_1q_2 \cdots q_n \in B$, with uniqueness at every step. ■

Thm. 7.2 gives a unique expression for every element in $B\sigma B$. We will next see that the product $u_1\sigma_1 \cdot u_2\sigma_2 \cdots u_n\sigma_n$ lies in $U\sigma$, and we will characterize which elements of $U\sigma$ are of this form.

Let $\overline{U}$ be the transpose of $U$. Note that $\overline{U} \cap B = \{1\}$.

**Corollary 7.3** *Every element $g \in B\sigma B$ may be uniquely expressed as $g = u\sigma b$ where $u \in U \cap \sigma\overline{U}\sigma^{-1}$ and $b \in B$.*

**Proof:** We have

$$u_1\sigma_1 \cdot u_2\sigma_2 \cdots u_n\sigma_n \cdot B = u\sigma B,$$

where

$$u = u_1(\sigma_1u_2\sigma_1^{-1})(\sigma_1\sigma_2u_3\sigma_2^{-1}\sigma_1^{-1}) \cdots (\sigma_1 \cdots \sigma_{n-1}u_n\sigma_{n-1}^{-1} \cdots \sigma_1^{-1}).$$

I claim that each term in parentheses belongs to $U$. Since each $u_q$ has all eigenvalues equal to 1, it suffices to show that each term is in $B$. As in section **??**, let $R$ be the set of ordered pairs $(i,j)$ of distinct integers in $[0,n]$, and let $R^+ = \{(i,j) \in R : \ i < j\}$, $R^- = \{(i,j) \in R : \ i > j\}$. For any $g \in G$ let $R(g) = \{(i,j) : \ g_{ij} \neq 0\}$. Since $B = \{b \in G : \ R(b) \subset R^+\}$, we must show that $R(u) \subset R^+$.

For $0 \leq q < n$ we have $R(u_{q+1}) = \{(i, k_q) : \ q \leq i < k_q\}$. From Lemma 11 we have

$$\sigma_1\sigma_2 \cdots \sigma_q R(u_{q+1}) \subset R^+$$

for all $1 \leq q < n$. The claim now follows from Lemma 5.1.

Next the element $\sigma^{-1}u\sigma$ is a product of terms of the form

$$x_p = \sigma_n^{-1}\sigma_{n-1}^{-1} \cdots \sigma_p^{-1} u_p \sigma_p \cdots \sigma_{n-1}\sigma_n$$

for $p \in [1,n]$. One checks that

$$\sigma_p^{-1} R(u_p) = \{(p, p-1), (p+1, p-1), \ldots, (k_p, p-1)\}.$$

If $q > p$ then $\sigma_q^{-1} = (q-1, q, \ldots, k_q)$ fixes $p-1$ and preserves $[p,n]$. It follows that

$$R(x_p) = \sigma_n^{-1}\sigma_{n-1}^{-1} \cdots \sigma_p^{-1} R(u_p) \subset R^-$$

so $x_p \in \overline{U}$. It follows that $u \in \sigma\overline{U}\sigma^{-1}$, as claimed.

If $u\sigma b = u'\sigma b'$ with $u, u'$ both in $U \cap \sigma\overline{U}\sigma^{-1}$ then $b(b')^{-1} = \sigma^{-1}uu'\sigma \in B \cap \overline{U} = \{1\}$. It follows that $b = b'$ and $u = u'$, so we have uniqueness of expression.

■

Note that

$$U \cap \sigma\overline{U}\sigma^{-1} = \{u \in U : \ R(u) \subset N(\sigma^{-1})$$

so that $U \cap \sigma\overline{U}\sigma^{-1}$ is an affine space of dimension equal to the length $\ell(\sigma)$.

We have already seen that $S_{n+1}$ has a unique longest element $\tilde{\sigma} = (n \ \cdots 0)(n \ \cdots \ 1)\cdots(n \ n-1)$. It has order two. As a matrix, $\tilde{\sigma}$ is the unique permutation matrix with the property that $U \cap \tilde{\sigma}\overline{U}\tilde{\sigma} = U$ is maximal. The Bruhat cell $U\tilde{\sigma}B$ is called the **big cell**. If we multiply the big cell on the left by $\tilde{\sigma}$ we obtain

$$\tilde{\sigma}U\tilde{\sigma}B = \overline{U}B.$$

These are the matrices admitting an "LU" decomposition, as it is called in elementary linear algebra. The matrices which have no LU decomposition are exactly those in the translates $\tilde{\sigma}U\sigma B$ for $\sigma \neq \tilde{\sigma}$.

**Example:** We give the explicit Bruhat decomposition for $G = \mathrm{GL}_3(F)$. Let $\Delta_1, \Delta_2$ be the functions on $G$ given for $g = [g_{ij}]$ by

$$\Delta_1(g) = g_{31}, \qquad \Delta_2(g) = g_{21}g_{32} - g_{31}g_{22}.$$

One checks that for $b, b' \in B$ we have $\Delta_i(bgb') = \chi_i(b,b')\Delta_i(g)$ where $\chi_i(b,b') \in F^\times$. It follows that the zero-sets $Z_i$ of $\Delta_i$ are unions of Bruhat cells. Writing elements of $S_3$ in their descending cycle decomposition, let

$$W_1 = \{(1\,0)(2\,1), (1\,0), (2\,1), e\}, \qquad W_2 = \{(2\,1\,0), (1\,0), (2\,1), e\}.$$

Using the algorithm in the proof above we find that

$$Z_i = \bigsqcup_{\sigma \in W_i} B\sigma B, \quad \text{so} \quad Z_1 \cap Z_2 = \bigsqcup_{\sigma \in W_1 \cap W_2} B\sigma B,$$

and also (using the notation of the proof) that $B \sqcup B(1\,0)B = P_0$, $B \sqcup B(2\,1)B = P_1$. One can now decide which Bruhat cell contains a given $g \in G$ according to the vanishing of certain minors.

# 8 Abelian Groups

We give brief introductions to the most fundamentally important groups here.

## 8.1 Cyclic groups

Let $\mathbb{Z}$ be the group of integers under addition, with identity element $0$. Since addition of integers is commutative, the group $\mathbb{Z}$ is abelian. Using the division algorithm, one proves that for any subgroup $H \leq \mathbb{Z}$, there is an integer $n \geq 0$ such that $H = n\mathbb{Z}$, the set of multiples of $n$. If $n = 0$ we have $H = \{0\}$. Assume now that $n \geq 1$. Then the quotient $\mathbb{Z}/n\mathbb{Z}$ is finite of order $n$, and consists of the cosets $n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}$. The subgroups of $\mathbb{Z}/n\mathbb{Z}$ correspond to the subgroups of $\mathbb{Z}$ containing $n\mathbb{Z}$. These are the subgroups $d\mathbb{Z}/n\mathbb{Z}$, for positive integers $d \mid n$. Note that multiplication by $d^{-1}$ induces an isomorphism

$$d\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/d^{-1}n\mathbb{Z}.$$

Every subgroup is normal in $\mathbb{Z}$, and we have

$$(\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/d\mathbb{Z}.$$

Cyclic groups play an important role in any group $G$. For each element $g \in G$ determines a homomorphism

$$e_g : \mathbb{Z} \to G, \qquad \text{given by} \qquad e_g(n) = g^n.$$

The image of $e_g$ is the subgroup generated by $g$

$$\operatorname{im} e_g = \langle g \rangle = \{g^n : \ n \in \mathbb{Z}\}.$$

The kernel of $e_g$ is a subgroup of $\mathbb{Z}$, hence is of the form $m\mathbb{Z}$, for some integer $m \geq 0$. If $m = 0$ then $g$ has infinite order and $\langle g \rangle \simeq \mathbb{Z}$. If $m > 0$ then $m$ is the order of $g$.

A group $G$ is **cyclic** if $G = \langle g \rangle$ for some $g \in G$. That is, $G$ is cyclic iff there exists $g \in G$ such that every element of $G$ is a power of $g$. We can also say that $G$ is cyclic iff there exists $g \in G$ such that the homomorphism $e_g : \mathbb{Z} \to G$ is surjective.

We have seen that every infinite cyclic group $G$ is isomorphic to $\mathbb{Z}$, and every finite cyclic group of order $n$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Usually we will encounter cyclic groups while we are working with multiplicative notation, where we will let $C_n$ denote a generic cyclic group of order $n$. Thus, $C_n = \langle g \rangle$, for any element $g \in G$ of order $n$.

Since $C_n \simeq \mathbb{Z}/n\mathbb{Z}$, it is immediate from our discussion of $\mathbb{Z}$ and its subgroups that $C_n$ has a unique subgroup of every order $d$ dividing $n$, namely $\langle g^d \rangle \simeq C_d$. Every subgroup of $C_n$ is of this form and we have

$$C_n/C_d \simeq C_{n/d}.$$

This is a complete description of all of the subgroups and quotients of $C_n$.

**Example:** Let $m, n$ be positive integers. The subgroups $C_n[m] = \{x \in C_n : x^m = 1\}$ and $(C_n)^m = \{x^m : x \in C_n\}$ of $C_n$ are the kernel and image of the homomorphism $C_n \xrightarrow{m} C_n$ sending $x \mapsto x^m$, so these fit into the exact sequence

$$1 \longrightarrow C_n[m] \longrightarrow C_n \longrightarrow (C_n)^m \longrightarrow 1.$$

If $g$ is a generator of $C_n$, one can check that $C_n[m] = \langle g^{n/d} \rangle$, where $d = \gcd(m, n)$. Thus, $C_n[m] \simeq C_d$ and $(C_n)^m \simeq C_{n/d}$.

A final remark on cyclic groups: The word "isomorphic" does not mean "equal". We have $\mathbb{Z}/n\mathbb{Z} \simeq C_n$, but there is a subtle distinction between these groups: Note that $\mathbb{Z}/n\mathbb{Z}$ has a canonical generator, namely $1 + n\mathbb{Z}$. But $C_n$ has no canonical generator. For if $\langle g \rangle$ generates $C_n$ then so does $g^k$ for any integer $k$ with $\gcd(k, n) = 1$ (exercise...). For example, if

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \right\}$$

then $G \simeq C_3$ and either nonidentity matrix generates $G$, but there is no natural preference for either generator. The root of this issue is that the isomorphism $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} C_n$ induced by $e_g$ depends on the choice of generator $g$ of $C_n$; a different choice would give a different isomorphism. An isomorphism of this sort, which depends on one or more arbitrary choices, is called **noncanonical**.

## 8.2 Finite abelian groups

Every finite abelian group is a direct product of cyclic groups. The first basic result in this direction is as follows.

**Proposition 8.1** *Let $A, B, C$ be finite abelian groups fitting into the exact sequence*

$$1 \longrightarrow A \longrightarrow C \xrightarrow{\pi} B \longrightarrow 1.$$

*Assume that the orders of $A$ and $B$ are relatively prime. Then $C \simeq A \times B$.*

**Proof:** Set $m = |A|$ and $n = |B|$, so that $|C| = mn$. Let $D$ be the set of elements in $C$ whose order is relatively prime to $m$. Then $D \cap A = \{1\}$. I claim that $\pi(D) = B$. Let $b \in B$ and choose $c \in C$ such that $\pi(c) = b$. Since $|C| = mn$ we have $(c^m)^n = 1$, so the order of $c^m$ divides $n$, which is relatively prime to $m$. Hence $c^m \in D$, and $\pi(c^m) = b^m$. But the map $x \mapsto x^m$ is an automorphism of $B$, again since $\gcd(m, n) = 1$. Hence $\pi(D) = B^m = B$. It follows that $C = AD$, and that $\pi$ maps $D$ isomorphically onto $B$. By Prop. 2.10 we have

$$C = A \times D \simeq A \times B.$$

■

However, a direct product decomposition of an abelian group need not be unique.

**Proposition 8.2** *Suppose $n_1, n_2, \ldots, n_k$ are relatively prime integers with product $n = n_1 n_2 \cdots n_k$. Then*

$$C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k} \simeq C_n.$$

**Proof:** Let $g_i$ be a generator of $C_{n_i}$ for each $i$. I claim that the element $(g_1, g_2, \ldots, g_k) \in C_{n_1} \times \cdots \times C_{n_k}$ has order $n$. We have $(g_1, g_2, \ldots, g_k)^n = (g_1^n, g_2^n, \ldots, g_k^n) = (1, 1, \ldots, 1)$, since $n_i \mid n$ for all $i$. And if $g_i^m = 1$ for all $i$ then $n_i \mid m$ for all $i$, so $n \mid m$, since the $n_i$ are relatively prime. Hence $n$ is the order of $(g_1, g_2, \ldots, g_k)$. ■

We can get a unique decomposition of a finite abelian group $G$ as follows. For each prime $p$ let $G(p)$ be the set of elements of $G$ whose order is a power of $p$.

**Theorem 8.3** *Let $G$ be a finite abelian group of order $n$. Then*

1. *$G \simeq \prod_{p|n} G(p)$ is the direct product of its nontrivial subgroups $G(p)$.*
2. *For each prime $p$ there exist unique positive integers $e_1 \geq e_2 \geq \cdots \geq e_k > 0$ such that $e_1 + e_2 + \cdots + e_k$ is the power of $p$ dividing $n$ and*

$$G(p) \simeq C_{p^{e_1}} \times C_{p^{e_2}} \times \cdots \times C_{p^{e_k}}.$$

**Proof:** Part 1 follows from Prop. 8.2, using induction on the number of primes dividing $|G|$. We will prove part 2 later, using modules over principal ideal domains. See Milne for an elementary proof. ■

**Example 1:** If $n = p_1 p_2 \cdots p_k$ is a product of distinct primes, then there is only one abelian group of order $n$, up to isomorphism, namely $C_n$. For the unique decomposition of Thm. 8.3 would be

$$G \simeq C_{p_1} \times C_{p_2} \times \cdots \times C_{p_k},$$

which is isomorphic to $C_n$, by Prop. 8.2.

**Corollary 8.4** *A finite subgroup of the multiplicative group of a field is cyclic.*

**Proof:** Let $F$ be a field and let $G$ be a finite subgroup of the multiplicative group $F^\times$. If $n$ is a positive integer and $g \in G$ has order dividing $n$, then $g$ is a root of the polynomial $x^n - 1$, which has at most $n$ roots in $F$. Hence $G$ has at most $n$ elements of order dividing $n$, for any $n \geq 1$. Write $G = \prod_p G(p)$, according to part 1 of Thm. 8.3. Each $G(p)$ has at most $p$ elements of order dividing $p$. Hence $G(p)$ is cyclic, by part 2 of Thm. 8.3. Now $G$ is cyclic, by Prop. 8.2. ■

**Example 2:** If $F$ is a finite field with $|F| = q$, then $F^\times \simeq C_{q-1}$. Consequently, for any positive integer $m$ the subgroup $\mu_m(F) = \{x \in F : \ x^m = 1\}$ is also cyclic, of order $\gcd(m, q-1)$:

$$\mu_n(F) \simeq C_{\gcd(m,q-1)} \tag{24}$$

### 8.2.1 Unit Groups

Let $m$ be a positive integer and consider $\mathbb{Z}/m\mathbb{Z}$ under multiplication (that is, as a ring):

$$(k + m\mathbb{Z})(k' + m\mathbb{Z}) = kk' + m\mathbb{Z},$$

which is a well-defined operation. It is not a group operation, however, since the element $0+m\mathbb{Z}$ has no multiplicative inverse. In fact, from the Euclidean algorithm it follows that $k+m\mathbb{Z}$ has a multiplicative inverse in $\mathbb{Z}/m\mathbb{Z}$ iff $\gcd(k, m) = 1$. Hence the set

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{k + m\mathbb{Z} : \ \gcd(k, n) = 1\}$$

forms a group under multiplication in $\mathbb{Z}/m\mathbb{Z}$, with identity element $1 + m\mathbb{Z}$. Since multiplication in $\mathbb{Z}$ is commutative, the group $(\mathbb{Z}/m\mathbb{Z})^\times$ is abelian, of order

$$\phi(m) = \{k \in \mathbb{Z} : \ 1 \leq k < m, \ \gcd(k, m) = 1\}.$$

**Proposition 8.5** *Let $m = p_1^{r_1} \cdots p_k^{r_k}$ be the factorization of $m$ into a product of powers of distinct primes $p_i$. Then*

1. $$(\mathbb{Z}/m\mathbb{Z})^\times \simeq \prod_{i=1}^{k} (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times.$$

2. *For any prime $p$ and integer $r \geq 1$ we have*

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \simeq \begin{cases} C_{(p-1)p^{r-1}} \simeq C_{p-1} \times C_{p^{r-1}} & \text{if } p \geq 3 \\ C_2 \times C_{2^{r-2}} & \text{if } p = 2 \text{ and } r \geq 2 \\ 1 & \text{if } p = 2 \text{ and } r = 1. \end{cases}$$

**Proof:** Part 1 follows from the Chinese Remainder Theorem. We prove part 2 for $p \geq 3$ and leave $p = 2$ as an exercise. Reduction modulo $p$ gives a surjective map

$$\pi : (\mathbb{Z}/p^r\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times.$$

By Prop. 8.2 and Example 2 above, it suffices to show that $\ker \pi$ is cyclic. Clearly $1+p \in \ker \pi$. We will show that $1+p$ has order $p^{r-1}$ modulo $p^r$.

Recall that $p \mid \binom{p}{k}$ for all positive integers $k < p$. Now if $a$ and $b$ are congruent integers modulo some power $p^\ell$, it follows that $a^p \equiv b^p \mod p^{\ell+1}$. Now using induction on $\ell \geq 2$ we have

$$(1+p)^{p^{\ell-2}} \equiv 1 + p^{\ell-1} \mod p^\ell,$$

which implies that $1+p$ has order $p^{\ell-1}$ modulo $\ell$ for any $\ell \geq 2$. ■

## 8.3 The dihedral groups $D_n$

A **dihedral group** is a group generated by two distinct elements of order two. As the name indicates, they arise naturally from pairs of reflections in affine spaces.

A **reflection** is an isometry of a Euclidean space $E$ whose set of fixed-points in $E$ is a hyperplane. Suppose $E$ is a plane. Each line $\ell$ in $E$ determines a reflection $r$ with fixed-point set $\ell$. If $P$ is a point not on $\ell$, then $r(P)$ is the mirror image of $P$ with respect to $\ell$. We say that $r$ is the "reflection about $\ell$". Note that $r$ is a nontrivial involution of the isometry group of the plane.

Suppose $\ell$ and $\ell'$ are two lines in the plane, with reflections $r$ and $r'$. If $\ell$ and $\ell'$ are not parallel, then they meet in a point $P$, and the product $rr'$ is rotation about twice the angle at $P$ from $\ell'$ to $\ell$. In particular, $r$ and $r'$ commute precisely when $\ell$ and $\ell'$ are perpendicular. If $\ell$ and $\ell'$ are parallel, the product $rr'$ is translation by twice the perpendicular vector from $\ell'$ to $\ell$.

For any integer $n \geq 1$ consider $n$ lines $\ell_1, \ldots, \ell_n$ in the plane meeting in a common point, with equal angles ($= \pi/n$) between adjacent lines. Let $r_i$ be the reflection about $\ell_i$. The *dihedral group* $D_n$ is the group generated by the reflections $r_1, \ldots, r_n$. We define $D_\infty$ similarly, by taking a countable number of parallel lines equally spaced apart (all meeting at infinity, with equal angle zero).

For $n = 1$ we have just one line, with reflection $r$ and

$$D_1 = \{1, r\} \simeq C_2.$$

For $n = 2$ we have two perpendicular lines $\ell_1, \ell_2$, whose reflections $r_1, r_2$ commute. Hence

$$D_2 = \{1, r_1, r_2, r_1 r_2\} \simeq C_2 \times C_2.$$

For $n = 3$ we have three lines $\ell_1, \ell_2, \ell_3$ intersecting at the angle $\pi/3$. Let $r, s$ be reflections about adjacent lines. Then $rs$ is a rotation of order $2\pi/3$, hence has order three. The equation $(rs)^3 = 1$ can be written as

$$rsr = srs.$$

This element $rsr = srs$ is the third reflection. It follows that $D_3$ is generated by $r$ and $s$ only, and its elements are

$$D_3 = \{1, r, s, rs, sr, rsr\}.$$

The product of any two elements in $D_3$ is completely determined by the three rules:

$$r^2 = 1, \qquad s^2 = 1, \qquad rsr = srs.$$

For example, we have $rs \cdot rsr = rs \cdot srs = r \cdot rs = s$.

It is a similar story for an arbitrary finite $n \geq 2$. We again let $r, s$ be reflections about adjacent lines $\ell_r, \ell_s$, so that $rs$ is a rotation by $2\pi/n$ and hence has order $n$. The equation $(rs)^n = 1$ can be written as

$$\underbrace{rsrs\ldots}_{n \text{ terms}} = \underbrace{srsr\ldots}_{n \text{ terms}}$$

The element $srs$ is reflection about the line $s(\ell_r)$, which is the other line adjacent to $s$. It follows that all reflections can be written in terms of $r$ and $s$, as $s(rs)^i$ for some $1 \leq i \leq n$ and that the elements of $D_n$ are

$$D_n = \{(rs)^i, s(rs)^i : \ 1 \leq i \leq n\}$$

and $|D_n| = 2n$. The element $t = rs$ generates a cyclic subgroup $\langle t \rangle \simeq C_n$, consisting of all rotations in $D_n$, which has index two in $D_n$. The reflections in $D_n$ are precisely the elements outside of $\langle t \rangle$, and for any reflection $r'$, we have $r'tr' = t^{-1}$.

As with cyclic groups, we can describe the subgroup lattice of $D_n$. For each divisor $m$ of $n$, we have first of all the unique cyclic subgroup $C_m \leq C_n = \langle t \rangle$, as well as $n/m$ copies of $D_m$ obtained as follows. Index the lines by $\mathbb{Z}/n\mathbb{Z}$, and partition them according to the fibers of the natural map $\pi_m : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/(n/m)\mathbb{Z}$. Let $D_m^{(i)}$ be the subgroup of $D_n$ generated by the reflections about lines in the fiber $\pi_m^{-1}(i)$. Since this fiber has $m$ equiangular lines, we indeed have $D_m^{(i)} \simeq D_m$. As $i$ ranges over $\mathbb{Z}/(n/m)\mathbb{Z}$, we obtain $n/m$ subgroups $D_m^{(i)}$, all containing the same cyclic subgroup $C_m$. In particular, we have $n/1 = n$ subgroups $D_1^{(i)} \simeq D_1$, each generated by the reflections about one of the lines. Finally, if $\ell \mid m \mid n$, we have $D_\ell^{(j)} \leq D_m^{(i)}$ iff $\pi_\ell^{-1}(j) \subseteq \pi_m^{-1}(i)$ iff $j \equiv i \mod \frac{n}{m}$.

The situation for $D_\infty$ is similar but simpler. The element $t = rs$ now has infinite order, hence generates a copy of $\mathbb{Z}$ in $D_\infty$, and for any reflection $r'$ we again have $r'tr' = t^{-1}$. We leave the subgroups of $D_\infty$ to the exercises.

Returning to finite $n$, we can view $D_n$ as a subgroup of $GL_2(\mathbb{R})$. Assume the lines intersect at $(0,0) \in \mathbb{R}^2$ and that the reflecting line $\ell_1$ is the $x$-axis. The reflection $r_1$ has matrix

$$r_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

For $1 \leq k < n$ let $\ell_{k+1}$ be the line rotated from $\ell$ counterclockwise by $k\pi/n$. Then $\ell_2$ is adjacent to $\ell_1$ and the rotation $(r_1 r_2)^k$ has matrix

$$(r_1 r_2)^k = \begin{bmatrix} \cos(2k\pi/n) & -\sin(2k\pi/n) \\ \sin(2k\pi/n) & \cos(2k\pi/n) \end{bmatrix}.$$

## 8.4 The quaternion and generalized quaternion groups $Q_{4n}$

The generalized quaternion groups are best understood as subgroups of the group $\mathrm{SL}_2(\mathbb{C})$ of $2 \times 2$ complex matrices with determinant =1. Let $T$ be the subgroup of diagonal matrices in $\mathrm{SL}_2(\mathbb{C})$. Its

normalizer $N(T)$ in $\mathrm{SL}_2(\mathbb{C})$ consists of two cosets of $T$:

$$N(T) = T \cup wT, \qquad \text{where} \quad w = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

The finite subgroups of $N(T)$ are of two types: Those contained in $T$ are cyclic. The *generalized quaternion groups* are the finite subgroups of $N(T)$ which are *not* contained in $T$. Let $Q < N(T)$ be such a subgroup. Since $Q \not< T$, it contains an element of the form $wt$ for some $t \in T$. Replacing $Q$ by $s^{-1}Qs$, where $s^2 = t$, we may and shall assume that $t = 1$, so that $w \in Q$. Since $w$ has order four, the order of $Q$ is divisible by four.

The generalized quaternion group $Q_{4n}$ is the unique subgroup of $N(T)$ containing $w$ and having order $4n$.

To see $Q_{4n}$ explicitly, let $\zeta_n = e^{\pi i/n}$, which has order $2n$ as an element of $\mathbb{C}^\times$. Then $Q_{4n}$ is generated by the two matrices

$$t_n = \begin{bmatrix} \zeta_n & 0 \\ 0 & \zeta_n^{-1} \end{bmatrix}, \qquad \text{and} \qquad w = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Note that $t_n$ has order $2n$, that $w$ has order four, and we have

$$wt_nw^{-1} = t^{-1}, \qquad w^2 = t^n = -I.$$

Thus, we have

$$Q_{4n} = \{t_n^i w^j : \ 0 \le i \le 2n-1, \quad j = 0 \text{ or } 1\},$$

so that $|Q_{4n}| = 4n$, as claimed. Note that

$$\langle t_n \rangle \cap \langle w \rangle = \langle t_n^n \rangle = \langle -I \rangle,$$

where $-I = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$. This is the unique element of order two in $Q_{4n}$, and the subgroup $\langle -I \rangle$ is normal in $Q_{4n}$, with quotient

$$Q_{4n}/\langle -I \rangle \simeq D_n.$$

Hence the subgroups of $Q_{4n}$ containing $\langle -I \rangle$ are in bijection with the subgroups of $D_n$. Recall the subgroups of $D_n$ are cyclic rotations or dihedral. The subgroups of $Q_{4n}$ corresponding to cyclic rotations are cyclic. These are precisely the subgroups of even order in $Q_{4n}$. The odd-order subgroups are cyclic and contained in $\langle t_n \rangle$.

For $k = 1$ we have $Q_4 = \langle w \rangle \simeq C_4$. This is the only generalized quaternion group which is abelian. Indeed, we have $Z(Q_{4n}) = \langle -I \rangle$ when $n \ge 2$.

For $k = 2$ the group $Q_8$ is commonly known as the *quaternion group* (of order eight), and has different notation. It is common to write

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\},$$

where

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad i = \begin{bmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{bmatrix}, \qquad j = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \qquad k = \begin{bmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{bmatrix},$$

which have relations $i^2 = j^2 = k^2 = -1$ and

$$ij = k, \quad jk = i, \quad ki = j, \quad ji = -k, \quad kj = -i, \quad ik = -j.$$

The proper subgroups of $Q_8$ are $\langle i\rangle, \langle j\rangle, \langle k\rangle, \langle -1\rangle$. We have

$$\langle -1\rangle = \langle i\rangle \cap \langle j\rangle \cap \langle k\rangle$$

and this subgroup is both the center $Z(Q_8)$ and the commutator subgroup $[Q_8, Q_8]$. The group $Q_8$ is the simplest non-abelian group in which every subgroup is normal. It can be shown that any finite non-abelian group with all subgroups normal is isomorphic to $Q_8 \times A$, where $A$ is abelian.

## 8.5 $p$-groups, a first look

A finite group $G$ is a $p$-**group** if the order of $G$ a power of a prime $p$.

Each abelian $p$-group is a direct product $G = C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_k}}$ of cyclic $p$-groups, there being one isomorphism class of such groups for every set of positive integers $\{n_1, \ldots, n_k\}$. When all $n_i = 1$, the group $C_p^k = C_p \times C_p \times \cdots \times C_p$ is called **elementary abelian of rank** $k$. The dihedral groups $D_{2^n}$ and generalized quaternion groups $Q_{2^n}$ are examples of nonabelian 2-groups.

One cannot hope to classify all $p$-groups, except those whose orders are small powers of $p$.

**Proposition 8.6** *Let $p$ be a prime and let $G$ be a $p$-group.*

1. *If $|G| = p$ then $G \simeq C_p$.*
2. *If $|G| = p^2$ then $G$ is abelian. We have $G \simeq C_{p^2}$ if $G$ is cyclic and $G \simeq C_p \times C_p$ if $G$ is not cyclic.*
3. *If $|G| = p^3$ then either $G$ is one of two nonabelian groups or $G$ is one of $C_{p^3}$, $C_p \times C_{p^2}$ or $C_p \times C_p \times C_p$.*

**Proof:** We already noted that part 1 is a consequence of Lagrange's theorem. We will prove part 2 here, and postpone the proof and a more detailed statement of part 3.

Assume $|G| = p^2$. We have seen in Cof. 2.15 that every $p$-group has a nontrivial center $Z(G)$. By Lagrange's theorem, we have $|Z(G)| = p$ or $p^2$. If $|Z(G)| = p$ then $G/Z(G)$ has order $p$, hence is cyclic, so $G$ is abelian, contradicting $Z(G) \neq G$. Hence $G$ is abelian.

The order of every element of $G$ also divides $p^2$. If $G$ has an element of order $p^2$ then $G \simeq C_{p^2}$. Assume $G$ has no element of order $p^2$. Then every nonidentity element of $G$ has order $p$. Choose $h, k \in G$ with $h \neq 1$ and $k \notin \langle h\rangle$. The subgroups $H = \langle h\rangle$ and $K = \langle k\rangle$ haver order $p$ and are both normal in the abelian group $G$. Now $HK$ is a subgroup of $G$ properly containing $H$. Since $[G : H] = p$, it follows that $HK = G$. Likewise, $H \cap K$ is a proper subgroup of $K$, which has order $p$, so $H \cap K = \{1\}$. Now by Prop. 2.10 we have $G \simeq H \times K \simeq C_p \times C_p$. ■

Prop. 2.15 can be extended to prove the converse of Lagrange's theorem for $p$-groups. First we need a lemma.

**Lemma 8.7** *If $A$ is a finite abelian group whose order is divisible by a prime $p$ then $A$ contains an element of order $p$.*

**Proof:** By induction, we may assume the result is true for groups of smaller order. Let $b \in A$ have order $m > 1$, and let $B = \langle b \rangle$. If $p \mid m$ then $b^{m/p}$ has order $p$. Assume $p \nmid m$. Then $p$ divides $|A/B|$ and $|A/B| < |A|$, so $A/B$ has an element of order $p$, by the induction hypothesis. This element is $aB$ for some $a \in A$ such that $a \notin B$, but $a^p \in B$. Therefore $a^p = b^r$ for some integer $r$. Since $\gcd(p, m) = 1$, we can write $r = kp + \ell m$ for integers $r, \ell$. The element $c = ab^{-k}$ does not belong to $B$ since $a \notin B$, but since $A$ is abelian we have

$$c^p = a^p b^{-kp} = b^{r-kp} = b^{\ell m} = 1.$$

Hence $c \in A$ has order $p$. ■

As we will see in the next result, the lemma is true without the assumption that $A$ is abelian, but the proof is not as constructive.

**Proposition 8.8** *Let $G$ be a finite group of order $p^r$, where $p$ is a prime. Then $G$ has a chain of subgroups*

$$1 = G_0 < G_1 < G_2 < \cdots < G_{r-1} < G_r = G$$

*such that for all $0 \leq i < r$ we have*

1. *$|G_i| = p^i$;*
2. *$G_i$ is a normal subgroup of $G$ and $G_{i+1}/G_i \simeq C_p$;*
3. *$G_{i+1}/G_i$ is contained in the center of $G/G_i$.*

**Proof:** We argue by induction on $r$. By Cor. 2.15, the center $Z(G)$ is a nontrivial abelian $p$-group. By Lemma 8.7, there exists a subgroup $G_1 \leq Z(G)$ of order $p$. Since $G_1$ is central in $G$ we have $G_1 \triangleleft G$. The group $\overline{G} = G/G_1$ has order $p^{r-1}$. Applying the induction hypothesis to $\overline{G}$, there is a chain of subgroups

$$1 = \overline{G}_0 < \overline{G}_1 < \overline{G}_2 < \cdots < \overline{G}_{r-2} < \overline{G}_{r-1} = \overline{G}$$

such that for all $0 \leq i < r-1$ we have $|\overline{G}_i| = p^i$ and $\overline{G}_i \triangleleft \overline{G}$ and $\overline{G}_{i+1}/\overline{G}_i$ is contained in the center of $\overline{G}/\overline{G}_i$.

By the Correspondence Theorem applied to $G/G_1$ there are normal subgroups $G_i \trianglelefteq G$ such that

$$\overline{G}_i = G_i/G_1.$$

Moreover, the canonical projection $G \to \overline{G}$ induces isomorphisms

$$G/G_i \xrightarrow{\sim} \overline{G}/\overline{G}_i$$

which restrict to isomorphisms

$$G_{i+1}/G_i \xrightarrow{\sim} \overline{G}_{i+1}/\overline{G}_i$$

for each $0 \leq i < r$. It follows that $G_{i+1}/G_i$ is contained in the center of $G/G_i$, as claimed. ■

Thus, every $p$-group has a tower of normal subgroups whose quotients are cyclic of order $p$. Despite this apparent simplicity, the number of isomorphism classes of groups of order $p^r$ grows rapidly with $r$, especially for the prime $p = 2$. Below is a table of the number of 2-groups for exponent $r \leq 10$.

| $\lvert G\rvert$ | number of groups |
|---|---|
| $2$ | $1$ |
| $2^2$ | $2$ |
| $2^3$ | $5$ |
| $2^4$ | $15$ |
| $2^5$ | $51$ |
| $2^6$ | $267$ |
| $2^7$ | $2\,328$ |
| $2^8$ | $56\,092$ |
| $2^9$ | $10\,494\,213$ |
| $2^{10}$ | $49\,487\,365\,422$ |

It has been determined [1] that the total number of all groups of order $\leq 2000$ is $49\,910\,529\,484$, so over $99\%$ of these groups have order $2^{10}$.

## 8.6 Simple groups

A group $G$ is **simple** if $G$ has no normal subgroups other than $\{1\}$ and $G$ itself. Such groups have remarkable properties. For example,

*Every homomorphism from a simple group to another group is either injective or trivial.*

For if $f : G \to G'$ is a nontrivial homomorphism from a simple group $G$ into some other group $G'$ then $f$ is automatically injective, since $\ker f$ is a normal subgroup of $G$.

Likewise,

*If $G$ is nonabelian simple, then the center $Z(G) = \{1\}$ and the commutator $[G, G] = G$.*

For both $Z(G)$ and $[G, G]$ are normal subgroups of $G$. As $G$ is nonabelian, we have $Z(G) \neq G$ and $[G, G] \neq \{1\}$, so we must have $Z(G) = \{1\}$ and $[G, G] = G$.

By Lagrange's Theorem, any group of prime order is simple. All other simple groups are nonabelian; they are extremely rare and interesting. Of the $49\,910\,529\,484$ groups of order at most $2000$, exactly

[1] *The groups of order at most* 2000, Besche et al., AMS Elec.Res.Ann. 2001.

six are nonabelian simple groups, namely

| simple group $G$ | $\lvert G\rvert$ |
|---|---|
| $A_5 \simeq PSL_2(5)$ | 60 |
| $\mathrm{PSL}_2(7) \simeq \mathrm{GL}_3(2)$ | 168 |
| $A_6 \simeq \mathrm{PSL}_2(9)$ | 360 |
| $\mathrm{PSL}_2(8)$ | 504 |
| $\mathrm{PSL}_2(11)$ | 660 |
| $\mathrm{PSL}_2(13)$ | 1092 |

These small simple groups belong to two families $A_n$ and $PSL_2(q)$ for $n \geq 5$ and $q \geq 5$ a prime power. We prove that the groups in these families are simple.

### 8.6.1 Simplicity of alternating groups

**Theorem 8.9** *For $n \geq 5$ the alternating group $A_n$ is simple.*

**Proof:** Every element of $A_n$ is a product of an even number of transpositions. Hence $A_n$ is generated by elements of the form $(a\ b)(c\ d)$ and $(a\ b)(b\ c)$. Now

$$(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d), \qquad \text{and} \qquad (a\ b)(b\ c) = (a\ b\ c),$$

so $A_n$ is also generated by 3-cycles.

Since $n \geq 5$, the centralizer of a 3-cycle in $S_n$ contains a transposition, so this centralizer is not contained in $A_n$. It follows that the 3-cycles form a single conjugacy class in $A_n$.

Let $N \trianglelefteq A_n$ be a nontrivial normal subgroup of $A_n$. We must show that $N = A_n$. For all $\sigma \in N$ and $\alpha \in A_n$ the commutator $\sigma^{-1}\alpha\sigma\alpha^{-1}$ belongs to $N$, since $N \trianglelefteq A_n$. We use this procedure to show that $N$ contains a 3-cycle or a 22-cycle. Since $N$ is a union of conjugacy classes of $A_n$, it will follow that $N$ contains all 3-cycles or 22-cycles and therefore $N = A_n$ by our previous remarks.

We write elements of $N$ as products of disjoint cycles.

Case 1: Suppose $N$ contains a disjoint product of the form

$$\sigma = \tau \cdot (a_1\ a_2\ \ldots\ a_r), \qquad r \geq 4.$$

Let $\alpha = (a_1\ a_2\ a_3)$. Then we compute

$$\sigma^{-1}\alpha\sigma\alpha^{-1} = (a_1\ a_3\ a_r) \in N,$$

so that $N$ contains a 3-cycle in this case.

Case 2: Suppose $N$ contains a disjoint product of the form

$$\sigma = \tau \cdot (a\ b\ c)(d\ e\ f).$$

Let $\alpha = (a\ b\ d)$. Then we compute

$$\sigma^{-1}\alpha\sigma\alpha^{-1} = (a\ d\ b\ f\ c) \in N.$$

Then case 1 applies, and shows that $N$ contains a 3-cycle.

Case 3: Suppose $N$ contains a disjoint product of the form

$$\sigma = \tau \cdot (a\ b\ c)$$

where $\tau$ is a product of transpositions. Then $\sigma^2 = (c\ b\ a)$ so $N$ contains a 3-cycle.

Case 4: Suppose $N$ contains a disjoint product of the form

$$\sigma = \tau \cdot (a\ b)(c\ d),$$

where $\tau$ is a product of transpositions. Since $C_{S_n}(\sigma)$ contains the transposition $(c\ d)$, it follows that $N$ also contains

$$\sigma' = \tau \cdot (a\ c)(b\ d),$$

which has the same cycle type as $\sigma$. Hence $N$ contains

$$\sigma\sigma' = (a\ b)(c\ d)(a\ c)(b\ d) = (a\ d)(c\ b)$$

Hence $N$ contains all elements of the class $[2, 2]$.

Every nonidentity element of $A_n$ can be written in one of these four forms. Hence $N$ must contain a 3-cycle or a 22-cycle. ■

### 8.6.2 Simplicity of $\mathrm{PSL}_2(F)$

We next prove that the group $\mathrm{PSL}_2(F)$ is simple for any field with at least four elements. The proof depends on a series of lemmas, each interesting in its own right. We work in the group $G = \mathrm{SL}_2(F)$, with the following subgroups and element:

$$B = \left\{ \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix} :\ a \in F^\times,\ b \in F \right\}, \quad U = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} :\ b \in F \right\}, \quad \overline{U} = \left\{ \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} :\ c \in F \right\},$$

$$T = \left\{ \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} :\ a \in F^\times \right\}, \quad Z = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\} = Z(G), \quad w = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

**Lemma 8.10 (Bruhat Decomposition)** *We have $G = B \cup BwB$, a disjoint union.*

**Proof:** A matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$ lies outside of $B$ exactly if $c \neq 0$. In this case,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c^{-1} & a \\ 0 & c \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & dc^{-1} \\ 0 & 1 \end{bmatrix} \in BwB.$$

■

**Lemma 8.11** *The subgroup $B$ is a maximal proper subgroup of $G$.*

**Proof:** Suppose $H$ is a subgroup of $G$ properly containing $B$. Then there exists $h \in H$ with $h \notin B$. By Lemma 8.10, we can write $h = b_1 w b_2$, with $b_i \in B$. It follows that $w \in H$, hence $BwB \subset H$, so $H = G$. ■

**Lemma 8.12** *The group $G$ is generated by $U$ and $\overline{U}$.*

**Proof:** Let $H$ be the subgroup of $G$ generated by $U$ and $\overline{U}$. If $a \in F^\times$, we have

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ a-1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -a^{-1} \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ a-a^2 & 1 \end{bmatrix}.$$

Since $B = TU$, we have $B \leq H$. And

$$w = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix},$$

so $w \in H$. From Lemma 8.10, it follows that $H = G$. ■

**Lemma 8.13** *If $|F| \geq 4$ then $SL_2(F)$ is its own commutator subgroup.*

**Proof:** By Lemma 8.12 it suffices to show that the elements of $U$ and $\bar{U}$ are commutators. This depends on the fact that $T$ normalizes $U$ and $\overline{U}$. Indeed, we have

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}^{-1} = \begin{bmatrix} 1 & ba^2 \\ 0 & 1 \end{bmatrix}, \quad \text{and} \quad \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 \\ ca^{-2} & 1 \end{bmatrix}.$$

We get the following commutators

$$\left[ \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}, \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \right] = \begin{bmatrix} 1 & b(a^2-1) \\ 0 & 1 \end{bmatrix}, \quad \text{and} \quad \left[ \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} \right] = \begin{bmatrix} 1 & 0 \\ c(a^{-2}-1) & 1 \end{bmatrix}.$$

Now if $F$ has at least four elements, we can find $a \in F$ such that $a \notin \{0, +1, -1\}$. For any $x \in F$ we take $b = x/(a^2-1)$ and $c = x/(a^{-2}-1)$, and find that

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix}$$

are commutators, as claimed. ■

**Lemma 8.14** *The intersection $\bigcap_{g \in G} {}^gB = Z$.*

**Proof:** Since $Z < B$, and $Z$ is central, it is clear that $Z < {}^gB$ for all $g \in G$. Conversely, we have $B \cap {}^wB = T$. Letting $v = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in \overline{U}$, one checks that $T \cap {}^vB = Z$. Hence $\bigcap_{g \in G} {}^gB \leq Z$, proving equality. ■

**Lemma 8.15** *Assume that $|F| \geq 4$. Let $H$ be a normal subgroup of $G = \mathrm{SL}_2(F)$. Then either $H \leq Z$ or $H = G$.*

**Proof:** Since $H \trianglelefteq G$, the product $HB$ is a subgroup of $G$ containing $B$. By Lemma 8.11 we have either $HB = B$ or $HB = G$. If $HB = B$ then $H \leq B$. But since $H \trianglelefteq G$, we have $H \subset \bigcap_{g \in G} {}^gB = Z$.

Suppose $HB = G$. Then we can write $w = hb$ for some $h \in H$, and $b \in B$. One checks that $B$ normalizes $U$ and ${}^wU = \overline{U}$. It follows that $\overline{U} = {}^wU = {}^{hb}U = {}^{hU}$. As $U$ and $\overline{U}$ generate $G$, we have then $G = HU$. By the second isomorphism theorem, we have

$$G/H = HU/H \simeq U/U \cap H.$$

The latter group is abelian since $U$ is abelian. Hence $H \geq [G, G]$. But $[G, G] = G$, as we proved in Lemma 12.1. Hence $H = G$, as claimed. ■

Now we can prove our result.

**Theorem 8.16** *If $F$ is a field with at least four elements then the group $\mathrm{PSL}_2(F)$ is simple.*

**Proof:** By the Correspondence Theorem, the normal subgroups of $\mathrm{PSL}_2(F)$ are the projections of the normal subgroups of $\mathrm{SL}_2(F)$ which contain $Z$. From Lemma 8.15 it follows that every normal subgroup of $\mathrm{PSL}_2(F)$ is either trivial or all of $\mathrm{PSL}_2(F)$. Hence $\mathrm{PSL}_2(F)$ is simple. ■

**Remark:** If $|F| \leq 3$ then $\mathrm{PSL}_2(F)$ is not simple. Indeed, we have

$$PSL_2(2) \simeq S_3, \qquad PSL_2(3) \simeq A_4.$$

These are the first two of the "exceptional isomorphisms" discussed in the next section. For $n \geq 3$, the group $\mathrm{PSL}_n(F)$ is simple for every field $F$ (see [Lang, XIII.9]).

## 8.7 Exceptional isomorphisms

The previous two sections exhibit two families of finite simple groups, namely the alternating groups $A_n$ for $n \geq 5$ and the groups $\mathrm{PSL}_2(q) = \mathrm{PSL}_2(F)$ where $F$ is a finite field with $|F| = q \geq 4$. A small number of groups are common to both families via isomorphisms whose subtlety ranges from the non-obvious to the miraculous. We list these exceptional isomorphisms, and a few others.

$$\begin{aligned} S_3 &\simeq \mathrm{GL}_2(2) = \mathrm{PSL}_2(2) \\ A_4 &\simeq \mathrm{PSL}_2(3) \\ A_5 &\simeq \mathrm{PSL}_2(4) \simeq \mathrm{PSL}_2(5) \\ \mathrm{PSL}_2(7) &\simeq \mathrm{GL}_3(2) = \mathrm{PSL}_3(2) \\ A_6 &\simeq \mathrm{PSL}_2(9) \\ A_8 &\simeq \mathrm{PSL}_4(2). \end{aligned} \tag{25}$$

The first two, as well as the isomorphism $A_5 \simeq \mathrm{PSL}_2(4)$, arise easily from the theory of group actions in the next section. For the remaining exceptional isomorphisms, see sections 10.4.1, 10.4.2, 13.5.2 and **??**.

### 8.7.1 Applications to simple groups

**Proposition 8.17** *Let $G$ be a simple group of order $|G| > 2$ and let $H$ be a subgroup of $G$ of index $m$. Then $G$ is isomorphic to a subgroup of the alternating group $A_m$. In particular, the order of $G$ divides $\frac{1}{2}m!$.*

**Proof:** The action of $G$ on $G/H$ gives a homomorphism $\sigma_H : G \to S_m$ which is automatically injective so $G$ is isomorphic to the image $G' = \sigma_H(G)$. The composition

$$G \xrightarrow{\sigma_H} S_m \xrightarrow{\text{sgn}} \{\pm 1\}$$

cannot be injective since $|G| > 2$, so it must be trivial. This means that $G' \leq A_m$. ■

**Corollary 8.18** *Let $G$ be a nonabelian simple group and let $H$ be a proper subgroup of $G$. Then $[G : H] \geq 5$.*

**Proof:** We know that $[G : H] \neq 2$. If $[G : H] = 3$ then $|G|$ divides 3, so $G$ is abelian, a contradiction. If $[G : H] = 4$ then $G$ is a subgroup of $A_4$. The subgroup $K < A_4$ generated by the 22-cycles is abelian and normal in $A_4$, so $G \cap K$ is normal in $G$. If $G \cap K = G$ then $G < K$ so $G$ is abelian, which it is not. So $G \cap K = 1$. Then the composition $G \hookrightarrow A_4 \to A_4/K$ is injective. As $|A_4/K| = 3$, we get same contradiction as before. Thus, we cannot have $[G : H] = 4$ either. ■

The inequality in Cor. 8.18 is sharp. For we have seen in Thm. 8.9 that the alternating group $A_5$ is simple. And $A_5$ contains $A_4$ with index $[A_5 : A_4] = 5$.

# 9 Finite linear groups

Let $F$ be a finite field, say $|F| = q$. Then $GL_n(F) = GL_n(q)$ is a finite group. We can use the Counting Formula to re-compute $|GL_n(F)|$ and $|X_k|$ (cf. (22)). First, for $n = 1$ we have $GL_1(F) = F^\times$, so

$$|GL_1(F)| = |F^\times| = q - 1.$$

For $n > 1$ the group $GL_n(F)$ acts transitively on the set $Y_n$ of nonzero vectors in $F^n$. The stabilizer of the vector $e_1$ is the subgroup

$$H_n = \left\{ \begin{bmatrix} 1 & C \\ 0 & B \end{bmatrix} : \ B \in GL_{n-1}(F), \ C \text{ an arbitrary } 1 \times (n-1) \text{ matrix over } F \right\}.$$

Counting the possible choices for $B$ and $C$ and observing that $|F^n| = q^n$, we find that

$$|Y_n| = q^n - 1, \qquad |H_n| = |GL_{n-1}(F)| \cdot q^{n-1}.$$

The Counting Formula says that

$$q^n - 1 = |Y_n| = \frac{|GL_n(F)|}{|H_n|} = \frac{|GL_n(F)|}{|GL_{n-1}(F)| \cdot q^{n-1}}.$$

This gives the recursive formula

$$|GL_n(F)| = q^{n-1}(q^n - 1) \cdot |GL_{n-1}(F)|.$$

and by induction we recover the formula from (22):

$$|GL_n(F)| = q^{n(n-1)/2}(q^n - 1)(q^{n-1} - 1) \cdots (q^2 - 1)(q - 1). \tag{26}$$

To simplify this formula, we define the $q$-factorial

$$[n!]_q = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^2 - 1)(q - 1)}{(q - 1)^n}.$$

If we pretend that $q$ is a variable, we have $(n!)_q \to n!$, the usual factorial, as $q \to 1$. With this notation, we have

$$|GL_n(F)| = q^{n(n-1)/2} \cdot (q - 1)^n \cdot [n!]_q.$$

Now to find $|X_k|$ we need only divide by $|H_k|$. Considering the possible choices for $A, B, C$ in the element $\begin{bmatrix} A & C \\ 0 & B \end{bmatrix} \in H_k$, we find

$$\begin{aligned} |P_k| &= |GL_k(F)| \cdot |GL_{n-k}(F)| \cdot q^{k(n-k)} \\ &= q^{k(k-1)/2} \cdot (q - 1)^k \cdot [k!]_q \cdot q^{(n-k)(n-k-1)/2} \cdot (q - 1)^{n-k} \cdot [(n - k)!]_q \cdot q^{k(n-k)} \\ &= q^{n(n-1)/2}(q - 1)^n \cdot [k!]_q \cdot [(n - k)!]_q. \end{aligned}$$

It follows that the number of $k$-dimensional subspaces of $F^n$ is given by

$$|X_k| = \frac{[n!]_q}{[k!]_q \cdot [(n - k)!]_q},$$

the **$q$-binomial coefficient**. If we pretend that $q$ is a variable, this reduces to the ordinary binomial coeffiecient $\binom{n}{k}$ as $q \to 1$. In this vague sense, $k$-element subsets of $\{1, 2, \ldots, n\}$ are like $k$-dimensional subspaces of $F^n$ over the (nonexistent) "field of one element", and $S_n$ is like $GL_n(F)$ over this "field".

All of these formulas came from the Counting Formula. Later we will see other relations between $S_n$ and $GL_n(F)$, where the field $F$ is arbitrary.

# 10 Sylow Theorems and Applications

We have seen that the converse of Lagrange's Theorem is false, in general: If $G$ is a group and $d$ is a divisor of $|G|$ then $G$ need not have a subgroup of order $d$. The simplest example is $G = A_4$ with $|G| = 12$, which has no subgroup of order $d = 6$. Note that $6$ is a product of the two smallest distinct primes. On the other hand, $A_4$ does have proper subgroups of orders $2, 3, 4$, which are the other proper divisors of $12$.

## 10.1 Sylow $p$-subgroups

A **$p$-subgroup** of a finite group $G$ is a subgroup of $G$ whose order is a power of a prime $p$. By Lagrange's theorem, $G$ can have nontrivial $p$-subgroups only if $p$ divides the order of $G$. Write the order as $|G| = m \cdot p^r$, where $p \nmid m$. A **Sylow $p$-subgroup** of $G$ is a $p$-subgroup $P \leq G$ having the maximal order $|P| = p^r$ allowed by Lagrange's theorem. Equivalently, a $p$-subgroup $P \leq G$ is a Sylow $p$-subgroup exactly when $p$ does not divide the index $[G : P]$.

**Example:** Let $F$ be a field with $|F| = q$, a power of a prime $p$. We have seen that the group $\mathrm{GL}_n(F) = \mathrm{GL}_n(q)$ has order

$$|\,\mathrm{GL}_n(q)| = q^{n(n-1)/2}(q-1)(q^2-1)\cdots(q^n-1).$$

Let $U_n(q) \leq \mathrm{GL}_n(q)$ be the subgroup of upper triangular matrices with $1$'s on the diagonal. Thus $U_n(q)$ consists of all matrices of the form

$$\begin{bmatrix} 1 & * & * & \dots & * \\ 0 & 1 & * & \dots & * \\ 0 & 0 & 1 & \ddots & * \\ \vdots & \vdots & \vdots & \ddots & * \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix},$$

where the entries "$*$" above the diagonal of a matrix in $U_n(q)$ can be arbitrary elements of $F$, so we have

$$|U_n(q)| = q^{0+1+2+\cdots+(n-1)} = q^{n(n-1)/2},$$

which is a power of $p$. Since $p$ does not divide $(q-1)(q^2-1)\cdots(q^n-1)$, it follows that $U_n(q)$ is a Sylow $p$-subgroup of $\mathrm{GL}_n(q)$.

For general groups it is not obvious that Sylow $p$-subgroups exist.

**Lemma 10.1** *Let $G$ be a finite group and let $H$ be a subgroup of $G$. Assume that $G$ has a Sylow $p$-subgroup. Then $H$ has a Sylow $p$-subgroup.*

**Proof:** Let $P$ be a Sylow $p$-subgroup of $G$ and consider the $H$-orbits on $G/P$ under the action $h \cdot gP = hgP$. Since $p$ does not divide the index $[G : P]$, there exists an $H$-orbit $\mathcal{O} \subset G/P$ such that $p$ does not divide $|\mathcal{O}|$. Let $gP \in \mathcal{O}$ and let $Q$ be the stabilizer in $H$ of $gP$.

For all $q \in Q$ we have $qgP = gP$, which implies that $q \in gPg^{-1}$. Hence $Q$ is contained in the Sylow $p$-subgroup $gPg^{-1}$. By Lagrange's theorem, $Q$ is a $p$-group. We chose $\mathcal{O}$ so that $p$ does not divide $|\mathcal{O}| = [H : Q]$. It follows that $Q$ is a Sylow $p$-subgroup of $H$. ■

**Remark:** The proof actually shows that if $G$ has Sylow $p$-subgroups, then one of them meets $H$ in a Sylow $p$-subgroup of $H$.

**Theorem 10.2 (Sylow I)** *Let $G$ be a finite group whose order is divisible by a power $p^i$ of a prime $p$. Then $G$ has a subgroup of order $p^i$.*

**Proof:** By Prop. 8.8 it suffices to prove that $G$ has a Sylow $p$-subgroup. Let $n = |G|$. Then $G$ is isomorphic to a subgroup of $S_n$ by Cayley's theorem. And $S_n$ is isomorphic to a subgroup of $\mathrm{GL}_n(p)$. Hence $G$ is isomorphic to a subgroup of $\mathrm{GL}_n(p)$. We have seen in the example above that $\mathrm{GL}_n(p)$ has a Sylow $p$- subgroup. By Lemma 10.1, the group $G$ has a Sylow $p$-subgroup $P$. ■

**Alternate proof:** The proof just given is very simple, and is my favorite, but one can object that such a fundamental fact as Thm. 10.2 should not depend on auxiliary groups like $S_n$ and $\mathrm{GL}_n(p)$. Here is another, more intrinsic proof that produces $p$-subgroups for all $0 \le i \le r$ at once. We first need a lemma about finite sets. For any nonzero integer $n$, let $\mathsf{v}_p(n)$ be the highest power of $p$ dividing $n$.

**Lemma 10.3** *Let $S$ be a finite set of cardinality $mp^r$, where $p$ is a prime. Let $X$ be the set of subsets of $S$ of cardinality $p^r$: $X = \{A \subset S : \ |A| = p^r\}$. Then $\mathsf{v}_p(|X|) = \mathsf{v}_p(m)$.*

**Proof of the lemma:** We have

$$|X| = \binom{mp^r}{p^r} = m \cdot \prod_{k=1}^{p^r-1} \left[\frac{mp^r - k}{p^r - k}\right].$$

Let $1 \le k \le p^r - 1$ and write $k = np^s$ for some integer $n$ not divisible by $p$, with $s = \mathsf{v}_p(k) < r$. Then

$$mp^r - k = mp^r - np^s = p^s(mp^{r-s} - n),$$

so $\mathsf{v}_p(mp^r - k) = \mathsf{v}_p(k)$ does not depend on $m$. Hence $\mathsf{v}_p(mp^r - k) = \mathsf{v}_p(p^r - k)$ and the lemma is proved.

Now we can prove Thm. 10.2. Let $X$ be the set of subsets of $G$ of cardinality $p^r$ and let $s = \mathsf{v}_p(m)$, so that $\mathsf{v}_p(|G|) = r + s$.

The group $G$ acts on $X$ by left multiplication: $g \cdot A = gA$, for $g \in G$ and $A \in X$. Thus, $X$ is partitioned into $G$-orbits. By the lemma, $\mathsf{v}_p(|X|) = s$. Hence there exists a $G$-orbit $O \subset X$ such that $|O|$ is not divisible by $p^{s+1}$. Choose $A \in O$ and let $G_A$ be the stabilizer of $A$. That is,

$$G_A = \{g \in G : \ gA = A\}.$$

We will prove the theorem by showing that $|G_A| = p^r$.

By the Orbit Counting Theorem, we have

$$|O| = [G : G_A].$$

Since $p^{s+1}$ does not divide $|O|$, it follows that $p^r$ must divide $|G_A|$. On the other hand, choose $a \in A$ and let $f : G_A \to A$ be the function $f(g) = ga$, which makes sense for $g \in G_A$. If $f(g) = f(g')$ for $g, g' \in G_A$ then $ga = g'a$ so $g = g'$. Hence $f$ is injective. Since $|A| = p^r$, this shows that $|G_A| \leq p^r$. It now follows that $|G_A| = p^r$, as claimed. ■

The next Sylow Theorem asserts that Sylow $p$-subgroups are unique up to conjugation. The proof of this also reveals information about the number of Sylow $p$-subgroups, which we put in the statement.

First we need two lemmas.

**Lemma 10.4** *Let $P$ be a Sylow $p$-subgroup of a group $G$. Then every $p$-subgroup of the normalizer $N_G(P)$ is contained in $P$.*

**Proof:** Let $H \leq N_G(P)$ be a $p$-subgroup. Since $H$ normalizes $P$, the product $HP$ is a subgroup of $N_G(P)$ and $P \trianglelefteq HP$. Since

$$HP/P \simeq H/H \cap P$$

is a quotient of the $p$-group $H$, and $P$ is a $p$-group, it follows that $HP$ is a $p$-group. And $P \leq HP$. But $P$ is a maximal $p$-subgroup of $G$, by the definition of Sylow $p$-subgroup. Hence $HP = P$, meaning that $H \leq P$. ■

**Lemma 10.5** *Let $H$ be a $p$-group acting on a finite set $X$, and let $X^H = \{x \in X : \ h \cdot x = x\}$ be the fixed-point set of $H$ in $X$. Then*

$$|X^H| \equiv |X| \mod p.$$

**Proof:** The size $|X|$ of $X$ is the sum of the sizes of the orbits of $H$ in $X$. If $\mathcal{O}$ is an $H$-orbit in $X$ and $|\mathcal{O}| \geq 1$ then $|\mathcal{O}|$ is a power of $p$, since $H$ is a $p$-group. In this case $|\mathcal{O}| \equiv 0 \mod p$. Hence $|X|$ is congruent modulo $p$ to the number of orbits consisting of one element only. That is, $|X| \equiv |X^H| \mod p$. ■.

Now we can state and prove the second Sylow theorem.

**Theorem 10.6 (Sylow II)** *Let $G$ be a finite group of order $mp^r$, where $p$ is a prime not dividing $m$. Then the following hold.*

1. *Any two Sylow $p$-subgroups of $G$ are conjugate. That is, if $P$ and $Q$ are two subgroups of $G$ of order $p^r$ then there exists $g \in G$ such that $gPg^{-1} = Q$.*
2. *The number $n_p$ of $p$-Sylow subgroups of $G$ divides $m$ and is of the form $1 + kp$ where $k$ is an integer.*
3. *Every $p$-subgroup of $G$ is contained in a Sylow $p$-subgroup of $G$.*

**Proof:** Let $X = \{P \leq G : \ |P| = p^r\}$ be the set of Sylow $p$-subgroups of $G$. Then $G$ acts on $X$ by conjugation. For this action we have $g \cdot P = gPg^{-1}$ for $g \in G$ and $P \in X$, and the stabilizer of $P$ is the normalizer $N_G(P)$.

Consider the fixed points of a Sylow $p$-subgroup $P$ acting on $X$ by conjugation. I claim that

$$X^P = \{P\}. \tag{27}$$

That is, I claim that $P$ normalizes no other Sylow $p$-subgroup but itself. For suppose $Q \in X^P$ is any fixed point of $P$ in $X$. This means $P \leq N_G(Q)$, so that $P$ is $p$-subgroup of the normalizer of the Sylow $p$-subgroup $Q$. By Lemma 10.4, we have $P \leq Q$, hence $P = Q$ since both $P$ and $Q$ have order $p^r$. This proves (27).

Now let $P \in X$ and let $\mathcal{O} = \{gPg^{-1} : \ g \in G\}$ be the $G$-orbit of $P$ in $X$. By (27), we have $\mathcal{O}^P = \{P\}$. From Lemma 10.5 we have $|\mathcal{O}| \equiv |\mathcal{O}^P| \mod p$. Since $|\mathcal{O}^P| = 1$, this means that

$$|\mathcal{O}| \equiv 1 \mod p. \tag{28}$$

I claim that that $X = \mathcal{O}$. Suppose not. Then there exists $Q \in X$ with $Q \notin \mathcal{O}$. Applying (27) to the Sylow $p$-subgroup $Q$, we have $X^Q = \{Q\}$. Since $Q \notin \mathcal{O}$, it follows that $\mathcal{O}^Q$ is empty. Applying Lemma 10.5 to the action of the $p$-group $Q$ on the set $\mathcal{O}$, we have

$$|\mathcal{O}| \equiv |\mathcal{O}^Q| = 0 \mod p. \tag{29}$$

This contradicts equation (28). Hence $Q$ cannot exist and we have $X = \mathcal{O}$.

Now equation (28) says that $|X| \equiv 1 \mod p$. And since $X$ is a single orbit, the Orbit Counting Formula says that

$$n_p = |X| = [G : N_G(P)] = [G : P]/[N_G(P) : P] = m/[N_G(P) : P],$$

or

$$m = [N_G(P) : P] \cdot n_p,$$

so $n_p \mid m$. Thus, items 1 and 2 are proved.

For item 3, let $H$ be any $p$-subgroup of $G$. Then $|X^H| \equiv |X| \equiv 1 \mod p$, by Lemma 10.5 again and item 2 which has been proved. It follows that $X^H$ is nonempty. This means $H \leq N_G(P)$ for some $P \in X$. By Lemma 10.4 again, we have $H \leq P$. ■

From item 1 of Thm. 10.6 we get the following condition for a Sylow $p$-subgroup to be normal.

**Corollary 10.7** *A Sylow $p$-subgroup of $G$ is normal in $G$ if and only if it is the unique Sylow $p$-subgroup of $G$.*

It follows from Thm. 10.6 that the order of $G$ may be written as

$$|G| = p^r \cdot \nu \cdot (1 + kp), \tag{30}$$

where

$$p^r = |P|, \qquad \nu = |N_G(P)/P|, \qquad 1 + kp = [G : N_G(P)].$$

Of course $r, \nu, k$ all depend on $p$, and $p \nmid \nu$. Let us call (30) the $p$-**factorization** of $|G|$. Besides giving $|G|$, it displays $|P| = p^r$ and $|N_G(P)| = p^r \cdot \nu$, as well as $n_p = 1 + kp$. We have $k = 0$ if and only if $P \trianglelefteq G$.

### 10.1.1 Small examples.

For $G = A_4, S_4, A_5, S_5, \mathrm{SL}_2(7), \mathrm{PSL}_2(7)$, the $p$-factorizations for each prime $p$ dividing $|G|$ are shown.

$A_4$ :

| $p^r \cdot \nu \cdot (1 + pk)$ | $N_G(P)$ |
|---|---|
| $3 \cdot 1 \cdot (1 + 3)$ | $C_3$ |
| $2^2 \cdot 3 \cdot (1 + 0)$ | $A_4$ |

$S_4$ :

| $\lvert p^r \cdot \nu \cdot (1 + pk)$ | $N_G(P)$ |
|---|---|
| $3 \cdot 2 \cdot (1 + 3)$ | $S_3$ |
| $2^3 \cdot 1 \cdot (1 + 2)$ | $D_4$ |

$A_5$ :

| $p^r \cdot \nu \cdot (1 + pk)$ | $N_G(P)$ |
|---|---|
| $5 \cdot 2 \cdot (1 + 5)$ | $D_5$ |
| $3 \cdot 2 \cdot (1 + 3)$ | $S_3$ |
| $2^2 \cdot 3 \cdot (1 + 2 \cdot 2)$ | $A_4$ |

$S_5$ :

| $p^r \cdot \nu \cdot (1 + pk)$ | $N_G(P)$ |
|---|---|
| $5 \cdot 4 \cdot (1 + 5)$ | $F_{20}$ |
| $3 \cdot 4 \cdot (1 + 3 \cdot 3)$ | $S_3 \times S_2$ |
| $2^3 \cdot 1 \cdot (1 + 2 \cdot 7)$ | $D_4$ |

The normalizer $N_{S_5}(P)$ of the Sylow 5-subgroup $P = \langle (1\,2\,3\,4\,5) \rangle$ in $S_5$ is generated by $P$ and the 4-cycle which squares $(1\,2\,3\,4\,5)$ via conjugation, namely $(2\,3\,5\,4)$. It is called $F_{20}$ in honor of Frobenius, although Galois discussed it at length much earlier. One can think of $F_{20}$ as the $ax + b$-group over the field of five elements, isomorphic to

$$\left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : \ a \in (\mathbb{Z}/5\mathbb{Z})^\times, \ b \in \mathbb{Z}/5\mathbb{Z} \right\},$$

which corresponds to a Borel subgroup of $\mathrm{PGL}_2(5)$ under the isomorphism $S_5 \simeq \mathrm{PGL}_2(5)$.

$\mathrm{SL}_2(7)$ :

| $p^r \cdot \nu \cdot (1 + pk)$ | $N_G(P)$ |
|---|---|
| $7 \cdot 6 \cdot (1 + 7)$ | $G_{21} \times C_2$ |
| $3 \cdot 4 \cdot (1 + 3 \cdot 3)$ | $C_3 \rtimes C_4$ |
| $2^4 \cdot 1 \cdot (1 + 2 \cdot 10)$ | $Q_{16}$ |

$\mathrm{PSL}_2(7)$ :

| $p^r \cdot \nu \cdot (1 + pk)$ | $N_G(P)$ |
|---|---|
| $7 \cdot 3 \cdot (1 + 7)$ | $G_{21}$ |
| $3 \cdot 2 \cdot (1 + 3 \cdot 3)$ | $S_3$ |
| $2^3 \cdot 1 \cdot (1 + 2 \cdot 10)$ | $D_4$ |

Here $G_{21}$ is the unique nonabelian group of order 21 (see Prop. 14.6) realized here as the subgroup of the upper-triangular matrices in $SL_2(7)$ whose diagonal entries have odd order. The group $C_3 \rtimes C_4$ is the nonabelian group of order 12 other than $A_4$ and $Q_{16}$ is the generalized quaternion group of order 16 (see 8.4).

### 10.1.2 Groups of order $pq$

We can use Sylow's theorems to classify groups of order $pq$, where $p$ and $q$ are distinct primes. Assume $p < q$ and let $P, Q$ be Sylow $p$- and $q$- subgroups of $G$, respectively. Consider the $q$-factorization

$qp = q \cdot \nu \cdot (1 + qk)$. Since $p$ is prime and $p < q$ we must have $k = 0$ and $\nu = p$. Hence $Q \trianglelefteq G$ and $QP$ is a subgroup of $G$, with $Q \cap P = \{1\}$ because the orders of $P, Q$ are relatively prime. Since $QP/P \simeq Q/Q \cap P = Q$, it follows that $|QP| = pq$, so $QP = G$. Therefore $G$ is a semidirect product: $G = Q \rtimes P$.

The structure of $G$ is now completely determined by the homomorphism

$$\alpha : P \to (\mathbb{Z}/q\mathbb{Z})^\times \qquad \text{given by} \qquad xyx^{-1} = y^{\alpha(x)},$$

where $x \in P$ and $y \in Q$. For if $y$ generates $Q$ then every element $g \in G$ can be uniquely expressed as $g = y^b \cdot x$, for $b \in \mathbb{Z}/q\mathbb{Z}$ and $x \in P$, and the product of two such elements is

$$(y^b \cdot x)(y^{b'} \cdot x') = y^b \cdot (xy^{b'}x^{-1}) \cdot xx' = y^b \cdot y^{b'\alpha(x)} \cdot xx' = y^{b+b'\alpha(x)} \cdot xx'.$$

If $\alpha$ is trivial then $G$ is abelian and $G = Q \times P \simeq C_{pq}$.

Suppose $\alpha$ is nontrivial. Then $\alpha$ is injective, since $p$ is prime, and we must have $q \equiv 1 \mod p$. The group $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic of order $q - 1$, hence has a unique subgroup $A_p$ of order $p$, and we have $\alpha(P) = A_p$.

Let $G_{pq}$ be the following subgroup of the $ax + b$-group over $\mathbb{Z}/q\mathbb{Z}$:

$$G_{pq} = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : \ a \in A_p, \ b \in \mathbb{Z}/q\mathbb{Z} \right\}.$$

The function $\varphi : G \to G_{pq}$ defined by

$$\varphi(y^b \cdot x) = \begin{bmatrix} \alpha(x) & b \\ 0 & 1 \end{bmatrix}$$

is clearly bijective. In fact it is a group homomorphism, for we have

$$\varphi(y^b x \cdot y^{b'} x') = \varphi(y^{b+b'\alpha(x)} \cdot xx') = \begin{bmatrix} \alpha(xx') & b + b'\alpha(x) \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \alpha(x) & b \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} \alpha(x') & b' \\ 0 & 1 \end{bmatrix} = \varphi(y^b x) \cdot \varphi(y^{b'} x).$$

Hence $\varphi$ is an isomorphism $G \simeq G_{pq}$. To summarize, we have shown the following.

**Proposition 10.8** *Let $G$ be a group of order $pq$ where $p, q$ are primes with $p < q$.*

1. *If $G$ is abelian then $G \simeq C_{pq}$ is cyclic of order $pq$.*
2. *If $G$ is nonabelian then $q \equiv 1 \mod p$ and $G \simeq G_{pq}$.*

For example the two groups of order $2q$, where $q$ is an odd prime, are $C_{2q}$ and the dihedral group $D_q \simeq G_{2q}$.

## 10.2 Sylow subgroups in $\mathrm{GL}_n$ and flag varieties

Let $F$ be a finite field with $|F| = q$, a power of a prime $p$ and let $G = \mathrm{GL}_n(q)$. We have seen that the subgroup

$$U = U_n(q) = \begin{bmatrix} 1 & * & * & \dots & * \\ 0 & 1 & * & \dots & * \\ 0 & 0 & 1 & \ddots & * \\ \vdots & \vdots & \vdots & \ddots & * \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix} \leq G \tag{31}$$

is a Sylow $p$-subgroup of $G$. The normalizer of $U$ is the Borel subgroup $B$ appearing in the Bruhat decomposition:

$$N_G(U) = B = \begin{bmatrix} \times & * & * & \dots & * \\ 0 & \times & * & \dots & * \\ 0 & 0 & \times & \ddots & * \\ \vdots & \vdots & \vdots & \ddots & * \\ 0 & 0 & 0 & \dots & \times \end{bmatrix},$$

where the entries $*$ are arbitrary in $F$ as before, and the diagonal entries $\times$ are nonzero elements of $F$. We have $B = U \rtimes T$, where $T$ is the diagonal subgroup of $G$, and $|B| = q^{n(n-1)/2} \cdot (q-1)^n$. The $p$-factorization of $|G|$ is therefore

$$|G| = q^{n(n-1)/2} \cdot (q-1)^n \cdot \frac{(q^n-1)\cdots(q^2-1)(q-1)}{(q-1)^n}.$$

We observe that

$$\frac{(q^n-1)\cdots(q^2-1)(q-1)}{(q-1)^n} = \prod_{k=1}^{n}(1+q+\cdots+q^{k-1}) \equiv 1 \mod p,$$

as guaranteed by Sylow's theorem. This is the number of Sylow $p$-subgroups of $G$, of which $U$ is only one. Let $X$ be the set of all Sylow $p$-subgroups of $G$. By the Main Theorem of Group Actions, the mapping

$$G/B \longrightarrow X, \qquad \text{sending} \quad gB \mapsto gUg^{-1}$$

is a $G$-equivariant bijection. The set $X$ involves the complete projective geometry of the vector space $V = F^n$, as I will explain.

For $n = 2$, we have seen that $B$ is the stabilizer of the line $\ell_o = Fe_1$ in $V$, so in this case $G/B$ is also identified with the set $\mathbb{P}(V)$ of all lines $\ell \subset V$. Thus we have a $G$-equivariant bijective correspondence

$$\mathbb{P}(V) \ni \ell = g \cdot \ell_o \leftrightarrow gB \leftrightarrow gUg^{-1} = U_\ell \in X$$

between lines in $V$ and Sylow $p$-subgroups of $G = \mathrm{GL}_2(q)$. Given a line $\ell$, the subgroup $U_\ell$ is the set of elements in $G$ which act trivially on both $\ell$ and $V/\ell$. All elements of $U_\ell$ have the form $\begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}$ with respect to any basis $\{v_1, v_2\}$ of $V$ with $v_1 \in \ell$, but not all elements of $U_\ell$ have this form with respect to the original basis $\{e_1, e_2\}$, unless $\ell = \ell_o$.

For $n = 3$ we have both lines and planes in $V = F^3$, and a given plane may or may not contain a given line. A **flag** in $V$ is a pair $(\ell, \pi)$, where $\ell$ is a line contained in a plane $\pi \subset V$. Such configurations comprise the complete projective geometry of $V$. Let $\mathcal{F}(V)$ be the set of all flags in $V$. The group $G = \mathrm{GL}_3(F)$ acts on $\mathcal{F}(V)$ via $g \cdot (\ell, \pi) = (g \cdot \ell, g \cdot \pi)$. This $G$-action is transitive and $B$ is the stabilizer of the flag $(\ell_o, \pi_o)$, where $\ell_o = Fe_1$ and $\pi_o = Fe_1 \oplus Fe_2$. Thus we have a $G$-equivariant bijective correspondence

$$\mathcal{F}(V) \ni (\ell, \pi) = g \cdot (\ell_o, \pi_o) \quad \leftrightarrow \quad gB \quad \leftrightarrow \quad gUg^{-1} = U_{(\ell,\pi)} \in X$$

between flags in $V$ and Sylow $p$-subgroups of $G = \mathrm{GL}_3(q)$. Given a flag $(\ell, \pi)$, the subgroup $U_{(\ell,\pi)}$ is the set of elements in $G$ which preserve $\ell$ and $\pi$ and act trivially on $\ell$, $\pi/\ell$ and $V/\pi$. All elements of $U_{(\ell,\pi)}$ have the form $\begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix}$ with respect to any basis $\{v_1, v_2, v_3\}$ of $V$ for which $v_1 \in \ell$ and $v_1, v_2 \in \pi$, but not all elements of $U_{\ell,\pi}$ will have this form with respect to the original basis $\{e_1, e_2, e_3\}$, unless $\ell = \ell_o$ and $\pi = \pi_o$.

For general $n \geq 2$, a **flag** in $V = F^n$ is a sequence of subspaces

$$f = (V_0, V_1, \ldots, V_{n-1}, V_n), \qquad \text{where} \qquad \{0\} = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_{n-1} \subset V_n = V,$$

and $\dim V_i = i$ for all $0 \leq i \leq n$. The **flag variety** of $G$ is the set $\mathcal{F}(V)$ of all flags $f \in V$. The action of $G = \mathrm{GL}_n(q)$ on $\mathcal{F}(V)$ permutes the flags in $V$. That is, we have

$$g \cdot (V_0, V_1, \ldots, V_n) = (V_0, gV_1, \ldots, gV_{n-1}, V_n).$$

This $G$-action is transitive and $B$ is the stabilizer of the flag

$$f_o = (0, Fe_1, Fe_1 \oplus Fe_2, \cdots, Fe_1 \oplus Fe_2 \oplus \cdots \oplus Fe_{n-1}, V).$$

Thus we have a $G$-equivariant bijective correspondence

$$\mathcal{F}(V) \ni f = g \cdot f_o \quad \leftrightarrow \quad gB \quad \leftrightarrow \quad gUg^{-1} = U_f \in X$$

between flags $f \in V$ and Sylow $p$-subgroups $U_f \leq G = \mathrm{GL}_n(q)$. Given a flag $f = (V_0, V_1, \ldots, V_n)$, the subgroup $U_f$ is given by

$$U_f = \{g \in G : \ gV_i = V_i \quad \text{and } g \text{ acts trivially on} \quad V_i/V_{i-1} \quad \text{for all} \quad \leq i \leq n\}.$$

All elements of $U_f$ have the form (31) with respect to any basis $\{v_1, v_2, \ldots, v_n\}$ of $V$ for which $V_i = Fv_1 \oplus \cdots \oplus Fv_i$, but not all elements of $U_f$ have this form for the original basis $\{e_1, \ldots, e_n\}$ unless $f = f_o$.

The total number of flags in $V$ is

$$|\mathcal{F}(V)| = |G/B| = \frac{(q^n - 1) \cdots (q^2 - 1)(q - 1)}{(q - 1)^n},$$

which we have seen to be a polynomial $P_n(q)$ in $q$ of degree $n(n-1)/2$.

For any field $F$ there is still a complete geometry of flags in $V$, defined in the same way. Let us take $F = \mathbb{C}$, with $G = \mathrm{GL}_n(\mathbb{C})$ and $U, B$ defined as above for the field $F = \mathbb{C}$. The polyomial $P_n(q)$ still counts something about $G/B$, but not something so elementary as points, because now the flag variety $G/B$ is infinite.

In fact, $G/B$ is a complex projective variety of dimension $n(n-1)/2$. [2] Any smooth complex projective variety $X$ of dimension $d$ has cohomology groups $H^i(X)$ for $i = 0, 1, \ldots, 2d$ which are finite dimensional complex vector spaces whose dimensions $\dim H^i(X)$ are called the **Betti numbers** of $X$. For example if $X = \mathbb{P}^d(\mathbb{C})$ then $\dim X = d$ and the Betti numbers are $\dim H^i(X) = 1$ for $i = 0, 2, 4, \ldots, 2d$ and $\dim H^i(X) = 0$ for all other $i$.

It turns out that the polynomial $P_n(q)$ above encodes the Betti numbers of $G/B$: Regarding $q$ as a variable, we have

$$\sum_{i=0}^{n(n-1)/2} \dim H^{2i}(G/B) q^i = P_n(q) = \frac{(q^n - 1) \cdots (q^2 - 1)(q - 1)}{(q-1)^n}.$$

The observation that Betti numbers of $G/B$ over $\mathbb{C}$ are determined by the number of points on $G/B$ over finite fields is deep; it led to Weil's conjectures, which were eventually proved by Deligne.

## 10.3 The Burnside Transfer Theorem

If the order of a finite group $G$ factors as $|G| = mp^r$ with $p$ a prime not dividing $m$, it is natural to ask if the group $G$ itself has a corresponding factorization as $G \simeq M\dot{P}$, where $P$ is a Sylow $p$-subgroup of $G$ and $M \leq G$ has order $m$. For example if $G = C_{mp^r}$ is cyclic then $G \simeq C_m \times C_{p^r}$. Since Sylow $p$-subgroups are not normal in general groups, the only reasonable hope would be that $M \trianglelefteq G$ and $G \simeq M \rtimes P$. Such a subgroup $M$, if it exists, is called a **normal $p$-complement**.

Normal $p$-complements do not always exist. For example, $S_4$ has no normal $p$-complement for either $p = 2$ or $p = 3$.

**Lemma 10.9** *Suppose $|G| = mp^r$, where $p \nmid m$. Then $G$ has a normal $p$-complement if and only if the elements of $G$ of order prime to $p$ form a subgroup of $G$.*

**Proof:** Suppose the elements of $G$ of order prime to $p$ form a subgroup $M \leq G$. Then $M$ is normal in $G$, since conjugation preserves orders of elements. Hence $MP \simeq M \rtimes P$ is a subgroup of $G$. To show that $MP = G$, we must show that $|M| = m$. By Cauchy's theorem, $p$ does not divide $|M|$ since $M$ has no elements of order $p$. It therefore suffices to show that $G/M$ is a $p$-group. If this fails, then $G/M$ has an element $xM$ of order $d > 1$, where $p \nmid d$. Then $x^d \in M$, so $x^d$ has order $k$, where $p \nmid k$. That means the order of $x$ divides $kd$, and $p \nmid kd$, so $x \in M$, a contradiction. Hence $G/M$ is a $p$-group, and $G = MP$ as claimed.

[2] A complex projective variety is a closed subset of some projective space $\mathbb{P}^N(\mathbb{C})$ defined by polynomial equations. It turns out that $G/B \subset \mathbb{P}^N(\mathbb{C})$ for $N = 2^{n(n-1)/2} - 1$.

Conversely, let $M$ be a normal subgroup of $G$ of order $m$. Since $p \nmid m$, every element of $M$ has order prime to $p$. Suppose $g \in G$ has order $k$, with $p \nmid k$. Then the order of $gM$ in $G/M$ has order dividing $k$. But $G/M$ is a $p$-group, so $gM = 1$, meaning that so $g \in M$. Therefore $M$ is exactly the set of elements of $G$ of order prime to $p$, and this set is a subgroup of $G$. ■

**Example 1:** Let $G = D_n$ be dihedral of order $2n$. Write $n = m2^r$, where $m$ is odd. Let $M \simeq C_m$ be the subgroup generated by a rotation of order $m$. Then $M$ is a normal 2-complement in $G$. The Sylow 2-subgroups are isomorphic to $D_{2^r}$, and we have

$$D_n \simeq C_m \rtimes D_{2^r},$$

where the reflections in $D_{2^r}$ act by inversion on $C_m$.

**Example 2:** Let $G = A_4$. The subgroup of elements of order prime to 2 forms a subgroup $K \simeq C_2 \times C_2$, and $A_4 = K \rtimes P$, where $P$ is a Sylow 3-subgroup, acting on $M$ via an element of order three in $\mathrm{Aut}(M) = GL_2(2)$. Thus, $K$ is a normal 3-complement. However, $A_4$ has no normal 2-complement, since the elements of order three lie in no proper subgroup of $A_4$.

Having a normal $p$-complement is equivalent to having a surjective homomorphism

$$f : G \longrightarrow P.$$

In general, a group $G$ does not admit nontrivial homomorphisms onto a proper subgroup $H \leq G$. Suppose, however that $H$ is *abelian*, and let $n = [G : H]$. Let $x_1, x_2, \ldots, x_n$ be representatives for the cosets in $G/H$, and let $\sigma : G \to S_n$ be the action of $G$ on $G/H$. Thus, each $g \in G$ gives a permutation $\sigma_g \in S_n$ such that

$$gx_iH = x_{\sigma_g(i)}H, \qquad \forall\, 1 \leq i \leq n.$$

This means that for each $i$ we have an element $h_i(g) \in H$ such that

$$gx_i = x_{\sigma_g(i)}h_i(g).$$

Thus, for each $i$ we have a function $h_i : G \to H$ given by

$$h_i(g) = x^{-1}_{\sigma_g(i)} \cdot g \cdot x_i.$$

Each individual function $h_i$ is not a group homomorphism. However, we have

**Lemma 10.10** *If $H$ is an abelian subgroup of $G$ then the function $T : G \to H$ given by*

$$T(g) = \prod_{i=1}^{n} h_i(g)$$

*is a group homomorphism which does not depend on the choice of coset representatives $\{x_i\}$.*

**Proof:** Let $\{x'_i\}$ be another set of coset representatives for $G/H$. Then $x'_i = x_i k_i$ for some elements $k_i \in H$. The new functions $h'_i(g)$ are given by

$$h'_i(g) = (x'_{\sigma_g(i)})^{-1} \cdot g \cdot x'_i = k^{-1}_{\sigma_g(i)} x^{-1}_{\sigma_g(i)} \cdot g \cdot x_i k_i = k^{-1}_{\sigma_g(i)} h_i(g) k_i = h_i(g) k^{-1}_{\sigma_g(i)} k_i,$$

since $H$ is abelian. Taking the product we get

$$\prod_{i=1}^{n} h_i'(g) = \prod_{i=1}^{n} h_i(g) k_{\sigma_g(i)}^{-1} k_i = T(g),$$

since $\prod k_{\sigma_g(i)} = \prod k_i$. Hence $T(g)$ is independent of the choice of coset representatives $\{x_i\}$.

If $g, y$ are two elements of $G$, we have

$$\begin{aligned} T(gy) &= \prod_{i=1}^{n} x_{\sigma_{gy}(i)}^{-1} gyx_i \\ &= \prod_{i=1}^{n} (x_{\sigma_{gy}(i)}^{-1} g x_{\sigma_y(i)}) \cdot (x_{\sigma_y(i)}^{-1} y x_i) \\ &= \prod_{i=1}^{n} (x_{\sigma_g(\sigma_y(i))}^{-1} g x_{\sigma_y(i)}) \cdot T(y) \\ &= \prod_{i=1}^{n} (x_{\sigma_g(i)}^{-1} g x_i) \cdot T(y) = T(g)T(y), \end{aligned}$$

again since the product over $\sigma_y(i)$ equals the product over $i$. Hence $T : G \to H$ is a homomorphism.

■

The homomorphism $T$ in Lemma 10.10 is called the **Transfer map**. We can compute $T(g)$, for fixed $g \in G$, as a product over double cosets as follows. Let $\Gamma = \langle g \rangle$ and choose a $\Gamma$-orbit $O = \Gamma \cdot xH$ in $G/H$, and set $a = |O|$. Let $x_1 = x,\ x_2 = gx,\ x_3 = g^2x,\ \ldots\ , x_a = g^{a-1}x$. Then

$$h_1 = h_2 = \cdots = h_{a-1} = 1 \qquad \text{and} \qquad h_a = x^{-1} g x_a = x^{-1} g^a x.$$

The last term is the only contribution from $O$ to the product in $T(g)$. Note that if $\Gamma$ acts freely on $O$ then $g^a = 1$, so $x^{-1} g^a x = 1$. Doing this for each orbit, we find that if $xH,\ yH,\ zH,\ \ldots$ are representatives of the distinct $\Gamma$-orbits on $G/H$, having sizes $a, b, c, \ldots$, then

$$T(g) = (x^{-1} g^a x) \cdot (y^{-1} g^b y) \cdot (z^{-1} g^c z) \cdots .$$

Each term in parentheses lies in the abelian group $H$, so the product can be taken in any order, and the only terms contributing to $T(g)$ come from $\Gamma$-orbits which are not free.

Now suppose $p$ is a prime dividing $|G|$ and $P$ is a Sylow $p$-subgroup of $G$. The center $Z(P)$ is nontrivial, and abelian, so we have the transfer homomorphism

$$T : G \longrightarrow Z(P).$$

**Lemma 10.11** *If $x, y \in Z(P)$ are conjugate in $G$, then they are conjugate in $N_G(P)$.*

**Proof:** If $x^g = y$, then $y \in Z(P) \cap Z(P)^g = Z(P) \cap Z(P^g)$, so $P, P^g \leq C_G(y)$. Thus, $P$ and $P^g$ are two Sylow $p$-subgroups of $C_G(y)$, so there is $h \in C_G(y)$ such that $P = P^{gh}$. Then $gh \in N(P)$ and $x^{gh} = y^h = y$, so $x$ and $y$ are conjugate in $N(P)$, as claimed. ■

**Remark:** Two elements $x, y$ in a subgroup $H \leq G$ are *fused* in $G$ if they are conjugate in $G$, but not necessarily conjugate by an element of $N_G(H)$. A result like Lemma 10.11 is therefore said to *control fusion*.

Now, if $g \in Z(P)$, each term $x^{-1}g^a x$ in $T(g)$ is conjugate in $G$ to $g^a$ hence is conjugate in $N_G(P)$ to $g^a$, by Lemma 10.11.

Let us now assume that that

$$N_G(P) = C_G(P).$$

This is equivalent to assuming that $P = Z(P)$ (that is, $P$ is abelian) and that the conjugation action of $N_G(P)$ on $P$ is trivial. Consider the transfer map

$$T : G \longrightarrow P.$$

Then $x^{-1}g^a x = g^a$ for each term in $T(g)$, so that

$$T(g) = g^{a+b+c+\cdots} = g^m,$$

where $a, b, c, \ldots$ are the sizes of the $P$-orbits on $G/P$ and $m = [G : P]$. Since $p \nmid m$, the map $g \mapsto g^m$ is an automorphism of the abelian group $P$. Hence the transfer map $T : G \to P$ is surjective; we even have $T(P) = P$. This proves the following.

**Theorem 10.12 (Burnside Transfer Theorem)** *Let $G$ be a finite group and let $P$ be a Sylow $p$-subgroup of $G$ such that $N_G(P) = C_G(P)$. Then $G$ has a normal $p$-complement. In fact, $G = M \rtimes P$, where $M$ is the kernel of the transfer map $T : G \to P$.*

**Example 3:** Let $G$ be a group of order $728 = 2^3 \cdot 7 \cdot 13$ and consider the 7-factorization

$$|G| = 7 \cdot \nu \cdot (1 + 7k).$$

Assume the Sylow 7-subgroups of $G$ are not normal in $G$. Then, since $n_7 = 1 + 7k$ divides $8 \cdot 13$ and $k > 0$, we must have $n_7 = 8$. Hence $|N_G(P)| = 7 \cdot 13$. Since $7 \not\equiv 1 \mod 13$, it follows from Prop. 14.6 that $N_G(P)$ is abelian, so that $N_G(P) = C_G(P)$. Hence $G$ contains a normal 7-complement $M$ of order $8 \cdot 13$.

**Corollary 10.13** *Let $p$ be the smallest prime dividing $|G|$. If the Sylow $p$-subgroups in $G$ are cyclic, then $G$ has a normal $p$-complement.*

**Proof:** Let $P$ be a Sylow $p$-subgroup of $G$ and assume that $P$ is cyclic of order $p^r$. Then

$$N_G(P)/C_G(P) \leq \mathrm{Aut}(P) \simeq (\mathbb{Z}/p^r\mathbb{Z})^\times.$$

The latter group has order $p^{r-1}(p-1)$. Since $P$ is abelian, we have $P \leq C_G(P)$, so that the order of $N_G(P)/C_G(P)$ is prime to $p$, hence must divide $p - 1$. But $p$ is the smallest prime dividing $|G|$, so no prime can divide $N_G(P)/C_G(P)$. Hence $N_G(P) = C_G(P)$ and $G$ has a normal $p$-complement, by the Burnside Transfer Theorem. ■

**Corollary 10.14** *Suppose $|G| = p_1 \cdot p_2 \cdots p_k$ is a product of distinct primes, ordered so that $p_1 > p_2 > \cdots > p_k$. Let $P_i$ be a Sylow $p_i$-subgroup of $G$ for each $i$. Then $P_1 P_2 \cdots P_i$ is a normal subgroup of $P_{i+1}$ for each $i = 1, \ldots, k-1$. In particular, we have $G = P_1 P_2 \cdots P_k$.*

**Proof:** Each $P_i$ is cyclic. By Cor. 10.13 the Sylow $p_k$-subgroup $P_k$ has a normal complement $M$ of order $p_1 \cdot p_2 \cdot p_3 \cdots p_{k-1}$, so $G = M \rtimes P_k$. Repeat with $G$ replaced by $M$, etc. ■

**Corollary 10.15** *Let $p$ be the smallest prime dividing $|G|$. If the Sylow $p$-subgroups in $G$ are isomorphic to $C_p \times C_p$ then either $G$ has a normal $p$-complement or the following holds: $p = 2$ and $|N_G(P)/C_G(P)| = 3$ and $G$ has a unique conjugacy class of elements of order two.*

**Proof:** The idea is similar to that of Cor. 10.13, so we sketch the proof and leave the details as an exercise. In this situation we have

$$N_G(P)/C_G(P) \hookrightarrow \mathrm{Aut}(P) = GL_2(p),$$

which leads to $|N_G(P)/C_G(P)|$ dividing $p+1$. If $N_G(P) \neq C_G(P)$ then $p = 2$ and the result follows from Lemma 10.11. ■

The second possibility in Cor. 10.15 occurs for the alternating group $A_5$.

## 10.4 Simple groups

The Sylow and Burnside Transfer Theorems can be used to narrow the possible orders of small simple groups, and to prove uniqueness of simple groups of a given order.

Throughout this section $P$ is a Sylow $p$-subgroup of a simple group $G$ with $p$-factorization

$$|G| = p^r \cdot \nu \cdot (1 + pk),$$

where $\nu = [N_G(P) : P]$ and $1 + pk = n_p = [G : N_G(P)]$.

The first lemma is a variant of the Burnside Transfer Theorem with a weaker hypothesis, and weaker, but still useful result.

**Lemma 10.16** *If $P$ is abelian then no non-identity element $g \in P$ is centralized by $N_G(P)$.*

**Proof:** The proof of Thm. 10.12 shows that the transfer $T : G \to P$ is nontrivial on any non-identity element of $P$ which is centralized by $N_G(P)$. ■

**Lemma 10.17** *We have $k \geq 1$. If $\nu = 1$ then $r \geq 3$.*

**Proof:** If $k = 0$ then $G$ has a normal Sylow $p$-subgroup. If $r \leq 2$ then the Sylow $p$-subgroups $P \leq G$ are abelian, hence $\nu \geq 2$ by Lemma 10.16. ■

**Lemma 10.18** *If $k = 1$ then $r = 1$ and $\nu \mid (p-1)$.*

**Proof:** Let $X$ be the set of Sylow $p$-subgroups of $G$. The action of $G$ on $X$ embeds $G \hookrightarrow S_{p+1}$. Since $p^2 \nmid (p+1)!$ we have $r = 1$.

The condition $k = 1$ also implies that $P$ is transitive on $X - \{P\}$. If $g \in C_G(P)$ fixes some $Q \in X - \{P\}$, then ${}^{gx}Q = {}^{x}Q$ for all $x \in P$, so $g$ is trivial on $X$, hence $g = 1$, since $G$ is simple. Hence $C_G(P)$ acts freely on $X - \{P\}$, so $C_G(P) = P$ and $N_G(P)/P = N_G(P)/C_G(P)$ embeds in $\mathrm{Aut}(P) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$. Therefore $\nu \mid (p-1)$. ■

We study the minimal case:

**Proposition 10.19** *Let $G$ be a simple group of order $p \cdot 2 \cdot (1+p)$, where $p$ is a prime. Then this is the $p$-factorization of $G$ and we have*

1. *The normalizer of a Sylow $p$-subgroup of $G$ is dihedral of order $2p$.*
2. $p \equiv 5 \mod 24$.

**Proof:** Note that $p > 2$ since no group of order 12 is simple. Hence $\mathsf{v}_p(|G|) = 1$, so the $p$-factorization of $|G|$ is $p \cdot \nu \cdot (1 + kp)$ for some $\nu \geq 2$ and $k \geq 1$. Thus we have $2 \cdot (1+p) = \nu \cdot (1+kp)$, which implies $\nu = 2$ and $k = 1$.

Now $N(P)/P$ is the unique subgroup of order two in $\mathrm{Aut}(P) = C_{p-1}$, hence acts by inversion on $P$. This proves that $N(P) \simeq D_p$. More precisely, we have $N(P) = \langle a \rangle \rtimes \langle s \rangle$ where $a$ has order $p$ and $s$ has order two and $sas = a^{-1}$. Moreover, $N(P)$ contains $p$ involutions $a^i s a^{-i}$, for $1 \leq i \leq p$.

The set $X$ of Sylow $p$-subgroups of $G$ has cardinality $|X| = n_p = p + 1$ and the conjugation action of $G$ on $X$ gives a homomorphism

$$\sigma : G \to S_{p+1}$$

whose image lies in $A_{p+1}$ since $G$ is simple.

Since $\sigma(a)$ normalizes $P$ and no other Sylow $p$-subgroup, the cycle type of $\sigma(a)$ is $[p, 1]$. This element generates its own centralizer in $S_{p+1}$. We number the elements of $X$ so that $\sigma(a) = (1\ 2\ \ldots p)$. This element is inverted by the involution $\tau = (1\ p)(2\ p-1)\cdots((p-1)/2\ (p+3)/2)$, as well as the involution $\sigma(s) \in \sigma(G)$. It follows that $\tau^{-1} \cdot \sigma(a) \in \sigma(P)$, so $\tau \in \sigma(P) \subset A_{p+1}$. It follows that $p \equiv 1 \mod 4$.

Now the 2-factorization of $|G|$ is

$$2^2 \cdot \nu_2 \cdot (1 + 2k_2).$$

And a Sylow 2-subgroup $Q$ is isomorphic to $C_2 \times C_2$. The centralizer $C(s)$ of an involution $s \in N(P)$ must permute its two fixed points $\{P, P_1\}$ on $X$, but $s$ generates its own centralizer in $N(P)$, so $C(s)$ acts transitively on $\{P, P_1\}$. Hence $|C(s)| = 4$ and $C(s) = Q$ is a Sylow 2-subgroup of $G$ and $C(Q) = Q$.

The quotient $N(Q)/Q$ is a nontrivial subgroup of $Aut(P) = GL_2(2)$ of order three. Hence $N(Q) \simeq A_4$, acting transitively on $Q - \{1\}$, so $G$ has exactly one conjugacy class of involutions and there are $p(p+1)/2$ of them. Also $G$ has

$$n_2 = p\left(\frac{p+1}{6}\right)$$

Sylow 2-subgroups. In particular, we must have $p \equiv 2 \mod 3$.

Having established that

$$p \equiv 1 \mod 4 \qquad \text{and} \qquad p \equiv 2 \mod 3,$$

we conclude from the Chinese Remainder theorem that $p \equiv 5 \mod 12$.

Each of the $\binom{p+1}{2}$ involutions in $G$ can be conjugated into $Q$ and all involutions in $Q$ are conjugate by $N(Q)$. Since $Q$ is the full centralizer of its involutions, it follows that $s$ can normalize no other 2-Sylow but $Q$, hence $s$ has cycle type $12^{(n_2-1)/2}$ on the set of 2-Sylows, so $(n_2-1)/2$ is even. Writing $p = 12k+5$, it follows that $(n_2-1)/2 = (3k+2)(4k+1)$ is even, so $k$ is even and $p \equiv 5 \mod 24$.

■

If $p = 5$ such a simple group exists, namely $A_5$ has 5-factorization

$$|A_5| = 60 = 5 \cdot 2 \cdot (1+5).$$

Perhaps this is the only simple group of order $2p(p+1)$. For the next possibility $p = 29$ we would have

$$|G| = 29 \cdot 2 \cdot (1+29) = 5724,$$

whose 5-factorization shows that $G$ is not simple.

### 10.4.1 The simple group of order 60

The smallest group order divisible by three primes $p < q < r$ for which the Sylow $p$-subgroup is not cyclic is $2^2 \cdot 3 \cdot 5 = 60$. We have proved that such a simple group exists, namely the alternating group $A_5$. We now prove that this simple group is the unique one of its order.

**Corollary 10.20** *Any simple group $G$ of order 60 is isomorphic to the alternating group $A_5$.*

**Proof:** The 2-factorization is $60 = 2^2 \cdot \nu \cdot (1+2k)$, so $\nu = 3$ or $\nu = 5$. But a Sylow 2-subgroup $P \leq G$ is isomorphic to $C_2 \times C_2$, by Prop. 10.13, so $\mathrm{Aut}(P) = \mathrm{GL}_2(2)$ has order six. Hence $\nu = 3$, and $n_2 = 5$, giving an injective homomorphism $\varphi : G \hookrightarrow S_5$, whose image is contained in $A_5$, since $G$ is simple. Since $G$ and $A_5$ have the same order, $\varphi$ is an isomorphism $G \simeq A_5$. ■

The group $\mathrm{PSL}_2(5)$ has order $5 \cdot (5^2-1)/2 = 60$ and is simple. See Thm. 8.16. Hence Cor. 10.20 implies that

$$\mathrm{PSL}_2(5) \simeq A_5. \tag{32}$$

An explicit isomorphism

$$\mathrm{PGL}_2(5) \simeq S_5 \tag{33}$$

which restricts to an isomorphism (32) may be obtained as follows.

The group $\mathrm{PGL}_2(5)$ acts faithfully by fractional transformations $\frac{ax+b}{cx+d}$ on the projective space $\mathbb{P}^1(5) = F \cup \{\infty\}$ over the field $F$ of five elements. Thus, $\mathrm{PGL}_2(5) \hookrightarrow S_6$ and elements of $\mathrm{PGL}_2(5)$ may be regarded as permutations of $\{\infty, 0, 1, 2, 3, 4\}$. From the Bruhat decomposition, $\mathrm{PGL}_2(5)$ is generated by three elements $a, b, w$, where

$$a(x) = 2x, \qquad b(x) = x + 1, \qquad w(x) = 1/x$$

as fractional transformations. As permutations, we have

$$a = (1\ 2\ 4\ 3), \qquad b = (0\ 1\ 2\ 3\ 4), \qquad w = (\infty\ 0)(2\ 3).$$

Consider the 222 cycle $\pi_0 = (\infty\ 0)(1\ 4)(2\ 3) \in S_6$. This is the unique 222-cycle fixed under conjugation by both $a$ and $w$, which follows from the fact that $1 + 4 = 2 + 3 = 0$. We take the conjugates of $\pi_0$ under $b$, obtaining $\pi_1, \pi_2, \pi_3, \pi_4$, where $\pi_i = b^i \pi_0 b^{-i}$. Explicitly, we have [3]

$$\begin{aligned}
\pi_0 &= (\infty\ 0)(1\ 4)(2\ 3) \\
\pi_1 &= (\infty\ 1)(2\ 0)(3\ 4) \\
\pi_2 &= (\infty\ 2)(3\ 1)(4\ 0) \\
\pi_3 &= (\infty\ 3)(4\ 2)(0\ 1) \\
\pi_4 &= (\infty\ 4)(0\ 3)(1\ 2).
\end{aligned}$$

The set $\Pi = \{\pi_i : i \in \mathbb{Z}/5\mathbb{Z}\}$ is closed under conjugation by all of $\mathrm{PGL}_2(5)$. To see this, we note first that $\Pi$ is closed under $b$ by construction, and since $a\pi_0 a^{-1} = \pi_0$, it follows that $a\pi_i a^{-1} = \pi_{2i}$. So far we could have made similar $2^k$-cycles for any prime $p = 2k + 1$. But since $p = 5$, it happens that $w$ interchanges $\pi_1 \leftrightarrow \pi_3$ and $\pi_2 \leftrightarrow \pi_4$. As $\pi_0$ has been chosen to be fixed by $w$, it follows that $\Pi$ is indeed closed under conjugation by $\mathrm{PGL}_2(5)$, so we have a homomorphism $\varphi : \mathrm{PGL}_2(5) \to S_5$ sending

$$\begin{aligned}
a &\mapsto (1\ 2\ 4\ 3) \\
b &\mapsto (0\ 1\ 2\ 3\ 4) \\
w &\mapsto (1\ 3)(2\ 4).
\end{aligned}$$

Since $\mathrm{PSL}_2(5)$ is simple, it follows that $\varphi$ is injective, hence is an isomorphism by orders, and it must restrict to an isomorphism $\mathrm{PSL}_2(5) \xrightarrow{\sim} A_5$.

### 10.4.2 The simple group of order 168

**Proposition 10.21** *Let $G$ be a group of order $168 = 7 \cdot 3 \cdot 8$ such that no Sylow subgroup of $G$ is normal in $G$. Then $G \simeq \mathrm{PSL}_2(7)$.*

[3] As an aside, note that these 222-cycles partition the 15 transpositions of $S_6$ into five sets of three.

**Proof:** [4] The idea is to find a copy of the Bruhat decomposition in $G$ and use this to determine the multiplication table. For $p \in \{2, 3, 7\}$, let $n_p$ be the number of Sylow $p$-subgroups of $G$.

The 7-factorization of $G$ has the form $7 \cdot \nu \cdot (1 + 7k) = 7 \cdot 24$. Since $n_7 > 1$, we must have $n_7 = 8$. Let $P$ be a Sylow 7-subgroup. Its normalizer $H = N_G(P)$ has order $|H| = 21$, and $H = PQ$, where $Q$ is a Sylow 3-subgroup of $G$ contained in $H$.

(i) *$H$ is a maximal proper subgroup of $G$.*
Suppose $H \leq K \leq G$. Then $H = N_K(P)$, so there are $[K : H]$ Sylow 7-subgroups of $K$ and $[K : H] = 1 + 7\ell$ divides $[G : H] = 8$. Hence $[K : H] = 1$ or $8$, meaning $K = H$ or $K = G$.

(ii) *$H$ is the unique nonabelian group of order 21*
If $H$ were abelian, we would have $H \leq N_G(Q) \neq G$, forcing $H = N_G(Q)$ by maximality. But then $n_3 = [G : H] = 8$, which is impossible since $8 \not\equiv 1 \mod 3$. Therefore $H$ is nonabelian. We have seen there is a unique nonabelian group of order 21; it is isomorphic to a Borel subgroup of $\mathrm{PSL}_2(7)$.

(iii) *$G$ has 28 Sylow 3-subgroups*
We have seen that $Q$ is not normal in $H$. Since $[H : Q] = 7$ is prime, it follows that $N_H(Q) = Q$, so $H$ has 7 Sylow 3-subgroups, any two of which generate $H$. If these were all of the Sylow 3-subgroups of $G$ then they would generate a normal subgroup of $G$, implying $H \triangleleft G$. But $H$ has only one Sylow 7-subgroup, and $G$ has a Sylow 7-subgroup not contained in $H$, contradicting the conjugacy of Sylow 7-subgroups. Hence $n_3 > 7$, with $n_3 \equiv 1 \mod 3$ and $n_3 \mid 56$. The only possibility is $n_3 = 28$.

(iv) *The normalizer $K = N_G(Q)$ is isomorphic to the symmetric group $S_3$.*
From the previous step, we have $|K| = 168/28 = 6$. Any Sylow subgroup is characteristic in its normalizer, so $N_G(K) = K$. Hence $K$ has 28 conjugates. If $K$ were abelian, it would be cyclic. If this were true, each conjugate of $K$ would contain a distinct pair of generators of order six, giving 56 elements of order six, along with $56 = 2 \cdot n_3$ elements of order 3 and $48 = 6 \cdot n_7$ elements of order 7. This makes 160 elements, forcing $n_2 = 1$, a contradiction.

Let $t$ be an element in $K$ of order two.

(v) *The group $H \times P$ acts freely on the double coset $HtP$, and $G = H \cup HtP$.*
Since $|H| = 21$, we have $t \notin H$, so $P^t \neq P$. Since $P$ is the unique Sylow 7-subgroup of $H$, we have $H \cap P^t = \{1\}$. It follows that $H \times P$ acts freely on $HtP$. Hence $|HtP| = 21 \cdot 7 = |G| - |H|$. Therefore $H$ and $HtP$ are distinct and exhaust $G$.

The preceding step shows that every element $g \in G - H$ can be decomposed as $g = pqtp'$ for unique elements $p, p' \in P$ and $q \in Q$. We wish to calculate this decomposition for certain elements in $G - H$. Let $P^* = P - \{1\}$. Then $tP^*t \subset G - H$ since $H \cap P^t = \{1\}$.

**Lemma 10.22** *The intersection $P \cap tPtPt$ consists of a pair of distinct mutually inverse elements:*

$$P \cap tPtPt = \{u, u^{-1}\} \subset P^*.$$

*Let $s \in Q$ be the unique element such that $u^s = u^2$. Then $P^* = \{u, u^{-1}, u^2, u^{-2}, u^4, u^{-4}\}$ and the*

[4] This proof comes from [Suzuki *Group Theory I*], with some simplifications made.

*elements of $tP^*t$ decompose in $PQtP$ as*

$$\begin{array}{lll} tut = u^{-1}tu^{-1} & tu^2t = u^{-4}s^2tu^{-4} & tu^4t = u^{-2}stu^{-2} \\ tu^{-1}t = utu & tu^{-2}t = u^4stu^4 & tu^{-4}t = u^2stu^2. \end{array} \tag{34}$$

**Proof:** Since $Q = \{1, s, s^2\}$, we have a partition

$$PQtP = PtP \cup PstP \cup Ps^2tP.$$

Since $tP^*t \subset PQtP$, we have a partition

$$tP^*t = A_0 \cup A_1 \cup A_2,$$

where $A_i = tP^*t \cap Ps^itP$. Since $s$ normalizes $P$, we have

$$[tP^*t]^s = tsP^*s^{-1}t = tP^*t,$$

and

$$[Ps^itP]^s = Ps^{-1}s^itsP = Ps^{i-2}tP = Ps^{i+1}tP.$$

It follows that $A_i^s = A_{i+1}$, with subscripts read modulo 3. As $|tP^*t| = |P^*| = 6$, it follows that $|A_i| = 2$ for each $i$. And as each $A_i$ is closed under inversion, we must have

$$A_0 = \{tu^{\pm 1}t\}, \qquad A_1 = \{s^{-1}tu^{\pm 1}ts\}, \qquad A_2 = \{stu^{\pm 1}ts^{-1}\}.$$

We next show that

$$tut = u^{-1}tu^{-1}. \tag{35}$$

Since $tut \in PtP$, we have

$$tut = vtw$$

for some $v, w \in P$. Since $t^2 = 1$ this means also that

$$tvt = utw^{-1}.$$

Now $w \neq 1$, lest $tu = v \in PtP \cap P = \varnothing$. Since $w \in P$ which has odd order, we cannot have $w^2 = 1$ either. From (v) it then follows that $tut \neq tvt$. But both $tut$ and $tvt$ are in $tPt \cap PtP = \{tu^{\pm 1}t\}$. It follows that $v = u^{-1}$. Now we have

$$utw^{-1} = tu^{-1}t = (tut)^{-1} = w^{-1}tu,$$

so again by (v) we have $w = u^{-1}$ and (35) is proved.

The remaining formulas in (34) follow upon conjugating (35) by $s$ and taking inverses.

■

We now show how the product of two elements $g, g' \in G$ is determined.

Case 1: $g, g' \in H$. Here the product $gg'$ is determined by the known structure of $H$.

Case 2: $g \in H$ and $g' \in HtP$. Here $g' = htp$ and $gg' = (gh)tp$ where $gh$ is again computed in $H$.

Case 3: $g \in HtP$ and $g' \in H$. Here $g = htp$ and $gg' = ht(pg')$. Since $pg' \in H = QP$, we can write $pg' = qp'$ for some $q \in Q$ and $p' \in P$. Then $t, q \in K = S_3$, so $tq = q^{-1}t$ so we have $gg' = ht(pg') = ht(qp') = hq^{-1}p'$, with $hq^{-1} \in H$. Hence $gg'$ can again be computed from the structure of $H$.

Case 4: This final case is where $g$ and $g'$ are both in $HtP$. Here $g = htp$ and $g' = h'tp'$. Write $h' = p_1q_1$, with $p_1 \in P$, $q_1 \in Q$. Then

$$gg' = htp \cdot h'tp' = ht(pp_1)q_1tp' = h \cdot t(pp_1)t \cdot q_1^{-1}p'. \tag{36}$$

If $pp_1 = 1$ this is a product in $H$. If $pp_1 \neq 1$ then $pp_1 \in P^* = \{u, u^{-1}, u^2, u^{-2}, u^4, u^{-4}\}$, so the decomposition of $t(pp_1)t$ in $PQtP$ is given by Lemma 34. Thus the product $gg'$ is determined.

We have shown that there is only one isomorphism class of groups of order 168 having no normal Sylow subgroups. As $\mathrm{PSL}_2(7)$ is one such group, the theorem is proved. ■

The group $G = \mathrm{GL}_3(2)$ also has order $2^3(2^3-1)(2^2-1)(2-1) = 168$. The upper and lower triangular matrices in $G$ are distinct Sylow 2-subgroups. The elements

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \tag{37}$$

generate distinct Sylow 3-subgroups. The elements

$$u = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \qquad v = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} \tag{38}$$

generate distinct Sylow 7-subgroups. [5] From Prop. 10.21 it follows that we have another exceptional isomorphism

$$\mathrm{PSL}_2(7) \simeq \mathrm{GL}_3(2). \tag{39}$$

This makes clear, for example, that the Sylow 2-subgroups of $\mathrm{PSL}_2(7)$ are $D_4$, and that $\mathrm{PSL}_2(7)$ acts faithfully on two sets of seven elements: the seven lines and the seven planes in $(\mathbb{Z}/2\mathbb{Z})^3$.

These two actions imply that $\mathrm{PSL}_2(7)$ has an outer automorphism $\sigma$ given by $\sigma(g) = {}^tg^{-1}$, the inverse transpose in $\mathrm{GL}_3(2)$. Indeed, since the normalizer of a Sylow 7-subgroup is $G_{21}$ (see step (ii) above), it follows that $G$ has exactly two conjugacy-classes of elements of order 7. The elements $u, v$ in (38) have $\mathrm{tr}(u) = 0$ and $\mathrm{tr}(v) = 1$, so they are not conjugate. Thus, the trace function distinguishes the two classes of elements of order 7. Since

$$\sigma(u) = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

[5] The matrices $u, v$ were found by factoring the cyclotomic polynomial

$$\Phi_7(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 = (1 + x + x^3)(1 + x^2 + x^3)$$

over $\mathbb{Z}/2\mathbb{Z}$ and using rational canonical form.

has $\mathrm{tr}(\sigma(u)) = 1$, it follows that $\sigma(u)$ is not conjugate to $u$, so $\sigma$ is not inner. Hence there are in fact two non-conjugate isomorphisms (39).

We can see them explicitly as follows. To give a homomorphism $\mathrm{PSL}_2(7) \to \mathrm{GL}_3(2)$ is to give an elementary abelian 2-group $E$ of rank 3 and an action of $\mathrm{PSL}_2(7)$ on $E$ by automorphisms. Now, $\mathrm{PSL}_2(7)$ acts by fractional transformations of the projective line $\mathbb{P}^1(F) = F \cup \{\infty\}$, by which we view $\mathrm{PSL}_2(7)$ as a subgroup of the symmetric group $S_8$, permuting the points in $\mathbb{P}^1(F) = \{\infty, 0, 1, 2, 3, 4, 5, 6\}$. We will find $E$ as a subgroup of $S_8$ normalized by $\mathrm{PSL}_2(7)$.

Since $F^{\times 2} = \langle 2 \rangle$, the Bruhat decomposition implies that $\mathrm{PSL}_2(7)$ is generated by three transformations

$$a(x) = 2x, \qquad b(x) = x + 1, \qquad w(x) = -1/x.$$

As permutations of $\{\infty, 0, 1, 2, 3, 4, 5, 6\}$, these are elements of $S_8$ given by

$$a = (1\ 2\ 4)(3\ 6\ 5), \qquad b = (0\ 1\ 2\ 3\ 4\ 5\ 6), \qquad w = (\infty\ 0)(1\ 6)(2\ 3)(4\ 5).$$

The subgroup $\langle a, b \rangle$ is the Borel subgroup of $\mathrm{PSL}_2(7)$ fixing $\infty$ and is the $G_{21}$ from step (ii). To find $E$ in $S_8$, we note that the matrices (37) and (38) permute the seven nonzero vectors in $(\mathbb{Z}/2\mathbb{Z})^3$ in cycle types $[331]$ and $[7]$, respectively. So $E - \{1\}$ must consist of seven commuting elements $e_1, \ldots, e_7$ of order two permuted in the same way. Exactly one of them, say $e_1$, is fixed by $a$ and the remaining $e_{i+1} = b^i e_1 b^{-i}$ for $1 \le i \le 6$. From our experience with $\mathrm{PGL}_2(5)$ we guess $e_1$ has the form

$$e_1 = (\infty\ 0)(1\ x)(2\ 2x)(4\ 4x),$$

for some $x \in \{3, 5, 6\}$. But the element

$$e_2 = be_1b^{-1} = (\infty\ 1)(2\ x+1)(3\ 2x+1)(5\ 4x+1)$$

must commute with $e_1$. If $x = 6$ these two elements would be

$$(\infty\ 0)(1\ 6)(2\ 5)(4\ 3) \qquad \text{and} \qquad (\infty\ 1)(2\ 0)(3\ 6)(5\ 4),$$

which do not commute. Therefore $x \in \{3, 5\}$. In fact both of these choices work, and we get two subgroups $E = \{e_i\}, E' = \{e'_i\}$, where $e_0 = e'_0$ is the identity of $S_8$ and [6]

$$\begin{array}{ll|ll}
e_1 & = (\infty\ 0)(1\ 3)(2\ 6)(4\ 5) & e'_1 & = (\infty\ 0)(1\ 5)(2\ 3)(4\ 6) \\
e_2 & = (\infty\ 1)(2\ 4)(3\ 0)(5\ 6) & e'_2 & = (\infty\ 1)(2\ 6)(3\ 4)(5\ 0) \\
e_3 & = (\infty\ 2)(3\ 5)(4\ 1)(6\ 0) & e'_3 & = (\infty\ 2)(3\ 0)(4\ 5)(6\ 1) \\
e_4 & = (\infty\ 3)(4\ 6)(5\ 2)(0\ 1) & e'_4 & = (\infty\ 3)(4\ 1)(5\ 6)(0\ 2) \\
e_5 & = (\infty\ 4)(5\ 0)(6\ 3)(1\ 2) & e'_5 & = (\infty\ 4)(5\ 2)(6\ 0)(1\ 3) \\
e_6 & = (\infty\ 5)(6\ 1)(0\ 4)(2\ 3) & e'_6 & = (\infty\ 5)(6\ 3)(0\ 1)(2\ 4) \\
e_7 & = (\infty\ 6)(0\ 2)(1\ 5)(3\ 4) & e'_7 & = (\infty\ 6)(0\ 4)(1\ 2)(3\ 5)
\end{array}$$

Each set $E, E'$ contains 7 commuting involutions normalized by $\langle a, b \rangle$. To see they are closed under multiplication we need only check that $e_1e_2 = e_4$, $e'_1e'_2 = e'_6$ and conjugate these equations by $a$. Hence $E$ and $E'$ are indeed elementary abelian 2-groups of rank 3 normalized by $\langle a, b \rangle$. The remarkable thing is that both sets $\{e_i\}$ and $\{e'_i\}$ are also normalized by the permutation $w = (\infty\ 0)(1\ 6)(2\ 3)(4\ 5)$, so they are normalized by the entire subgroup $\langle a, b, w \rangle \le S_8$. Thus, we recover the two isomorphisms $\mathrm{PSL}_2(7) \simeq \mathrm{GL}_3(2)$ explicitly inside $S_8$.

[6] As an aside, note that these $[2222]$ cycles partition the 28 transpositions of $S_8$ into seven sets of four.

### 10.4.3 Simple groups of order $\leq 720$

We begin with a few more lemmas to help narrow the cases.

**Lemma 10.23** *If $H$ is a group of order $p^r q^s$, where $p$ and $q$ are primes and $r, s \leq 2$ then $H$ is not simple*

**Proof:** We may assume $p > q$. If $H$ is simple then it has $p$-factorization $p^r q^s = p^r \cdot \nu \cdot (1 + kp)$ wth $k \geq 1$. Since $r \leq 2$, the Sylow $p$-subgroups are abelian, so $\nu > 1$. Hence $\nu = q$, $s = 2$ and $q = 1 + kp > p$, a contradiction ■

**Remark:** The restrictions on $r$ and $s$ are unnecessary. Using character theory, Burnside proved that any finite group whose order is divisible by just two primes is not simple.

**Lemma 10.24** *If $|G| = m \cdot p^r$ where $p$ is a prime not dividing $m$, then $m > 7$.*

**Proof:** Since $G$ is simple, the action on Sylow $p$-subgroups embeds $G \hookrightarrow A_m$, so $m \in \{5, 6, 7\}$ and $m \cdot p^r$ divides $m \cdots 3 \cdot 2$. If $m \leq 6$ then $mp^r < 60$ so $G$ is not simple. If $m = 7$ then $p = 5, 3, 2$ and $r \leq 1, 2, 3$ respectively. and the 7-factorization is $\nu \cdot (1 + 7k)$ with $\nu > 1$ and $k > 0$. There are no values of $p$ and $r$ satisfying these conditions. ■

**Lemma 10.25** *If $|G| \leq N$ then $p < \sqrt{N/2}$.*

**Proof:** From Lemma. 10.17, we have $p \cdot 2 \leq p^r \cdot \nu$. Hence

$$p \cdot 2 \cdot (1 + p) \leq |G| \leq N,$$

so $p^2 < p(1 + p) \leq N/2$, and the estimate follows. ■

Now let $G$ be a simple group of order $|G| \leq 720$. Let $p$ be the largest prime dividing $|G|$, with $p$-factorization

$$|G| = p^r \cdot \nu \cdot (1 + kp).$$

We will assume $p \geq 5$ because groups of order $3^a 2^b$ are not simple, by Burnside's $p^a q^b$ theorem (which uses character theory and is not yet in these notes). By Cor. 10.25, we have $p < \sqrt{360} < 19$ so $p \leq 17$. By Prop. 10.19, we exclude the case $(r, \nu, k) = (1, 2, 1)$. This further excludes $p = 17$. Since $p^r \cdot (1 + p) \leq |G| \leq 720$ we have $r = 1$ for $p = 13, 11$, $r \leq 2$ for $p = 7, 5$, $r \leq 4$ for $p = 3$.

We note also:

1. If $r = 1$ then $(\nu, p - 1) > 1$.
2. If $\nu = 2$ then $k$ is odd and $k \geq 3$ by Cors. 10.13 and 10.19.

3. If $k = 1$ then $r = 1$ since $p^2$ does not divide $(p + 1)!$

4. If $r \leq 2$ then $\nu \geq 2$ so $1 + pk \leq 720/2p^r$.

5. No prime divisor of $1 + kp$ can be larger than $p$.

6. If $k$ is even then either $4 \mid \nu$ or $\nu$ is odd.

Since $p^r \cdot (1 + p) \leq |G| \leq 720$ we have $r = 1$ for $p = 13, 11$, $r \leq 2$ for $p = 7, 5$, $r \leq 4$ for $p = 3$.

For $p = 13$ the only surviving case is

$$|G| = 13 \cdot 4 \cdot (1 + 13) = 728,$$

which we showed cannot be the order of a simple group, see Example 3 of section 10.3.

For $p = 11$ it the only surviving case is

$$|G| = 11 \cdot 5 \cdot (1 + 11) = 660,$$

which is the order of the simple group $PSL_2(11)$.

For $p = 7$, we have $r \leq 2$. If $r = 2$ then $\nu \geq 2$ so $1 + 7k \leq (720/2 \cdot 49) < 8$, forcing $k = 0$. Hence $r = 1$ and $\nu \geq 2$. And if $k = 1$ then $\nu \mid 6$, and if $k$ is even then $4 \mid \nu$.

The surviving 7-factorizations are

$$\begin{aligned}
7 \cdot 3 \cdot (1 + 7) &= 2^3 \cdot 3 \cdot 7 = 168 \\
7 \cdot 6 \cdot (1 + 7) &= 2^4 \cdot 3 \cdot 7 = 336 \\
7 \cdot 4 \cdot (1 + 2 \cdot 7) &= 2^2 \cdot 3 \cdot 5 \cdot 7 = 420 \\
7 \cdot 2 \cdot (1 + 5 \cdot 7) &= 2^3 \cdot 3^2 \cdot 7 = 504 \\
7 \cdot 2 \cdot (1 + 7 \cdot 7) &= 2^2 \cdot 5^2 \cdot 7 = 700
\end{aligned}$$

The case $|G| = 168$ is the order of a simple group $\mathrm{PSL}_2(7)$, and this is the unique simple group of order 168 (see Prop. 10.21).

The case $|G| = 336$ has $N_G(P) \simeq P \rtimes C_6$, the $ax + b$ group over $\mathbb{Z}/7\mathbb{Z}$. An element $n \in C_6$ of order six fixes a point $Q \in X - \{P\}$ and is free on $X - \{P, Q\}$, hence has cycle type $[61]$ so is an odd permutation. Hence $G$ has a subgroup of index two. This occurs in nature: The group $\mathrm{PGL}_2(7)$ has order 336 and contains $\mathrm{PSL}_2(7)$ with index two.

The case $|G| = 420$ has an involution $s \in C_G(P)$. Suppose there exists $Q \in X - \{P\}$ and $x \in P$ such that ${}^sQ = {}^xQ$. Then $sx \in N_G(Q)$ so $x^2 \in Q$ so $P = Q$. Hence $s$ interchanges the two $P$-orbits in $X - \{P\}$ and has cycle type $[2^7 1]$ on $X$, which is an odd permutation, so $G$ has a normal subgroup of index two.

The case $|G| = 504$ is the order of a simple group $\mathrm{PSL}_2(8)$.

The case $|G| = 700$ is ruled out by Cor. 10.15.

For $p = 5$ we have $k = 1, 3, 7$ since 5 is the largest prime dividing $1 + 5k$. If $k = 1$ then $r = 1$ and $\nu = 2, 4$ by Lemma 10.18. If $k = 3$ then $5^r \cdot \nu \leq 720/16 = 45$ so $r = 1$ and $\nu \leq 9$ is even. Since groups of order $5 \cdot 2^n$ are not simple, by Lemma 10.24 we have $\nu = 6$. If $k = 7$ then $5^r \cdot \nu \leq 720/36 = 20$ so $r = 1$ and $\nu = 2, 4$.

Thus the surviving 5-factorizations are

$$\begin{aligned} 5 \cdot 2 \cdot (1 + 5) &= 2 \cdot 3 \cdot 5 = 60 \\ 5 \cdot 4 \cdot (1 + 5) &= 2^3 \cdot 3 \cdot 5 = 120 \\ 5 \cdot 6 \cdot (1 + 3 \cdot 5) &= 2^5 \cdot 3 \cdot 5 = 480 \\ 5 \cdot 2 \cdot (1 + 7 \cdot 5) &= 2^3 \cdot 3^2 \cdot 5 = 360 \\ 5 \cdot 4 \cdot (1 + 7 \cdot 5) &= 2^3 \cdot 3^2 \cdot 5 = 720 \end{aligned}$$

The case $5 \cdot 2 \cdot (1 + 5) = 60$ arises from the simple group $A_5 = PSL_2(5)$.

In the case $5 \cdot 4 \cdot (1 + 5) = 120$ the normalizer of a Sylow 5-subgroup contains a 4-cycle in $S_6$, which is odd. Hence $G$ contains a normal subgroup of index two. This actually occurs: The group $S_5$ has order 120 and contains $A_5$ of index two.

In the case $5 \cdot 6 \cdot (1 + 3 \cdot 5) = 480$, we have $N_G(P)$ of order 30, so $N_G(P) = \langle g, s \rangle$ where $g, s$ have order 15 and 2 respectively, and $\langle g^3 \rangle = P$. There are four groups of order 30 according to the possible actions of $s$ on $\langle g \rangle = C_3 \times C_5$ by inverting one or both or no factors. Note that all four groups occur inside the normalizer of a 15-cycle in $S_{15}$. By the Transfer Theorem, $s$ must invert the $C_5$-factor (which is $P$). Now look at the embedding of $N_G(P)$ in $S_{15}$ via its action on $X - \{P\}$. Since $g^3$ acts with cycle type $[5\ 5\ 5]$, it follows that $g$ has cycle type $[15]$, so $\langle g \rangle$ acts freely and transitively on $X - \{P\}$. Hence the action of $s$ on $X - \{P\}$ is equivalent to its action on $C_3 \times C_5$. If $s$ inverts both factors then its cycle type is $[1\ 2^7]$ which is odd. Therefore $s$ centralizes the $C_3$ factor and $N_G(P) \simeq C_3 \times D_5$. [7] Hence the centralizer $C_G(Q)$ of a Sylow 3-subgroup has order at least 30. In the 3-factorization $3 \cdot \nu_3 \cdot n_2$ we must have $\nu_3 = 5 \cdot 2^a$ with $a \geq 2$, lest $C_G(Q) = N_G(Q)$. This forces $n_3 = 4$, so $G$ is not simple

The case $5 \cdot 2 \cdot (1 + 7 \cdot 5) = 360$ arises from the simple group $A_6$.

The case $|G| = 720$ is harder, but still elementary; in the next section we show there are no simple groups of order 720.

Assuming that result, we have shown that the only possible orders $\leq 720$ of nonabelian simple groups $G$ are 60, 168, 360, 504 and 660. Moreover, there exists a simple group of each of these orders, namely

| simple group $G$ | $\lvert G \rvert$ |
|---|---|
| $A_5 \simeq PSL_2(5)$ | 60 |
| $PSL_2(7) \simeq GL_3(2)$ | 168 |
| $A_6 \simeq PSL_2(9)$ | 360 |
| $PSL_2(8)$ | 504 |
| $PSL_2(11)$ | 660 |

[7] Cole (*Simple groups from Order 201 to Order 500*, Am. J. Math, vol 14, no. 4 1892, 378-88), seems to have missed this possibility.

In fact, there is exactly one simple group having each of these orders, but we have only proved this for $|G| = 60$ and $|G| = 168$.

### 10.4.4 Almost-simple groups of order 720

Suppose that $G$ is a simple group of order $720 = 8 \cdot 9 \cdot 10$. Writing the order this way makes it plausible that $G$ should act 3-transitively on a set with 10 elements, as $\mathrm{PGL}_2(9)$ has this order and acts 3-transitively on its set of 10 Sylow 3-subgroups. Since $\mathrm{PGL}_2(9)$ is not simple, it may make sense to look in that direction for a contradiction. So we begin by studying the 3-local structure of our hypothetical simple group $G$ of order 720. However, since there does exist a simple group of order 360, the 2-local structure must eventually be decisive. It is here that Burnside's sketch (which begins with the 5-local structure) [8] seems to have a serious gap. Our treatment of the 3-local part is based on that of Derek Holt [9] which I have recast to better highlight his essential point, with different arguments in places. Then we will have enough information for a correct 2-local argument in the spirit of Burnside.

From the Sylow and Burnside Transfer theorems, the possible 3-factorizations of $|G|$ are

$$|G| = 3^2 \cdot 2 \cdot 40, \qquad \text{or} \qquad |G| = 3^2 \cdot 8 \cdot 10. \tag{40}$$

In the former case, where $n_3(G) = 40$, the normalizer of a Sylow 3-subgroup $P$ acts by an involution on $P$ with trivial fixed points, and normalizes every subgroup of $P$.

Holt's crucial observation about the 3-local structure is as follows.

**Lemma 10.26** *Every subgroup of order three in $G$ is contained in just one Sylow 3-subgroup of $G$.*

**Proof:** Let $Q < G$ be a subgroup of order three, with normalizer $N = N_G(Q)$, and let $P$ be a Sylow 3-subgroup of $G$ containing $Q$. The 3-factorization of $N$ is

$$|N| = 3^2 \cdot \nu \cdot n_3(N),$$

where $\nu = [N \cap N_G(P) : P]$ and $n_3(N)$ is the number of Sylow 3-subgroups in $N$. Since the Sylow 3-subgroups are abelian, any such subgroup containing $Q$ must lie in $N$. So the lemma is equivalent to the assertion that $n_3(N) = 1$.

If $n_3(G) = 40$ then $N_G(P)$ contains an element inverting $P$, hence normalizing $Q$, so $\nu > 1$. If $n_3(G) = 10$ then again $\nu > 1$, lest we have at least $[N_G(P) : N \cap N_G(P)] = [N_G(P) : P] = 8$ conjugates of $Q$ in $P$, whereas the group $P$ of order $3^2$ can have at most four subgroups of order three. Thus, in either case we have $\nu > 1$. We also have $n_3(N) < 10$, lest $G \leq S_4$. It follows that $n_3(N) \in \{1, 4\}$.

Assume that $n_3(N) = 4$. Then $\nu = 2$, lest $[G : N] \leq 5$, so $N$ has 3-factorization

$$|N| = 3^2 \cdot 2 \cdot 4.$$

[8] *Notes on the theory of groups of finite order*, Bull. London Math. Soc. 1894

[9] http://sci.tech-archive.net/Archive/sci.math/2006-12/msg07456.html

Let $P = P_1,\ P_2,\ P_3,\ P_4$ be the Sylow 3-subgroups in $N$, and let $X = \{{}^gQ :\ g \in G\}$ be the set of $G$-conjugates of $Q$. We have $|X| = [G : N] = 10$. The group $G$ acts on $X$ by conjugation and we consider the fixed points of $Q$:

$$X^Q = \{Q' \in X : Q < N_G(Q')\}.$$

Since a group of order three admits no automorphism of order three, we have

$$Q < N_G(Q') \quad \Leftrightarrow \quad Q < C_G(Q') \quad \Leftrightarrow \quad Q' < C_G(Q) \quad \Leftrightarrow \quad Q' < N,$$

in which case $Q' < P_i$ for some $i$. Therefore

$$X^Q = \bigcup_{i=1}^{4} X(P_i), \tag{41}$$

where, for any Sylow $p$-subgroup $P'$ of $G$ we define $X(P') := \{Q' \in X :\ Q' < P'\}$ to be the set of conjugates of $Q$ which are contained in $P'$. Note that ${}^gX(P') = X({}^gP')$ for any $g \in G$. In particular, the sets $X(P_i)$ all have the same cardinality. Since $P$ is abelian, $N_G(P)$ acts transitively on $X(P)$ (by the same argument used for Lemma 10.11) and the stabilizer of $Q$ in $N_G(P)$ has cardinality $|N \cap N_G(P)| = 3^2 \cdot 2$, so $m = [N_G(P) : N_G(P) \cap N] \in \{1, 4\}$, according to the two possibilities for $N_G(P)$ in (40). Finally, since $P_i$ is generated by any two elements of $X(P_i)$, we have $X(P_i) \cap X(P_j) = \{Q\}$ for $i \neq j$. It now follows from (41) that $|X^Q| = 1 + 4(m-1)$. Since $|X^Q| \leq |X| = 10$ we must have $m = 1$, so $X^Q = \{Q\}$ and the $Q$-orbits in $X$ have sizes $1, 3, 3, 3$.

As $\mathrm{Aut}(Q) = C_2$, the centralizer $C_G(Q)$ has order 36 or 72, with Sylow 2-subgroup $R$ of order 4 or 8. As $R$ fixes $Q$ and $G$ is simple, $R$ acts faithfully on $X - \{Q\}$, permuting the three $Q$-orbits therein, giving a homomorphism $R \to S_3$. If $r \in R$ preserves a $Q$-orbit $\{Q_1, Q_2, Q_3\}$ in $X$ then $r$ normalizes each $Q_i$, since $r$ commutes with $Q$. Hence the image of $R$ in $S_3$ is nontrivial, so some $r \in R$ maps to a 2-cycle in $S_3$. This means $r$ has cycle type $[1^3 2^3]$ on $X - \{Q\}$ and cycle type $[1^4 2^3]$ on $X$. Thus $r$ is an odd permutation on $X$, contradicting the simplicity of $G$. It follows that $n_3(N) = 1$ and the lemma is proved. ■

Let $Y$ be the set of Sylow 3-subgroups of $G$ and let $P \in Y$. The lemma implies that $P$ acts simply transitively on $Y - \{P\}$, so $|Y| \equiv 1 \mod 9$. This rules out $n_3(G) = 40$, so we must have $n_3(G) = 10$ and $|N_G(P)| = 3^2 \cdot 8$. Regarding $G$ as a subgroup of $A_{10}$ via its action on $Y$ by conjugation shows that $P$ cannot be cyclic because the normalizer of a 9-cycle in $S_{10}$ has order $3^2 \cdot 6$, hence cannot contain $N_G(P)$. Thus, we find that $P \simeq C_3 \times C_3$.

Choose $P'$ in $Y$ distinct from $P$ and let

$$H = N_G(P) \cap N_G(P')$$

be the normalizer of $P'$ in $N_G(P)$. Since $N_G(P)$ acts transitively on $Y - \{P\}$, it follows that $|H| = 8$, so $H$ is a Sylow 2-subgroup of $N_G(P)$ and $N_G(P) = P \cdot H$. I claim that $H$ acts freely on $P - \{1\}$ by conjugation. For by the lemma again, any nonidentity element $t \in P$ has cycle type $[1333]$ in $Y$, whose centralizer in $A_{10}$ has order $3^3 \cdot 6/2 = 81$ and intersects $H$ trivially. [10]

[10] Since $|H| = 8 = |P - \{1\}|$, it follows that $H$ is also transitive on $P - \{1\}$, so $G$ has a unique conjugacy class of elements of order three, and this class has 80 elements. However we do not need this.

Let $s \in H$ be an involution (an element of order two). Since $s$ acts freely on $P - \{1\}$, it must act by inversion, hence $s$ is the unique involution in $H$. The only groups of order $8$ containing a unique involution are $Q_8$ and $C_8$. In the latter case $H$ would be generated by an $[8]$-cycle on $Y$ which is odd, contradicting the simplicity of $G$. Hence $H \simeq Q_8$. [11] Since $Q_8$ does not embed in $S_n$ for $n < 8$, the faithful action of $H$ on $Y - \{P, P'\}$ must also be free and transitive. Hence the elements of order four in $H$ have cycle type $[1^2 4^4]$ on $Y$, and $s$ has cycle type $[1^2 2^4]$.

If $x \in P - \{1\}$ and $H \cap H^x \neq 1$, then $s \in H \cap H^x$, say $s = h^x$ for some $h$ in $H$. But then $h$ is an involution, so $h = s$, meaning that $x$ and $s$ commute. This contradicts $H$ acting freely on $P - \{1\}$, so $H \cap H^x = 1$. It follows that there are exactly nine $N_G(P)$-conjugates of $s$ in $H$, and these are all of the involutions in $N_G(P)$. From the cycle type of $s$ on $Y$, we see that $N_G(P)$ and $N_G(P')$ are the only conjugates of $N_G(P)$ containing $s$. As there are ten conjugates of $N_G(P)$, there are $9 \cdot 10/2 = 45$ conjugates of $s$ in $G$. Hence the centralizer $S = C_G(s)$ is a Sylow 2-subgroup of $G$. By the same argument there are $45$ conjugates of $H$ in $G$, so $S = N_G(H)$ is also the normalizer of $H$ in $G$.

I claim that distinct involutions have distinct centralizers. For suppose $t \neq s$ is an involution with $C_G(t) = C_G(s)$. Then $t \in N_G(H) - H$ so preserves the fixed point set $Y^H = \{P, P'\}$, but $t$ cannot normalize $P$ or $P'$, so $t$ must switch $P$ and $P'$. But $t$ is a product of 2-cycles and is even, while $10/2$ is odd, so $t$ must have at least two fixed-points on $Y$. This means $t \in N_G(P'') \cap N_G(P''')$ for some pair $P'', P''' \in Y - \{P, P'\}$. But $t$ cannot act trivially on $Y - \{P, P'\}$ lest it be a 2-cycle on $Y$. As $H$, which centralizes $t$, must preserve the fixed points of $t$ in $Y - \{P, P'\}$, this contradicts the transitivity of $H$ on $Y - \{P, P'\}$. [12]

Now take $h \in H$ of order $4$ and consider the action of $H$ on the set $Z$ of Sylow 2-subgroups of $G$. We have $h^2 = s$. Since $s$ is contained in just one Sylow 2-subgroup, namely $C_G(s)$, the cycle type of $s$ on $Z$ is $12^{22}$. Hence the cycle type of $h$ is $[14^{11}]$, which is an odd permutation, contradicting the simplicity of $G$.

■

The argument is difficult for several reasons. First, $720 = 2 \cdot 360$, and there does exist a simple group of order $360$, namely the alternating group $A_6$. Secondly, $A_6 \simeq \mathrm{PSL}_2(9)$ (see section 13.5.2), so $\mathrm{SL}_2(9)$ is a group of order $720$ surjecting onto $A_6$. Thirdly, there are three groups of order $720$ containing $A_6$ with index two (see below). All these groups of order $720$ flirt with the simple group $A_6$, but themselves just fail to be simple, for different reasons, which is why it is hard to rule them out.

The three groups containing $A_6$ with index two can be seen as follows. We have seen that automorphism group of $S_6$ is $\mathrm{Aut}(S_6) = S_6 \rtimes C_2$. It follows that $\mathrm{Out}(A_6) \simeq C_2 \times C_2$. By the Correspondence Theorem, there are three subgroups of $\mathrm{Aut}(A_6)$ of order $720$, containing $A_6$. One of these is $S_6$. Via the isomorphism $A_6 \simeq \mathrm{PSL}_2(9)$, another one is $\mathrm{PGL}_2(9)$. The third group is the **Mathieu Group** $M_{10}$, which is part of a family of highly transitive simple (or almost simple, in the case of $n = 10$) subgroups $M_n \leq S_n$.

To see $M_{10}$ more explicitly, we start with $\mathrm{PGL}_2(9)$, which we think of as the group of permutations of

[11] We do not actually need to know that $H = Q_8$ and not $C_8$.

[12] A similar argument shows that all involutions are conjugate in $G$, but we do not need this.

$\mathbf{P}^1(\mathbb{F}_9)$ given by

$$PGL_2(9) = \left\{ z \mapsto \frac{az+b}{cz+d} : \ ad - bc \neq 0. \right\}.$$

The field $\mathbb{F}_9$ of 9 elements is built from $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ just as $\mathbb{C}$ is built from $\mathbb{R}$, namely,

$$\mathbb{F}_9 = \{x + iy : \ x, y \in \mathbb{F}_3\}, \qquad i^2 = -1,$$

and just like $\mathbb{C}$, $\mathbb{F}_9$ has an automorphism $\overline{x+iy} = x - iy$. We define the group

$$\mathrm{P\Gamma L}_2(9) = \left\{ z \mapsto \frac{az+b}{cz+d} : \ ad - bc \neq 0 \right\} \cup \left\{ z \mapsto \frac{a\bar{z}+b}{c\bar{z}+d} : \ ad - bc \neq 0 \right\}.$$

This group contains $\mathrm{PGL}_2(9)$ with index two; a nontrivial coset representative is simply $z \mapsto \bar{z}$. It turns out that

$\mathrm{P\Gamma L}_2(9) \simeq \mathrm{Aut}(A_6)$. In this viewpoint, $M_{10}$ is the subgroup of $\mathrm{P\Gamma L}_2(9)$ given by

$$M_{10} = \left\{ z \mapsto \frac{az+b}{cz+d} : \ ad - bc \text{ is a square in } \mathbb{F}_9^\times \right\} \cup \left\{ z \mapsto \frac{a\bar{z}+b}{c\bar{z}+d} : \ ad - bc \text{ is a nonsquare in } \mathbb{F}_9^\times \right\}.$$

Thus, $M_{10}$ contains $\mathrm{PSL}_2(9)$ with index two; a nontrivial coset representative is $z \mapsto i\bar{z}$.

The subgroup $S_6$ is generated by $\mathrm{PSL}_2(9)$ and $z \mapsto \bar{z}$. In this guise an outer automorphism of $S_6$ is conjugation by $z \mapsto iz$.

# 11 Solvable and nilpotent groups

A group $G$ is **solvable** if it has a chain of subgroups

$$1 = G_0 < G_1 \lhd G_2 \lhd G_3 \lhd \cdots \lhd G_n = G \tag{42}$$

where each $G_i$ is normal in $G_{i+1}$ with abelian quotient $G_{i+1}/G_i$.

If $H \lhd G$ then $G$ is solvable if and only if both $H$ and $G/H$ are solvable (exercise). It follows that $G$ is *not* solvable precisely when there exist subgroups $H \lhd K \leq G$ with $K/H$ nonabelian simple. In this sense solvable groups are diametrically opposed to nonabelian simple groups.

**Examples of Solvable Groups:**

i) Any finite group $G$ with $|G| < 60$ is solvable, because there are no simple groups of order $< 60$. In particular $S_n$ is solvable for $n \leq 4$. However, $S_n$ is not solvable when $n \geq 5$, because it contains the simple group $A_5$.

ii) The dihedral group $D_n$ is solvable for every $n \geq 2$ because it has a chain of subgroups $1 < C_n < G$ and $G/C_n = C_2$.

iii) For any field $F$, the subgroup $B$ of upper triangular matrices in $\mathrm{GL}_n(F)$ is solvable. For example if $n = 3$ one can take the series

$$1 < \begin{bmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \lhd \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix} \lhd \begin{bmatrix} \times & * & * \\ 0 & \times & * \\ 0 & 0 & \times \end{bmatrix} = G,$$

with the obvious generalization to arbitrary $n$.

iv) Any group $G$ of order $pq$, where $p$ and $q$ are primes, is solvable. For if $p \leq q$ then $G$ has a normal subgroup $C_q$ with quotient $C_p$. More generally, any group whose order is divisible by at most two primes is solvable. This is Burnside's $p^a q^b$ theorem, whose original proof uses character theory and still appears to be the most accessible proof to non-experts.

v) A group $G$ is solvable if and only if it has the *factorization property*: If $|G| = m \cdot n$ for relatively prime integers $m, n$, then $G = MN$ for subgroups $M, N$ of $G$ of orders $m, n$. This is P. Hall's generalization of Burnside's theorem.

vi) Any finite group of odd order is solvable. This is the famous Feit-Thompson theorem from 1963, whose proof is much more difficult than the previous two theorems.

vii) Let $f(x)$ be a polynomial with rational coefficients having $n$ distinct roots. The *Galois group* $G_f$ is the subgroup of $S_n$ consisting of those permutations of the roots which preserve all polynomial relations among them. The group $G_f$ is solvable precisely when the roots of $f$ can be expressed in terms of rational and radical expressions in the coefficients of $f$, as in the quadratic, cubic or quartic formulas. This was discovered by E. Galois, and is the origin of the term "solvable". It explains why there is no general formula for a quintic polynomial: $S_5$ is not solvable.

viii) Same situation, where now the coefficients of $f$ lie in the field $\mathbb{Q}_p$ of $p$-adic numbers for some prime $p$. Then $G_f$ is always solvable. In fact, $G$ has a canonical chain of subgroups $G_1 \lhd G_0 \lhd G$, where $G_1$ is a $p$-group and $G_0/G_1$, $G/G_0$ are both cyclic.

Solvable groups occur naturally in many areas of mathematics. Being opposite to nonabelian simple groups, they are a very natural class of groups to study. However, some of the most interesting theorems about solvable groups are very difficult to prove. For example, the proof of the Feit-Thompson theorem takes 255 pages.

Among the solvable groups are the *nilpotent* groups, for which the first few interesting theorems are easy, including a version of Hall's theorem above.

The definition is as follows. For any group $G$, the **ascending central series** [13] of $G$ is the chain of subgroups of $G$:

$$Z_1 \trianglelefteq Z_2 \trianglelefteq Z_3 \trianglelefteq \cdots \tag{43}$$

defined inductively as follows: $Z_1 = Z(G)$ is the center of $G$, and given $Z_i$, define $Z_{i+1}$ to be the unique subgroup containing $Z_i$ such that $Z_{i+1}/Z_i = Z(G/Z_i)$ is the center of $G/Z_i$. We say $G$ is **nilpotent** if $Z_c = G$ for some $c \geq 1$. The minimal such $c$ is the **nilpotence class** of $G$.

[13] Also called the "upper central series".

A nontrivial nilpotent group must have nontrivial center, lest all $Z_i = 1$. If $G$ is nilpotent of class $c$ then $G/Z(G)$ has class $c-1$.

If $G$ is nilpotent and $H \triangleleft G$ then $H$ and $G/H$ are nilpotent, *but not conversely*: The symmetric group $S_3$ has trivial center, so its ascending central series has $Z_i = 1$ for all $i$. Hence $S_3$ is not nilpotent. However, its subgroup $A_3$ and quotient $S_3/A_3 = C_2$ are both nilpotent.

Direct products of nilpotent groups are nilpotent. So any direct product of $p$-groups is nilpotent. We will see that all nilpotent groups are of this form.

**Examples of Nilpotent Groups:**

i) The abelian groups are the nilpotent groups of class 1. The nilpotent groups $G$ of class 2 are those for which $G/Z(G)$ is abelian.

ii) Any finite $p$-group is nilpotent, because any $p$-group has nontrivial center, hence $Z_i \neq Z_{i+1}$, so eventually $Z_i$ has the same order as $G$. If $|G| = p^k$ then the nilpotence class of $G$ is at most $k-1$, since every group of order $p^2$ is abelian.

iii) The dihedral group $D_n$ is nilpotent if and only if $n$ is a power of 2 (use 5. in Thm. 11.1 below). If $n = 2^\ell$ and $r = st$ is the product of two generating reflections $s$ and $t$, then $r$ has order $2^\ell$ and $Z_i$ is cyclic, generated by $r^{2^{\ell-i}}$. As $D_{2^\ell}/\langle r^2\rangle \simeq C_2 \times C_2$ is abelian, it follows that $D_{2^\ell}$ has nilpotence class equal to $\ell$, the maximum possible for a group of order $2^{\ell+1}$. There are exactly two other families of groups of order $2^{\ell+1}$ having maximal nilpotence class: the generalized quaternion group $Q_{2^{\ell+1}}$ and the quasidihedral group $QD_{2^{\ell+1}}$.

iv) For any field $F$, the subgroup $U_n$ of strictly upper triangular matrices in $\mathrm{GL}_n(F)$ is nilpotent of class $n-1$. For example if $n = 4$ the ascending central series is

$$\begin{bmatrix} 1 & 0 & 0 & * \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} < \begin{bmatrix} 1 & 0 & * & * \\ 0 & 1 & 0 & * \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} < \begin{bmatrix} 1 & * & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & 1 \end{bmatrix} = G,$$

with the obvious generalization to arbitrary $n$. The matrices in $U_n$ are of the form $I + A$, where $A^n = 0$. This may be the origin of the term "nilpotent".

The main theorem on finite nilpotent groups is the following collection of characterizations.

**Theorem 11.1** *For a finite group $G$ the following are equivalent.*

1. *$G$ is nilpotent.*
2. *Any proper subgroup $H$ of $G$ is properly contained in its normalizer $N_G(H)$.*
3. *Every maximal subgroup of $G$ is normal in $G$.*
4. *Every Sylow $p$-subgroup of $G$ is normal in $G$.*

5. *$G$ is the direct product of its Sylow $p$-subgroups.*

6. *For every divisor $m$ of $|G|$ there is a normal subgroup $M \triangleleft G$ with $|M| = m$.*

**Proof:** $(1 \Rightarrow 2)$: By induction we assume the result for all groups of smaller order than $G$. Let $H$ be a proper subgroup of $G$. Since $G$ is nilpotent its center $Z$ is nontrivial and normalizes $H$. If $Z$ is not contained in $H$ then $H \neq HZ$, done. Assume $Z < H$. Let $\overline{G} = G/Z$, $\overline{H} = H/Z$ and let $\pi : G \to \overline{G}$ be the projection. Then $\overline{H}$ is a proper subgroup of $\overline{G}$, so by induction $\overline{H} \neq N_{\overline{G}}(\overline{H})$. One checks that

$$H = \pi^{-1}(\overline{H}) \qquad \text{and} \qquad N_G(H) = \pi^{-1}(N_{\overline{G}}(\overline{H})),$$

hence $H \neq N_G(H)$, by the Correspondence Theorem.

$(2 \Rightarrow 3)$: Apply 2 to a maximal proper subgroup of $G$.

$(3 \Rightarrow 4)$: Suppose the Sylow $p$-subgroup $P$ of $G$ is not normal. Then $N_G(P)$ is a proper subgroup of $G$, contained in a maximal proper subgroup $M$ of $G$ which is normal in $G$, by 3, and $P$ is a Sylow $p$-subgroup of $M$. For any $g \in G$, the conjugate $P^g$ is another Sylow $p$-subgroup of $M$, so $P^g = P^m$ for some $m \in M$. Then $g \in N_G(P)m \subset M$. [14] Since $g$ was arbitrary, we have shown that $G = M$, contradicting $M$ being proper.

$(4 \Rightarrow 5)$: Induct on the number of primes dividing $|G|$. Let $|G| = p_1^{r_1} \cdots p_n^{r^n}$. By 4, the Sylow $p_i$-subgroup $P_i$ is unique and any product of Sylow subgroups is a normal subgroup of $G$. In particular $H := P_1 \cdots P_{n_1}$ is normal in $G$. By induction $H = P_1 \times \cdots \times P_{n-1}$, so the primes dividing the orders of elements of $H$ are in $\{p_1, \ldots, p_{n-1}\}$. So $H \cap P_n = 1$ and $P_n$ is normal in $G$. Hence

$$G = H \times P_n = (P_1 \times \cdots \times P_{n-1}) \times P_n = P_1 \times \cdots \times P_n.$$

$(5 \Rightarrow 6)$: Let $|G| = p_1^{r_1} \cdots p_n^{r^n}$ as above. Then $m = p_1^{s_1} \cdots p_n^{s_n}$, for $s_i \leq r_i$. The $p$-group $P_i$ has a subgroup $Q_i$ of order $p^{s_i}$. By 5, the subgroup $M = Q_1 \times \cdots \times Q_n$ is a normal subgroup of $G$ with order $m$.

$(6 \Rightarrow 4)$: Take $m$ to be the full power of $p$ dividing $G$.

$(5 \Rightarrow 1)$: Each $p$-group is nilpotent and a direct product of nilpotent groups is nilpotent. ■

Part 5 of Thm. 11.1 implies that in a nilpotent group two elements of relatively prime orders commute. This explains why $D_n$ is not nilpotent for $n$ odd: there is a rotation of odd order inverted by a reflection.

An example of a nilpotent group which is not at first glance a direct product of $p$-groups is the cyclic group $C_n$, when $n$ has multiple prime divisors. If $n = p_1^{r_1} \cdots p_k^{r_k}$ for distinct primes $p_1, \ldots, p_k$ then

$$C_n = C_{p_1^{r_1}} \times \cdots \times C_{p^{r_k}}.$$

For a nonabelian example, let $R$ be any commutative ring and Define $U_3(R)$ to be the group

$$U_3(R) = \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix},$$

[14] This kind of transitivity proof is called the **Frattini Argument**. It is very similar to the proof of Lemma 10.11.

where the entries $*$ are arbitrary elements in $R$. Then $U_3(R)$ is nilpotent. If we take $R = \mathbb{Z}/n\mathbb{Z}$ then applying the Chinese Remainder theorem to each matrix entry gives an isomorphism

$$U_3(\mathbb{Z}/n\mathbb{Z}) \simeq U_3(\mathbb{Z}/p_1^{r_1}\mathbb{Z}) \times \cdots \times U_3(\mathbb{Z}/p_k^{r_k}\mathbb{Z}).$$

Nevertheless, Thm. 11.1 shows that the study finite nilpotent groups essentially reduces to $p$-groups.

# 12 $p$-groups, a second look

In this section $p$ is a prime.

Up to isomorphism, there is one group of order $p$, namely $C_p$. There are two groups of order $p^2$, namely $C_p \times C_p$, in which $x^p = 1$ for every element $x$, and $G \simeq C_{p^2}$, which contains an element of order $p^2$.

## 12.1 Groups of order $p^3$

Up to isomorphism there are three abelian groups of order $p^3$:

$$C_p \times C_p \times C_p, \qquad C_{p^2} \times C_p, \qquad C_{p^3}.$$

Assume from now on that $G$ is nonabelian with $|G| = p^3$ and let $Z = Z(G)$ be the center of $G$. As $G/Z$ cannot be cyclic, we have

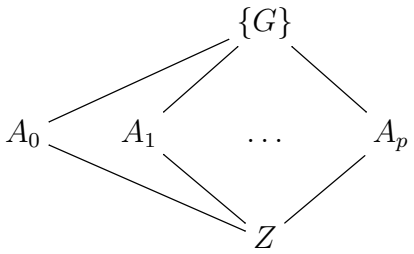
$$Z \simeq C_p, \qquad \text{and} \qquad G/Z \simeq C_p \times C_p.$$

The latter is abelian, so the commutator subgroup $[G, G]$ lies in $Z$. But $[G, G] \neq 1$ since $G$ is non-abelian, so in fact

$$[G, G] = Z.$$

Hence for any fixed $x \in G$ the commutator with $x$ gives a map $f : G \to Z$, sending $y \mapsto [y, x] = yxy^{-1}x^{-1}$. As $yxy^{-1} = [y, x]x$, it follows that the conjugacy class of $x \in G - Z$ is $xZ$. Hence $G$ has $p$ conjugacy classes inside $Z$ and $p^2 - 1$ conjugacy classes outside $Z$.

Any maximal subgroup $A \leq G$ has order $p^2$, is normal in $G$ and contains $Z = [G, G]$, since $G/A \simeq C_p$ is abelian. Hence the maximal subgroups of $G$ correspond to the subgroups of $G/Z \simeq C_p \times C_p$, which has $p + 1$ subgroups, corresponding to the points in the projective line over $\mathbb{Z}/p\mathbb{Z}$. The maximal subgroups $A_0,\ A_1, \ldots A_p$ form the part of the subgroup lattice of $G$ over $Z$.



The maximal subgroups $A_i$ may belong to different isomorphism classes, either $C_p \times C_p$ or $C_{p^2}$. If $p = 2$ then $D_4$ contains both kinds, while $Q_8$ contains $C_4$ but not $C_2 \times C_2$. We will see that the opposite holds for odd primes $p$.

First we need a commutator lemma:

**Lemma 12.1** *Let $G$ be a group, let $x, y \in G$, and let $[y, x] = yxy^{-1}x^{-1}$ be the commutator. Suppose $[y, x]$ commutes with $x$ and $y$. Then for all $n \in \mathbb{N}$ we have*

$$(xy)^n = x^n y^n [y, x]^{n(n-1)/2}.$$

**Proof:** We expand:

$$(xy)^n = (xy)(xy)\cdots(xy). \tag{44}$$

We want to put all the $y$'s to the right of all the $x$'s. The commutator is the price to pay for replacing $yx$ by $xy$:

$$yx = [y, x]xy,$$

which we can write as

$$yx = xy[y, x],$$

since $x, y$ commute with $[y, x]$. The left-most $y$ in (44) moves past $n - 1$ $x$'s, so contributes $[y, x]^{n-1}$. The new left-most $y$ then contributes $n - 2$ $x$'s, and so on. Thus, we get

$$(xy)^n = x^n y^n [y, x]^{(n-1)+(n-2)+\cdots+1} = x^n y^n [y, x]^{n(n-1)/2},$$

as claimed. ■

Next we need a lemma about $\mathrm{GL}_2(p)$.

**Lemma 12.2** *Any element of order $p$ in $\mathrm{GL}_2(p)$ is conjugate to $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.*

**Proof:** Let $g \in GL_2(p)$ have order $p$. By Sylow's theorem, $g$ is conjugate to an element $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$ of the Sylow $p$-subgroup $U = \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}$ of $\mathrm{GL}_2(p)$, with $b \neq 0$. Conjugating by $\begin{bmatrix} 1 & 0 \\ 0 & b \end{bmatrix}$, we arrive at $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

■

Now return to our group $G$ of order $p^3$, and assume $p > 2$. We have seen that all commutators lie in $Z$, so the conditions of Lemma 12.1 hold for any $x, y \in G$. Since $p$ is odd, it divides $p(p-1)/2$ and since $|Z| = p$ we have $[y, x]^{p(p-1)/2} = 1$. Hence for all $x, y \in G$ we have

$$(xy)^p = x^p y^p.$$

This means that the map $x \mapsto x^p$ is a group homomorphism; we it simply by $p : G \to G$. Clearly $Z \leq \ker p$. Since $G$ is not cyclic we have $x^{p^2} = 1$ for all $x \in G$, so $\operatorname{im} p \leq \ker p$. Now $Z$ cannot be the

whole of $\ker p$, lest $|\ker p| = p$ and $|\operatorname{im} p| = p^2$. Hence there is an element $y_0 \in \ker p$ outside $Z$. The subgroup $A = \langle y_0, z\rangle$ generated by $y_0$ and $z$ is then a normal subgroup of $G$ isomorphic to $C_p \times C_p$.

Now there are two cases.

Case 1: $\ker p = G$.

This means $g^p = 1$ for all $g \in G$. Choose any element $x \in G$ outside of $A$. Then $x$ acts on $A$ via an element of order $p$ in $\operatorname{Aut}(A) \simeq \mathrm{GL}_2(p)$. By Lemma 12.2 there are generators $y, z$ of $A$ such that

$$G = \langle x\rangle \ltimes A,$$

where $x$ acts on $A$ by

$$xzx^{-1} = z, \qquad xyx^{-1} = yz.$$

The structure of $G$ is thus determined uniquely. We have

$$G = \{z^c y^b x^a : \ a, b, c \in \mathbb{Z}/p\mathbb{Z}\}, \tag{45}$$

with multiplication

$$(z^c y^b x^a) \cdot (z^f y^e x^d) = z^{c+f+ae} y^{b+e} x^{a+d}.$$

The *Heisenberg group*

$$H := \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix} \tag{46}$$

is a nonabelian group of order $p^3$ and exponent $p$, is therefore isomorphic to the abstract group $G$ in (45). Indeed, one checks that sending

$$z^c y^b x^a \mapsto \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix}$$

is an explicit isomorphism $G \xrightarrow{\sim} H$.

Case 2: $\ker p \neq G$.

Here $G$ has an element $y$ of order $p^2$. Choose such a $y$ and let $Y = \langle y\rangle \simeq C_{p^2}$. Choose any $x_0$ in $A$ but not in $Y$. Then $G$ is again a semidirect product:

$$G = \langle x_0\rangle \ltimes Y,$$

with some action of $x_0$ on $Y$. Let $R$ be the ring $\mathbb{Z}/p^2\mathbb{Z}$. Then

$$R^\times \simeq \operatorname{Aut}(Y),$$

where $r \in R$ corresponds to the automorphism $y \mapsto y^r$. The elements of order $p$ in $R$ lie in $1 + pR$, so $x_0 y x_0^{-1} = y^{1+rp}$ for some $r \in R$. Let $s$ be the inverse of $r$ in $R$ and let $x = x_0^s$. Then $xyx^{-1} = y^{1+p}$, which determines the group structure on $G$. We have

$$G = \{y^b x^k : \ b \in R, \ k \in \mathbb{Z}/p\},$$

and the map sending

$$y^b x^k \mapsto \begin{bmatrix} (1+p)^k & b \\ 0 & 1 \end{bmatrix}$$

is an isomorphism from $G$ to the group of matrices

$$\left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : \ a \in 1 + pR, \ b \in R \right\}. \tag{47}$$

### 12.1.1 Automorphisms of the Heisenberg group

Let $p > 2$ and let $H$ be the Heisenberg group (46), with center

$$Z := \begin{bmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The automorphism group $\mathrm{Aut}(H)$ preserves $Z$ and therefore acts on $H/Z \simeq (\mathbb{Z}/p\mathbb{Z})^2$. Thus we get a map

$$\mathrm{Aut}(H) \longrightarrow \mathrm{Aut}(H/Z) \simeq \mathrm{GL}_2(p).$$

**Proposition 12.3** *This mapping fits into a split exact sequence*

$$1 \longrightarrow H/Z \longrightarrow \mathrm{Aut}(H) \longrightarrow \mathrm{Aut}(H/Z) \longrightarrow 1$$

*and* $\mathrm{Aut}(H) \simeq (\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathrm{GL}_2(p)$ *is the affine group of the plane over* $\mathbb{Z}/p\mathbb{Z}$.

**Proof:** Let

$$x = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad y = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \qquad z = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Then

$$z^c y^b x^a = \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix},$$

and $H$ has the presentation

$$H = \langle x, y, z |\ x^p = y^p = 1, \ [x, y] = z, \ xz = zx, \ yz = zy \rangle.$$

From this (or matrix multiplication) we derive the formulas

$$(z^c y^b x^a)(z^{c'} y^{b'} x^{a'}) = z^{ab' + c + c'} y^{b + b'} x^{a + a'},$$

$$(z^c y^b z^a)^{-1} = z^{ab - c} y^{-b} x^{-a},$$

$$[z^c y^b x^a, z^{c'} y^{b'} x^{a'}] = z^{ab'-ba'}.$$

The isomorphism $H/Z \simeq (\mathbb{Z}/p\mathbb{Z})^2$, sends (the coset mod $Z$ of) $z^c y^b x^a \mapsto (a, b)$. We now prove exactness of the sequence

$$1 \longrightarrow H/Z \xrightarrow{\iota} \mathrm{Aut}(H) \longrightarrow \mathrm{Aut}(H/Z) \longrightarrow 1, \tag{48}$$

where $\iota : h \mapsto \iota_h \in \mathrm{Aut}(H)$, with $\iota_h(h') = hh'h^{-1}$, is the action of $H$ on itself by inner automorphisms. Since $H/Z$ is abelian, $\iota_h$ induces the trivial automorphism on $H/Z$. Conversely, suppose $\sigma \in \mathrm{Aut}(H)$ is trivial on $H/Z$. Then there are $c, c' \in \mathbb{F}_p$ such that

$$\sigma(x) = z^c x, \qquad \sigma(y) = z^{c'} y.$$

Let $h = y^{-c} x^{c'}$. One checks that $\iota_h(x) = z^c x, \iota_h(y) = z^{c'} y$, so $\sigma = \iota_h$. Hence the sequence (48) is exact in the middle.

We next prove that $\mathrm{Aut}(H) \to \mathrm{Aut}(H/Z) = \mathrm{GL}_2(p)$ is surjective. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(p)$. The above commutation formula shows that

$$[y^b x^a, y^d x^c] = z^{\det(A)}.$$

Since every non-identity element has order $p$ (here we are using $p > 2$), the elements $y^b x^a,\ y^d x^c,\ z^{\det A}$ satisfy the relations of $x, y, z$. Hence there is a homomorphism $\alpha : H \to H$ such that

$$x^\alpha = y^b x^a, \qquad y^\alpha = y^d x^c, \qquad z^\alpha = z^{\det A}.$$

We must show that $\alpha$ is injective (hence is bijective). Since $\det A$ is invertible in $\mathbb{F}_p$, $\ker \alpha \cap Z = 1$. Hence $\ker \alpha$ injects into the kernel of $A$ in $G/Z$, which is trivial. This finishes the proof of exactness in (48).

However, the function $A \to \alpha$ just described is only a set-theoretic splitting; it is not a group homomorphism. In fact we could modify the definitions of $x^\alpha$ and $y^\alpha$ by multiplying by arbitrary elements of $Z$ and the relations of $H$ would still be satisfied. It turns out we can make such a modification to get a group-theoretic splitting, namely if we redefine $\alpha$ to be

$$x^\alpha = z^{ab/2} y^b x^a, \qquad y^\alpha = z^{cd/2} y^d x^c, \qquad z^\alpha = z^{ad-bc} \tag{49}$$

(note that $ab/2, cd/2$ are taken in $\mathbb{Z}/p\mathbb{Z}$, where 2 invertible) then if $A, B \in \mathrm{GL}_2(p)$ correspond to $\alpha, \beta$ via (49), one can check that

$$(x^\alpha)^\beta = x^{\alpha\beta}, \qquad (y^\alpha)^\beta = y^{\alpha\beta},$$

so that the new map $A \to \alpha$ is a group homomorphism, where $\mathrm{Aut}(H)$ acts via the right on $H$.

There is one more detail to check, that the action of $\mathrm{Aut}(H/Z)$ on $H/Z$ in the semidirect product arising from the splitting just described coincides with the action (by right multiplication) of $\mathrm{GL}_2(p)$ on $(\mathbb{Z}/p\mathbb{Z})^2$. We leave this as an exercise. ■

## 12.2 Higher powers of $p$

Let $N(p^r)$ be the number of isomorphism classes of groups of order $p^r$. We have found

| $r$ | $N(p^r)$ | groups |
|---|---|---|
| 1 | 1 | $C_p$ |
| 2 | 2 | $C_p \times C_p,\ C_{p^2}$ |
| 3 | 5 | $C_p^3,\ C_{p^2} \times C_p,\ C_{p^3},\ U_3(p),$ (47) |

The case of $p^3$ relied in a straightforward way on the classification for $p^2$. One might imagine that all $p$-groups could be classified inductively in a similar way. The case of $p^4$ is much harder, but still accessible to non-experts, at least for $p = 2$.

We give here the classification of groups of order 16 [15]. There are 14 groups of order 16:

- five abelian groups: $C_2^4,\ C_4 \times C_2^2,\ C_4 \times C_4,\ C_8 \times C_2,\ C_{16}$;
- two direct products: $D_4 \times C_2, Q_8 \times C_2$.
- the dihedral group $D_8 = C_8 \overset{-1}{\rtimes} C_2$ [16]
- the quasidihedral group $QD_{16} = C_8 \overset{3}{\rtimes} C_2$;
- another semidirect product $C_8 \overset{5}{\rtimes} C_2$;
- the unique nonabelian semidirect product $C_4 \rtimes C_4$;
- the unique nonabelian semidirect product $(C_2 \times C_2) \rtimes C_4$;
- the unique nontrivial semidirect product $Q_8 \rtimes C_2$;
- the generalized quaternion group $Q_{16}$;

Of these groups only $D_8, QD_{16}$ and $Q_{16}$ have maximal class 3; these groups have centers of order two, and their quotients by their centers are $D_4$. We will return to this.

It was also known in the $19^{th}$ century that for $p > 2$ there are 15 groups of order $p^4$.

So far, it seems the number of $p$-groups of a given order does not depend much on $p$. However, in the last decade it has been found [17] that

$$N(p^5) = \begin{cases} 2p + 61 + 2(3, p-1) + (4, p-1) & \text{if } p > 3 \\ 67 & \text{if } p = 3 \\ 51 & \text{if } p = 2, \end{cases}$$

[15] For a proof, see *The groups of order sixteen made easy*, Marcel Wild, Bulletin of the A.M.S. 2005.

[16] The notation $C_n \overset{k}{\rtimes} C_m$ means the generator of $C_m$ acts by the $k^{th}$ power on $C_n$.

[17] See the talk by B. Eick "The classification of $p$-groups by coclass", http://homeweb1.unifr.ch/ciobanul/pub/beamer.pdf.

and

$$N(p^6) = \begin{cases} 3p^2 + 39p + 344 + 24(3, p-1) + 11(4, p-1) + 2(5, p-1) & \text{if } p > 3 \\ 504 & \text{if } p = 3 \\ 267 & \text{if } p = 2. \end{cases}$$

We also have mentioned that

$$N(2^{10}) = 49\ 487\ 365\ 422.$$

It seems hopeless to classify $p$-groups whose order is a given power of $p$, but the fact that these remarkable values of $N(p^r)$ have recently been found indicates great progress in the classification of $p$-groups.

A big breakthrough came when people looked at groups of maximal nilpotence class, and found trees of infinite families of groups.

## 12.3 Projective limits and pro-$p$ groups

Suppose we have a sequence of groups (or rings) $X_n$, indexed by positive integers $n$, along with homomorphisms $f_n : X_n \to X_{n-1}$ for each $n \geq 2$. Thus we have an infinite sequence of groups (or rings) and maps:

$$\cdots \longrightarrow X_n \xrightarrow{f_n} X_{n-1} \longrightarrow \cdots \longrightarrow X_3 \xrightarrow{f_3} X_2 \xrightarrow{f_2} X_1.$$

The **projective limit** of the system $(X_n, f_n)$ [18] is the set of sequences

$$\varprojlim_n X_n := \{(x_1, x_2, \dots) : \ x_n \in X_n, \ f(x_n) = x_{n-1} \quad \forall n \geq 2\},$$

under componentwise group (or ring) operations.

The projective limit $X = \varprojlim_n X_n$ comes with a system of canonical projection maps

$$\pi_n : X \longrightarrow X_n, \qquad \pi_n(x) = x_n.$$

The quotients $X_n$ may be regarded as successive approximations to, or shadows of the single group $X$.

If all the $X_n$ are finite groups, the projective limit $X$ is called **pro-finite**. If $p$ is a prime and all the $X_n$ are $p$-groups, then $X$ is called a **pro-$p$** group. The single group $X$ describes an infinite family $\{X_n\}$ of finite $p$-groups.

The simplest example is when $X_n = \mathbb{Z}/p^n\mathbb{Z}$ and $f_n$ is the natural projection

$$f_n : \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z}.$$

With these maps, the inverse limit

$$\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

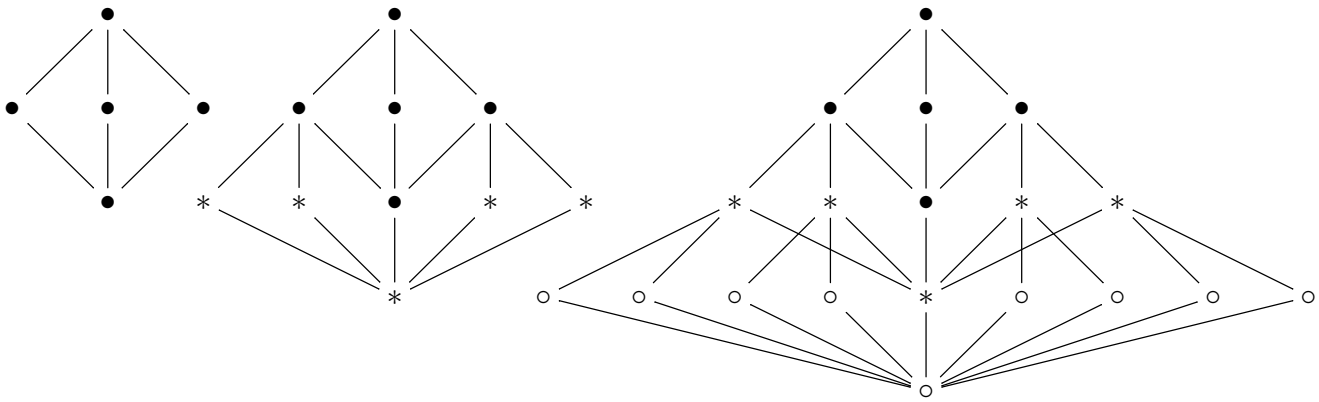
[18] This is also called the **inverse limit**.

is the **ring of $p$-adic integers**, whose additive group is a pro-$p$ group.

For a non-abelian example, let $X_n = D_{2^n}$ be the dihedral group of order $2^{n+1}$. Since the quotient of $D_{2^n}$ by its center is $D_{2^{n-1}}$, we have quotient maps $f_n : X_n \to X_{n-1}$. The successive shadows $D_2, D_4, D_8$ of the 2-adic dihedral group

$$D := \varprojlim_n D_{2^n}$$

can be seen in the sequence of subgroup lattices



If $(X_n, f_n)$ and $(Y_n, g_n)$ are two projective systems, and we have for each $n$ a homomorphism

$$h_n : X_n \longrightarrow Y_n$$

such that $h_{n-1} \circ f_n = g_n \circ h_n$ then we get a homomorphism

$$h : \varprojlim_n X_n \longrightarrow \varprojlim_n Y_n, \qquad (x_n) \mapsto (h(x_n)).$$

Let $Y_n = \{z \in \mathbb{C}^\times : \ z^{2^n} = 1\}$ with maps $g_n(z) = z^2$. Let $h_n : \mathbb{Z}/2^n\mathbb{Z} \to Y_n$ be the isomorphism

$$h_n([x]) = \exp(2\pi i/2^n).$$

Then we have an isomorphism

$$h : \mathbb{Z}_2 \xrightarrow{\sim} Y := \varprojlim_n Y_n$$

such that multiplication by $-1$ on $\mathbb{Z}_2$ corresponds to inversion on $Y$. It follows that the 2-adic dihedral group is a semidirect product

$$D = \mathbb{Z}_2 \rtimes C_2,$$

where the nontrivial element of $C_2$ acts on $\mathbb{Z}_2$ by negation.

## 12.4 Toward the classification of $p$-groups

Let $G$ have order $p^{n+1}$ and maximal nilpotence class $n$. The ascending central series for $G$ must have the form

$$Z_1 < Z_2 < \cdots < Z_{n-1} < Z_n = G,$$

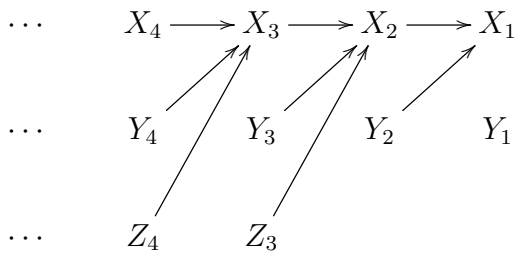
where $|Z_i| = p^i$ for $i < n$. In particular the center $Z_1 = Z(G)$ has order $p$. The group $H = G/Z(G)$ has order $p^n$ and nilpotence class $n-1$, which is again maximal. We indicate this relation between $G$ and $H$ by an arrow $G \to H$.

Let $\mathcal{G}(p,1)$ be the directed graph whose vertices are the isomorphism classes of finite $p$-groups of maximal nilpotence class, having edges $G \to H$ when $G/Z(G) \simeq H$, as above.

We will draw this graph for $p = 2$. Let

$$X_n = D_{2^n}, \qquad Y_n = Q_{2^{n+1}}, \qquad Z_n = QD_{2^{n+1}}$$

be the dihedral, generalized quaternion and quasidihedral groups of order $2^{n+1}$. For small $n$ we have $X_1 = C_2^2$, $Y_1 = C_4$ and $Z_2 = Y_2 = Q_8$. Since the quotient of each of $X_n, Y_n, Z_n$ by its center is $X_{n-1}$, the graph $\mathcal{G}(2,1)$ is




This graph is a tree with exactly one infinite path, over which the projective limit is the 2-adic dihedral group $D$. The other groups are contained in *branches* $\mathcal{B}_{n,k}$ consisting of all groups to the left of and distance at most $k$ from $X_n$. The groups in $\mathcal{G}(2,1)$ have different orders and nilpotence class, but they all have the same **coclass**: If $G$ has order $p^r$ and nilpotence class $c$ then its coclass is defined to be $r-c$.

For any prime $p$ and integer $c \geq 1$ one can define a coclass graph $\mathcal{G}(p,c)$ whose vertices are all the $p$-groups of coclass $c$ with an edge between $G$ and $H$ if there exists $N \trianglelefteq G$ with $G/N \simeq H$. The $p$-groups of a given coclass $c$ are then classified, at least qualitatively, via the structure of the graph $\mathcal{G}(p,c)$, about which the following is known.

1. There are only finitely many infinite paths in $\mathcal{G}(p,c)$.
2. The projective limit over each infinite path in $\mathcal{G}(p,c)$ is an infinite pro-$p$ group whose finite quotients all have coclass $c$.
3. Every infinite pro-$p$ group with all quotients of coclass $c$ arises from an infinite path in $\mathcal{G}(p,c)$.
4. The groups in $\mathcal{G}(p,c)$ lie on branches, and these eventually become periodic.

For more details, see the talks online by Bettina Eick and her collaborators, along with the book *The structure of groups of prime-power order* by Leedham-Green and McKay, two of the pioneers in this new era of group theory.

# 13 Presentations of Groups

It is often convenient to represent group elements as "words" in a few symbols, having certain relations. For example, the cyclic group $C_n$ can be expressed as

$$C_n = \langle a \mid a^n = 1 \rangle,$$

which is called a **presentation** of $C_n$. Here there is only one generator $a$, and one relation $a^n = 1$.

Now suppose $G$ is a group generated by two elements $a, b$ of order two. Let $C = \langle ab \rangle$ be the subgroup of $G$ generated by $ab$. Since $a$ and $b$ have order two, we have $a(ab)a = ba = (ab)^{-1}$, and one checks that every element of $G$ can be written either as $(ab)^i$ or $a(ab)^i$ for some $i \in \mathbb{Z}$. Thus, $C$ has index two in $G$ and we have

$$G = C \cup aC.$$

The multiplication in $G$ is then completely determined by the order of $C$. If $C$ is infinite, then we can describe $G$ via the presentations

$$G = \langle a, b \mid a^2 = b^2 = 1 \rangle. \tag{50}$$

If $|C| = n < \infty$, we have an additional relation $(ab)^n = 1$, so we write

$$G = \langle a, b \mid a^2 = b^2 = (ab)^n = 1 \rangle. \tag{51}$$

These groups $G$ are isomorphic to the dihedral groups $D_\infty$ and $D_n$, respectively, where $a$ and $b$ manifest as reflections about adjacent lines. However, the presentations (50) and (51) express $G$ independently of any manifestation. This allows us to identify $G$ in other settings, wherever we find a group generated by two elements of order two.

So we would like to view groups as generated by abstract symbols like $a, b, c, \ldots$ with certain relations among the symbols such that every possible relation in the group is completely determined by the given relations. To explain this precisely, we start with free groups, which are groups with no relations at all.

## 13.1 Free Groups

Let $S$ be a set. The **Free Group** on $S$ is the set $F(S)$ consisting of an element $e$, and all formal expressions $s_1^{n_1} s_2^{n_2} \cdots s_\ell^{n_\ell}$ where $\ell \geq 1$, the $n_i$ are nonzero integers, and $s_1, \ldots, s_\ell$ are elements of $S$ such that $s_i \neq s_j$ if $|i - j| = 1$. We multiply two such expressions according to the following rules.

- $e$ is the identity element of $F(S)$.
- For all $s \in S$ we have $s^n \cdot s^m = s^{n+m}$ if $n + m \neq 0$ and $s^n \cdot s^{-n} = e$.

- For distinct $s, t \in S$ we have $s^n \cdot t^m = s^n t^m$.
- Inductively, we have

$$(s_1^{n_1} s_2^{n_2} \cdots s_\ell^{n_\ell}) \cdot (t_1^{m_1} t_2^{m_2} \cdots t_k^{m_k}) = \begin{cases} s_1^{n_1} s_2^{n_2} \cdots s_\ell^{n_\ell} t_1^{m_1} t_2^{m_2} \cdots t_k^{m_k} & \text{if} \quad s_\ell \neq t_1 \\ s_1^{n_1} s_2^{n_2} \cdots s_\ell^{n_\ell + m_1} t_2^{m_2} \cdots t_k^{m_k} & \text{if} \quad s_\ell = t_1 \text{ and } n_\ell + m_1 \neq 0 \\ (s_1^{n_1} s_2^{n_2} \cdots s_{\ell-1}^{n_{\ell-1}}) \cdot (t_2^{m_2} \cdots t_k^{m_k}) & \text{if} \quad s_\ell = t_1 \text{ and } n_\ell + m_1 = 0 \end{cases}$$

**Proposition 13.1** *Let $f : S \to G$ be a map from a set $S$ to a group $G$. Then there is a unique extension of $f$ to a group homomorphism $\tilde{f} : F(S) \to G$.*

**Proof:** We define $\tilde{f}(e) = 1$ and

$$\tilde{f}(s_1^{n_1} s_2^{n_2} \cdots s_\ell^{n_\ell}) = f(s_1)^{n_1} f(s_2)^{n_2} \cdots f(s_\ell)^{n_\ell}.$$

This is a group homomorphism because the multiplication in $G$ obeys the same rules as those above for $F(S)$, with $s_i$ and $t_i$ replaced by $f(s_i)$ and $f(t_i)$.

If $f'$ is another extension of $f$ then for all $s \in S$ and integers $n > 0$ we have

$$f'(s^n) = f'(\underbrace{s \cdots s}_{n \text{ terms}}) = \underbrace{f'(s) \cdots f'(s)}_{n \text{ terms}} = f'(s)^n = f(s)^n = \tilde{f}(s)^n,$$

while if $n < 0$ we have $s^n = (s^{-n})^{-1}$, so by what we just proved, we have

$$f'(s^n) = f'((s^{-n})^{-1}) = f'(s^{-n})^{-1} = \tilde{f}(s^{-n})^{-1} = \tilde{f}((s^{-n})^{-1}) = \tilde{f}(s^n).$$

Finally, let $s_1, \ldots s_\ell \in S$ and take nonzero integers $n_1, \ldots n_\ell$. Multiplying in $F(S)$ we have

$$s_1^{n_1} s_2^{n_2} \cdots s_\ell^{n_\ell} = (s_1^{n_1}) \cdot (s_2^{n_2}) \cdots (s_\ell^{n_\ell}),$$

so

$$f'(s_1^{n_1} s_2^{n_2} \cdots s_\ell^{n_\ell}) = f'(s_1^{n_1}) \cdot f'(s_2^{n_2}) \cdots f'(s_\ell^{n_\ell}) = \tilde{f}(s_1^{n_1}) \cdot \tilde{f}(s_2^{n_2}) \cdots \tilde{f}(s_\ell^{n_\ell}) = \tilde{f}(s_1^{n_1} s_2^{n_2} \cdots s_\ell^{n_\ell}),$$

and therefore $f' = \tilde{f}$. Hence $\tilde{f}$ is the unique extension of $f$ to a homomorphism from $F(S)$ to $G$. ■

**Corollary 13.2** *If $S$ and $T$ are sets and $f : S \to T$ is a function, then $f$ extends uniquely to a group homomorphism $\tilde{f} : F(S) \to F(T)$.*

**Proof:** By Prop. 13.1 the composite map $\iota : S \to T \to F(T)$ extends uniquely to a homomorphism $\tilde{\iota} : F(S) \to F(T)$. ■

**Corollary 13.3** *If $S$ and $T$ are sets of the same cardinality and $f : S \xrightarrow{\sim} T$ is a bijection then $f$ extends uniquely to a group isomorphism $\tilde{f} : F(S) \xrightarrow{\sim} F(T)$.*

Consequently, for each positive integer $n$ there is a unique (up to isomorphism) free group on $n$ generators. We often denote this group by $F_n$.

Free groups abound in topology. Here are several related examples.

**Example 1:** If $n = 1$ then $F_1 \simeq \mathbb{Z}$. This is the fundamental group $\pi_1(C)$ of a circle $C$.

**Example 2:** Suppose $|S| = 2$, say $S = \{s_1, s_2\}$. We can visualize $F(S) = F_2$ as the fundamental group of the space $X$ consisting of two circles $C_1$ and $C_2$ touching at a point $p$ . Here $s_i$ is the counterclockwise (say) loop once around $C_i$ starting at $p$, while $s_i^{-1}$ loops around $C_i$ in the opposite direction. A word like $s_1^3 s_2^{-2} s_1$ is a loop going three counterclockwise times around $C_1$ then two clockwise times around $C_2$, then once counterclockwise time around $C_1$. The generalization to a bouquet of $n$ circles all touching at a single point is the obvious one.

**Example 3:** Let $X$ be a two-sphere punctured at $n + 1$ points. Then $X$ retracts onto a bouquet of $n$ circles, so $\pi_1(X) \simeq F_n$. More generally, let $X$ be a closed orientable surface of genus $g$, punctured at $n + 1$ points. Then $\pi_1(X) \simeq F_{2g+n}$.

**Example 4:** Let $G$ be a subgroup of $SL_2(\mathbb{Z})$ of finite index such $G$ has no elements of finite order, other than 1. Then $G$ acts on the upper-half plane $\mathcal{H} = \{z \in \mathbb{Z} : \Im z > 0\}$ by linear fractional transformations:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z = \frac{az + b}{cz + d}.$$

The quotient $X = \mathcal{H}/G$ is a finitely punctured Riemann Surface with $\pi_1(X) \simeq G$. Therefore $\Gamma$ is free.

**Example 5:** A **tree** is a contractible one dimensional simplicial complex (informally, a graph without loops). Any group acting freely on a tree is free.

**Example 6:** Any subgroup of a free group is free. The proof may be sketched thus: Given a free group $F$, one constructs a tree $T_F$ on which $F$ acts freely. Then any subgroup $F' < F$ also acts freely on $T_F$, hence $F'$ is free as well.

## 13.2 Generators and Relations

Let $S$ be a set, and let $R$ be a subset of $F(S)$. Let $N(R)$ be the smallest normal subgroup of $F(S)$ containing $R$. More precisely, $N(R)$ is the intersection of all normal subgroups of $F(S)$ containing $R$. We define a group

$$\langle S \mid R \rangle := F(S)/N(R).$$

This is the largest group with generators $S$ and relations $R$, in the following sense.

Let $G$ be any group and let $S$ be a subset of $G$. By Prop. 13.1, the inclusion map $\iota : S \to G$ extends uniquely to a group homomorphism

$$\tilde{\iota} : F(S) \longrightarrow G.$$

**Proposition 13.4 (Mapping Property)** *Let $R \subset F(S)$ be a subset contained in $\ker \tilde{\iota}$ and let $\pi : F(S) \to \langle S \mid R \rangle$ be the quotient map. Then there is a unique homomorphism $\phi_{S,R} : \langle S \mid R \rangle \to G$ such that $\phi_{S,R} \circ \pi = \tilde{\iota}$.*

**Proof:** By assumption, the elements of $R$ in $F(S)$ belong to the kernel of $\tilde{\iota}$. Hence $N(R) \leq \ker \tilde{\iota}$, so $\tilde{\iota}$ induces a homomorphism $\langle S \mid R \rangle \to G$, which is the desired map $\phi_{S,R}$. ■

Usually we take $S$ to be a generating set for $G$, in which case the map $\phi_{S,R}$ in Prop. 13.4 is surjective. If $\phi_{S,R}$ is an isomorphism, we say that $\langle S \mid R \rangle$ is a **presentation** of $G$, or more informally, that $G$ is "generated by $S$ with the relations $R$". Given a group $G$ with generators $S$, there is always some subset $R \subset F(S)$ such that $\phi_{S,R}$ is an isomorphism. For example, we could take $R$ to be the full kernel of $\tilde{\iota}$. In practice, we would like $S$ and $R$ to be small and simple. However, it has been proved that there is no algorithm that decides, for a given group $G$ with generating set $S$ and relations $R$, whether or not $\phi_{S,R}$ is an isomorphism. Indeed this is so even for $G = \{1\}$! It takes a combination of work, skill and luck to find a presentation for a given group $G$, but once found, a presentation can be very useful.

**Example 1:** For $1 \leq n < \infty$, the dihedral group $D_n$ has presentation with generating set $S = \{a, b\}$ and relations $R = \{a^2,\ b^n,\ abab\}$. We usually write $R$ in terms of equations that hold in the group, as follows:

$$D_n = \langle a, b \mid a^2 = b^n = 1,\ aba = b^{-1} \rangle. \tag{52}$$

To prove that (52) is correct, let $\Gamma = \langle a, b \mid a^2 = b^n = 1,\ aba = b^{-1} \rangle$. Let $r \in D_n$ be a reflection and let $t \in D_n$ be a rotation of order $n$. Then $rtr = t^{-1}$. Hence by the mapping property, we have a surjective homomorphism $\phi : \Gamma \twoheadrightarrow D_n$ such that $\phi(a) = r$ and $\phi(b) = t$. This is always the easy step towards verifying a presentation. The tricky part is to prove that $\phi$ is injective. In this case, we note that the relations in $\Gamma$ allow us to write every element in the form $b^i$ or $ab^i$, [19] with $1 \leq i \leq n$. This shows that $|\Gamma| \leq 2n = |D_n|$, so $\phi$ is injective and (52) is proved.

The same presentation works for $D_\infty$; we just drop the relation $b^n = 1$:

$$D_\infty = \langle a, b \mid a^2 = 1,\ aba = b^{-1} \rangle. \tag{53}$$

To prove this we again let $\Gamma = \langle a, b \mid a^2 = 1,\ aba = b^{-1} \rangle$. Let $r, r'$ be reflections about adjacent parallel lines $\ell, \ell'$ in the plane, so that $t := rr'$ is the translation by twice the distance from $\ell$ to $\ell'$. Then $rtr = t^{-1}$, so we have a surjection $\phi : \Gamma \twoheadrightarrow D_\infty$ such that $\phi(a) = r$ and $\phi(b) = t$. Now $\Gamma$ and $D_\infty$ are infinite groups, so we cannot count orders as we did previously. But every element of $\Gamma$ can still be expressed in the form $b^i$ or $ab^i$ for some $i \in \mathbb{Z}$, and since $t^i \neq 1 \neq rt^i$ in $D_\infty$, it follows that $\phi$ is injective.

## 13.3 A presentation of the symmetric group

A presentation for a given finite group $G$ can often be found as follows. We first find a set $S$ of generators of $G$, and some relations $R$ among the generators that appear to determine all the relations in $G$. Let $\Gamma = \langle S \mid R \rangle$. We then have a surjection $\phi : \Gamma \twoheadrightarrow G$. To prove that $\phi$ is an isomorphism

[19] Strictly speaking, we should write something like $\bar{b}^i$ and $\bar{a}\bar{b}^i$, where $\bar{a}$ and $\bar{b}$ are the images of $a$ and $b$ in $\Gamma$.

we try to show that $|\Gamma| \leq |G|$. Suppose we find a subgroup $H \leq \Gamma$ whose order is known, say by induction. It then suffices to show that $|\Gamma/H| \leq |G|/|H|$. This will succeed if we can find a set $X = \{aH, bH, \dots\} \subset \Gamma/H$, such that $|X| \leq |G|/|H|$ and such that $sX = X$ for every $s \in S$.

We illustrate with the group $G = S_{n+1}$.

**Lemma 13.5** *The group $S_{n+1}$ is generated by $\{s_1, \dots, s_n\}$, where $s_i = (i\ i+1)$.*

**Proof:** We use induction on $n$. For $n = 1$ we have $S_2 = \{e,\ (1\ 2)\} = \langle s_1 \rangle$, so the result holds in this case. Assume that $S_n$ is generated by $\{s_1, \dots, s_{n-1}\}$, and let $G = \langle s_1, \dots, s_n \rangle = \langle S_n,\ s_n \rangle$. Let $\tau \in S_{n+1}$ be arbitrary, and set $k = \tau(n+1)$. The 2-cycle

$$s_k s_{k+1} \cdots s_{n-1} s_n s_{n-1} \cdots s_{k+1} s_k = (k\ n+1)$$

belongs to $G$, and $(k\ n+1)\tau$ fixes $n+1$. Since $S_n$ is the stabilizer of $n+1$ in $S_{n+1}$, and $S_n \leq G$, it follows that $(k\ n+1)\tau \in G$, so $\tau \in G$. Hence $G = S_{n+1}$. ■

For $1 \leq i, j \leq n$ define

$$m_{ij} = \begin{cases} 1 & \text{if} \quad i = j \\ 2 & \text{if} \quad |i-j| > 1 \\ 3 & \text{if} \quad |i-j| = 1. \end{cases} \tag{54}$$

Let $\Gamma_n = \langle S \mid R \rangle$ be the group with generating set $S = \{s_1, \dots, s_n\}$ and relations

$$R = \{(s_i s_j)^{m_{ij}} :\ 1 \leq i, j \leq n\}.$$

More explicitly, these relations are

$$s_i^2 = 1 \quad \text{and} \quad s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \quad \text{for all} \quad 1 \leq i \leq n$$

and

$$s_i s_j = s_j s_i \quad \text{if} \quad |i-j| \geq 2.$$

**Proposition 13.6** *The map $s_i \mapsto \sigma_i$ extends to an isomorphism $\Gamma_n \xrightarrow{\sim} S_{n+1}$ so we have the presentation*

$$S_{n+1} \simeq \langle s_1, \dots, s_n \mid (s_i s_j)^{m_{ij}} = 1 \quad \forall\ 1 \leq i, j \leq n \rangle.$$

**Proof:** The 2-cycles $\sigma_i \in S_{n+1}$ satisfy the same relations as the generators $s_i \in \Gamma_n$, so there is a surjective homomorphism

$$\phi : \Gamma_n \twoheadrightarrow S_{n+1},$$

such that $\phi(s_i) = \sigma_i$ for all $1 \leq i \leq n$. It suffices to show that $|\Gamma_n| \leq (n+1)!$.

For $n = 1$, we have $\Gamma_1 = \langle s_1 \mid s_1^2 = 1 \rangle \simeq S_2$, so the result is true. Assume that $|\Gamma_{n-1}| \leq n!$. Let $t_1, \dots, t_{n-1}$ be the generators of $\Gamma_{n-1}$. Sending $t_i \mapsto s_{i+1}$ sends $\Gamma_{n-1}$ onto the subgroup $H \subset \Gamma_n$ generated by $s_2, \dots, s_n$. Note that $|H| \leq n!$.

Consider the $n+1$ cosets

$$H_0 = H, \quad H_1 = s_1 H, \quad H_2 = s_2 s_1 H, \quad , \ldots , \quad H_n = s_n s_{n-1} \cdots s_1 H.$$

I claim that for $1 \leq i \leq n$ we have

$$s_i H_i = H_{i-1}, \quad s_i H_{i-1} = H_i, \quad s_i H_j = H_j \quad \text{if } j \neq i, i-1. \tag{55}$$

The first two are clear from the definitions of $H_i$ and the relation $s_i^2 = 1$. For the last equation, suppose first that $j \leq i-2$. Then

$$s_i H_j = s_i s_j s_{j-1} \cdots s_1 H = s_j s_{j-1} \cdots s_1 s_i H = s_j s_{j-1} \cdots s_1 H = H_j.$$

Suppose next that $j \geq i+1$. Then (writing $\dot{s}_i$ for the generator which moves)

$$\begin{aligned} s_i H_j &= \dot{s}_i s_j s_{j-1} \cdots s_{i+1} s_i s_{i-1} \cdots s_1 H \\ &= s_j s_{j-1} \cdots \dot{s}_i s_{i+1} s_i \; s_{i-1} \cdots s_1 H \\ &= s_j s_{j-1} \cdots s_{i+1} s_i \dot{s}_{i+1} \; s_{i-1} \cdots s_1 H \\ &= s_j s_{j-1} \cdots s_{i+1} s_i s_{i-1} \cdots s_1 \dot{s}_{i+1} H \\ &= s_j s_{j-1} \cdots s_{i+1} s_i s_{i-1} \cdots s_1 H \\ &= H_j, \end{aligned}$$

as claimed. Since $s_1, \ldots, s_n$ generate $\Gamma_n$, it follows that $\Gamma_n$ preserves the set $\{H_0, H_1, \ldots, H_n\} \subset \Gamma_n / H$. By transitivity, this containment must be equality. Hence $|\Gamma_n / H| \leq n+1$ and $|\Gamma_n| \leq (n+1)|H| \leq (n+1)n! = (n+1)!$. ■

## 13.4 Coxeter groups and reflection groups

A **Coxeter system** is a pair $(G, S)$ where $G$ is a group with generating set $S \subset G$ and presentation $G \simeq \langle S | R \rangle$ where the relation set $R$ contains $s^2$ for all $s \in S$ and the remaining words in $R$ have the form $(ss')^{m(s,s')}$ for distinct elements $s, s' \in S$ and integers $m(s, s') \geq 2$. In particular, the elements of $S$ all have order two.

We also write $m(s, s') = \infty$ if $ss'$ has infinite order, but this does not appear in $R$. A group $G$ is a **Coxeter group** if $G$ is generated by a set $S \subset G$ of elements of order two such that $(G, S)$ is a Coxeter system. The **rank** of the Coxeter system $(G, S)$ is the cardinality of the set $S$.

The **Coxeter diagram** of $(G, S)$ is the graph with vertex set $S$, and edge set $\{\{s, s'\} : \; m(s, s') \geq 3\}$, with each edge $\{s, s'\}$ labelled by the integer $m(s, s')$. Thus, two vertices $s, s'$ have no edge between them exactly when $s, s'$ commute, and


means that $ss'$ has order $m = m(s, s') \geq 3$. The most common Coxeter systems have small values of $m(s, s')$, where the following alternate notation is used


if $m(s, s') = 3$

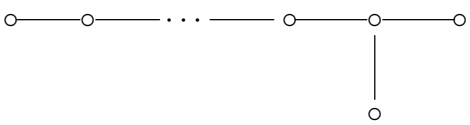
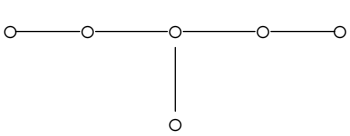
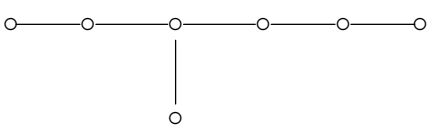
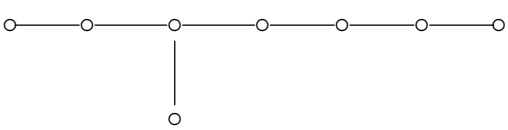
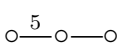
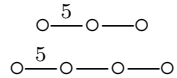

if $m(s, s') = 4$




if $m(s, s') = 6$

A Coxeter system $(G, S)$ is **irreducible** if $S$ is not a disjoint union $S = S' \cup S''$ with $m(s', s'') = 2$ for all $s' \in S'$ and $s'' \in S''$. In other words $(G, S)$ is irreducible if its graph is connected.

The classification of finite irreducible Coxeter groups is given below. Each has a label of the form $\mathsf{X}_n$ where the rank $n$ is the number of vertices in the Coxeter graph. Beware that $\mathsf{A}_n$ is $S_{n+1}$ and not the alternating group. And $\mathsf{D}_n$ is not the dihedral group $D_n$, but is the semidirect product of $S_n$ with the group ${}_+C_2^n = \{(\epsilon_1, \ldots, \epsilon_n) \in \{\pm 1\}^n : \prod \epsilon_i = 1\}$.

| Coxeter label | Coxeter diagram | Group structure |
|---|---|---|
| $\mathsf{A}_n$ |  | $S_{n+1}$ |
| $\mathsf{B}_n$ |  | $C_2^n \rtimes S_n$ |
| $\mathsf{D}_n$ |  | ${}_+C_2^n \rtimes S_n$ |
| $\mathsf{G}_2$ |  | $D_6$ |
| $\mathsf{F}_4$ |  | $\mathsf{D}_4 \rtimes S_3$ |
| $\mathsf{E}_6$ |  | order $= 51840$ |
| $\mathsf{E}_7$ |  | order $= 2903040$ |
| $\mathsf{E}_8$ |  | order $= 696729600$ |
| $\mathsf{I}_2(m), m \neq 2, 3, 4, 6$ |  | $D_m$ |
| $\mathsf{H}_3$ |  | $A_5 \times C_2$ |
| $\mathsf{H}_4$ |  | $(\mathrm{SL}_2(5) \cdot \mathrm{SL}_2(5)) \rtimes C_2$ |

Coxeter groups are a generalization of Euclidean geometry to higher dimensions, in the following sense.

Let $V = \mathbb{R}^n$ with the usual dot product $\mathbf{u} \cdot \mathbf{v}$. A **reflection** on $V$ is an element $r \in \mathrm{GL}_n(\mathbb{R})$ fixing a hyperplane $H$ pointwise and negating the line perpendicular to $H$. If $\mathbf{u}$ is a unit vector perpendicular to $H$ then $r$ is given by

$$r(\mathbf{v}) = \mathbf{v} - 2(\mathbf{u} \cdot \mathbf{v})\mathbf{u}.$$

A **real reflection group** of rank $n$ is a subgroup $G$ of $\mathrm{GL}_n(\mathbb{R})$ generated by reflections. We say $G$ is **irreducible** if no proper subspace of $V$ is preserved by $G$.

It turns out that finite Coxeter groups are finite reflection groups. More precisely we have the following. [20]

[20] For proofs, and much more information about Coxeter groups and reflection groups, see Bourbaki, *Lie groups and Lie algebras* chapters 4,5,6.

**Theorem 13.7** *Let $(G, S)$ be an irreducible Coxeter system of rank $n$ such that $G$ is finite. Then there is an injective homomorphism $\rho : G \to \mathrm{GL}_n(\mathbb{R})$ such that the following hold.*

1. *$\rho(s)$ is a reflection for each $s \in S$.*
2. *The image $\rho(G) \subset \mathrm{GL}_n(\mathbb{R})$ is an irreducible reflection group of rank $n$.*
3. *Every finite, irreducible and reflection-generated subgroup of $\mathrm{GL}_n(\mathbb{R})$ is $\rho(G)$ for a unique irreducible Coxeter system $(G, S)$ of rank $n$.*

## 13.5 Presentations of alternating groups

We can use the presentation of $S_{n+1}$ to get a presentation of $A_{n+1}$, as follows. Let

$$\alpha_i = (1\ 2)(i\ i+1) = \sigma_1\sigma_i, \quad \text{for} \quad 2 \le i \le n.$$

Now let $\Gamma_n$ be the group with generators $a_2, \ldots, a_n$ having relations

$$a_2^3 = a_i^2 = 1 \quad \text{for} \quad 3 \le i \le n$$

and

$$(a_i a_j^{-1})^{m_{ij}} = 1 \quad \text{for all} \quad i \ne j,$$

where $m_{ij}$ are as in (54).

**Proposition 13.8** *The map $a_i \mapsto \alpha_i$ extends to an isomorphism $\Gamma_n \xrightarrow{\sim} A_{n+1}$, so we have the presentation*

$$A_{n+1} \simeq \langle a_2, \ldots, a_n : \ a_2^3 = a_3^2 = \cdots = a_n^2 = 1, \quad (a_i a_j^{-1})^{m_{ij}} = 1 \ \ \forall\, i \ne j \in [2, n] \rangle.$$

**Proof:** We outline the proof, leaving some calculations to the reader. The elements $b_i = a_i^{-1} \in \Gamma_n$ satisfy the same relations as the elements $a_i$. Hence there is an automorphism $\vartheta : \Gamma_n \to \Gamma_n$ such that $\vartheta(a_i) = a_i^{-1}$.

Let $\tilde{\Gamma}_n$ be the set $\langle \vartheta \rangle \times \Gamma_n$ with multiplication

$$(\gamma, \vartheta^i)(\gamma', \vartheta^j) = (\gamma \cdot \vartheta^i(\gamma), \vartheta^{i+j})$$[21]

In $\tilde{\Gamma}$ let $s_1 = (\vartheta, 1)$ and $s_i = (\vartheta, a_i)$ for $2 \le i \le n$. Then the $\{s_i\}$ generate $\Gamma_n$ and satisfy the same relations as $\{\sigma_i\}$ in $S_{n+1}$. Hence we have a surjection $\phi : S_{n+1} \to \tilde{\Gamma}_n$ such that $\phi(\sigma_i) = s_i$. Reciprocally, the elements $s_1, \alpha_2, \ldots, \alpha_n \in S_{n+1}$ satisfy the same relations as $\{\vartheta, a_2, \ldots, a_n\}$ in $\tilde{\Gamma}_n$. Hence there is map $\psi : \tilde{\Gamma}_n \to S_{n+1}$ which is the inverse of $\phi$. One checks that $\psi(\Gamma_n) = A_{n+1}$ and this completes the proof. ■

[21] That is, $\tilde{\Gamma}_n = \Gamma \rtimes \langle \vartheta \rangle$, see section 14.2.

### 13.5.1 A presentation of $A_5$

The presentation of $A_n$ in Prop. 13.8 has many relations, which can be inefficient. The following well-known presentation of $A_5$ has fewer relations.

**Proposition 13.9** *We have* $A_5 \simeq \langle a, b \mid a^5 = b^3 = (ab)^2 = 1\}$.

**Proof:** Let $\Gamma = \langle a, b \mid a^5 = b^3 = (ab)^2 = 1\rangle$. We first find elements $\alpha, \beta \in A_5$ obeying the same relations as $a, b$. We may assume $\alpha = (1\ 2\ 3\ 4\ 5)$, and $\beta = (i\ j\ k)$ is a 3-cycle such that $\alpha\beta$ has order two. In $A_5$, this means $\alpha\beta$ is a 221 cycle, so has a unique fixed-point. Making this fixed-point 1, we have $\beta = (1\ 5\ k)$. To have this be the only fixed-point of $\alpha\beta$ we must have $k = 3$. Indeed, $(1\ 2\ 3\ 4\ 5)(1\ 5\ 3) = (2\ 3)(4\ 5)$. Hence $\beta = (1\ 5\ 3)$ works, and we have a homomorphism $\phi : \Gamma \to A_5$ sending $a \mapsto \alpha$, $b \mapsto \beta$. The image of $\phi$ contains elements of orders $2, 3, 5$, hence is divisible by 30, but $A_5$ is simple, hence has no subgroups of order 30, so $\phi$ is surjective.

It remains to show that $|\Gamma| \leq 60$. Consider the subgroups $A = \langle a\rangle$ and $B = \langle b\rangle$ of $\Gamma$. Since $a^5 = 1$ and $\phi(a) = \alpha \neq 1$, it follows that $|A| = 5$, and likewise $|B| = 3$. It suffices to show that $|\Gamma/A| \leq 12$. This will be achieved if we can exhibit a set of 12 cosets $gA$ which is closed under multiplication by $a$ and $b$.

The orbits of $A$ on $\Gamma/A$ have size 1 or 5, since 5 is prime. Since 3 and 5 are relatively prime it follows that no conjugate of $b$ lies in $A$, which means that $B$ acts freely on $\Gamma/A$. We number the cosets according to $a$-orbits as follows.

$$\mathbf{1} = A$$

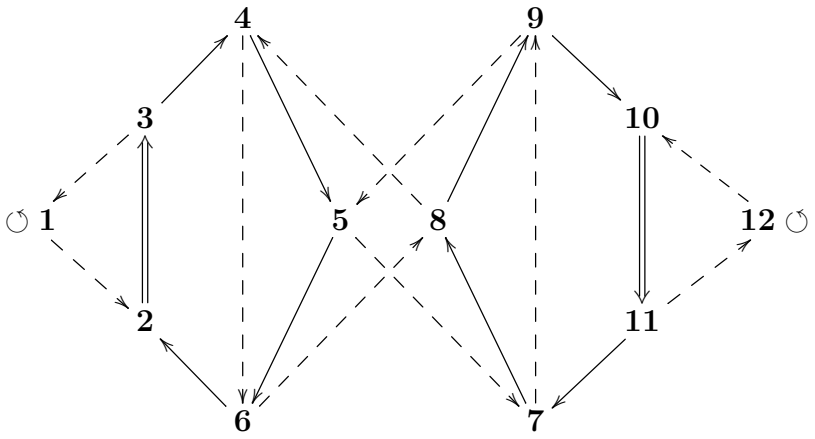
$$\mathbf{2} = bA, \quad \mathbf{3} = abA, \quad \mathbf{4} = a^2bA, \quad \mathbf{5} = a^3bA, \quad \mathbf{6} = a^4bA,$$

$$\mathbf{7} = a^4ba^4bA, \quad \mathbf{8} = ba^4bA = b\cdot\mathbf{6}, \quad \mathbf{9} = aba^4bA, \quad \mathbf{10} = a^2ba^4bA, \quad \mathbf{11} = a^3ba^4bA,$$

$$\mathbf{12} = ba^3ba^4bA = b\cdot\mathbf{11},$$

We do not need to know if these cosets are distinct, since we only seek an upper bound on $|\Gamma/A|$. That $\mathbf{1}, \ldots, \mathbf{12}$ are indeed distinct will result from the proof that they are closed under multiplication by $a$ and $b$.

In the following diagram, a solid arrow $\mathbf{i} \to \mathbf{j}$ means that $a\cdot\mathbf{i} = \mathbf{j}$, and $\circlearrowleft\ \mathbf{i}$ means $a\cdot\mathbf{i} = \mathbf{i}$. We will show that the $b$-action is given by the dashed arrows, where $\mathbf{i} \Rightarrow \mathbf{j}$ means $a\cdot\mathbf{i} = \mathbf{j} = b\cdot\mathbf{i}$.




Since $(ab)^2 = 1$ and $b^{-1} = b^2$, we have the relation $aba = b^2$, hence

$$b \cdot \mathbf{2} = b^2 A = abaA = abA = \mathbf{3}.$$

Since $b \cdot \mathbf{1} = \mathbf{2}$ and $b$ has order three, we have

$$b \cdot \mathbf{3} = b^3 \cdot \mathbf{1} = \mathbf{1},$$

so $\{\mathbf{1}, \mathbf{2}, \mathbf{3}\}$ is a $b$-orbit. Inverting the relation $aba = b^2$, we get $b = a^{-1}b^{-1}a^{-1}$. Using the known $b-$ orbit $\{\mathbf{1}, \mathbf{2}, \mathbf{3}\}$ we compute

$$b \cdot \mathbf{4} = a^{-1}b^{-1}a^{-1} \cdot \mathbf{4} = a^{-1}b^{-1} \cdot \mathbf{3} = a^{-1} \cdot \mathbf{2} = \mathbf{6}.$$

Since $b \cdot \mathbf{6} = \mathbf{8}$, it follows that $\{\mathbf{4}, \mathbf{6}, \mathbf{8}\}$ is a second $b$-orbit. Then we have

$$b \cdot \mathbf{5} = a^{-1}b^{-1}a^{-1} \cdot \mathbf{5} = a^{-1} \cdot \mathbf{8} = \mathbf{7},$$

$$b \cdot \mathbf{9} = a^{-1}b^{-1}a^{-1} \cdot \mathbf{9} = a^{-1} \cdot \mathbf{6} = \mathbf{5},$$

so $\{\mathbf{5}, \mathbf{7}, \mathbf{9}\}$ is a third $b$-orbit. Finally,

$$b \cdot \mathbf{10} = a^{-1}b^{-1}a^{-1} \cdot \mathbf{10} = a^{-1} \cdot \mathbf{7} = \mathbf{11},$$

and since $b \cdot \mathbf{11} = \mathbf{12}$, it follows that $\{\mathbf{10}, \mathbf{11}, \mathbf{12}\}$ is the fourth and final $b$-orbit.

It remains only to check that $a$ fixes $\mathbf{12}$:

$$a \cdot \mathbf{12} = aba^3b \cdot a^4b\mathbf{1} = aba^3b \cdot a\mathbf{5} = aba \cdot a \cdot aba\mathbf{5} = b^{-1}ab^{-1}\mathbf{5} = b^{-1}a\mathbf{9} = b^{-1}\mathbf{10} = \mathbf{12}.$$

This completes the proof that the cosets $\mathbf{1}, \ldots, \mathbf{12}$ exhaust $|\Gamma/A|$. It follows that $|\Gamma/A| = 12$ and $\Gamma \simeq A_5$ as claimed. ■

**Corollary 13.10** *Let $G$ be a group containing nontrivial elements $x, y$ satisfying the relations*

$$x^5 = y^3 = (xy)^2 = 1.$$

*Then the subgroup of $G$ generated by $\{x, y\}$ is isomorphic to $A_5$.*

**Proof:** By Prop. 13.9 and the Mapping Property Prop. 13.4, there is a homomorphism $\phi : A_5 \to G$ sending $a \mapsto x$, $b \mapsto y$. And $\phi$ is nontrivial since $x, y$ are nontrivial. Since $A_5$ is simple, $\phi$ is injective. Hence $A_5$ is isomorphic to the image of $\phi$, which is the subgroup generated by $x, y$. ■

### 13.5.2 The exceptional isomorphism $\mathrm{PSL}_2(9) \simeq A_6$

Here is an illustration of the use of Cor. 13.10. The field $\mathbb{F}_9$ of nine elements can be constructed from the field $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ just as $\mathbb{C}$ is constructed from $\mathbb{R}$, namely $\mathbb{F}_9 = \{a + bi : \ a, b \in \mathbb{F}_3\}$ with multiplication determined by the rule $i^2 = -1$. In $\mathrm{SL}_2(9)$ the matrices

$$X = \begin{bmatrix} 1+i & i \\ 1 & 1 \end{bmatrix}, \quad \text{and} \quad Y = \begin{bmatrix} 1 & 1-i \\ 0 & 1 \end{bmatrix}$$

satisfy $X^5 = -I$, $Y^3 = I$, $(XY)^2 = -I$. Hence the images $x, y$ of $X, Y$ in $\mathrm{PSL}_2(9)$ satisfy

$$x^5 = y^3 = (xy)^2 = 1$$

and therefore $x, y$ generate a subgroup $H \leq \mathrm{PSL}_2(9)$ with $H \simeq A_5$. Since $|\mathrm{PSL}_2(9)| = 9(9^2-1)/2 = 360$ and $|H| = 3 \cdot 4 \cdot 5 = 60$, we have $[\mathrm{PSL}_2(9) : H] = 6$. The action of $\mathrm{PSL}_2(9)$ on the six cosets of $H$ gives a homomorphism

$$\psi : \mathrm{PSL}_2(9) \longrightarrow S_6,$$

which is injective with image in $A_6$, since $\mathrm{PSL}_2(9)$ is simple. Since $|A_6| = 3 \cdot 4 \cdot 5 \cdot 6 = 360$, it follows that $\psi$ gives an isomorphism

$$\psi : \mathrm{PSL}_2(9) \xrightarrow{\sim} A_6,$$

which is one of the exceptional isomorphisms between linear and permutation groups.

## 13.6 The Platonic Groups

The groups $A_4, S_4$ and $A_5$ have presentations

$$\begin{aligned} A_4 &\simeq \langle a, b \mid a^3 = b^3 = (ab)^2 = 1 \rangle \\ S_4 &\simeq \langle a, b \mid a^4 = b^3 = (ab)^2 = 1 \rangle \\ A_5 &\simeq \langle a, b \mid a^5 = b^3 = (ab)^2 = 1 \rangle. \end{aligned} \tag{56}$$

We verified this presentation of $A_5$ above and the others can be done in the same way. The triples $(2, 3, 3), (2, 3, 4), (2, 3, 5)$ also arise from the Platonic solids, as follows.

Let $G$ be a finite group acting on a set $X$, with the following two properties:

1. For all $x \in X$ the stabilizer $G_x$ is nontrivial.
2. Any nonidentity element of $G$ has exactly two fixed-points in $X$.

What can we say about $G$? Let $|G| = n$, let $\mathcal{O}_1, \ldots, \mathcal{O}_r$ be the distinct orbits of $G$ in $X$, and let $m_i$ be the order of the stabilizer of a point in $\mathcal{O}_i$. By the Burnside Counting Formula we have

$$\sum_{i=1}^{r} 1 = \frac{1}{n} \sum_{g \in G} |X^g| = \frac{1}{n} \left( |X| + 2(n-1) \right) = \frac{1}{n} \left[ \sum_{i=1}^{r} \frac{n}{m_i} + 2(n-1) \right],$$

so

$$\sum_{i=1}^{r} \left( 1 - \frac{1}{m_i} \right) = 2 - \frac{2}{n}. \tag{57}$$

We have $r > 1$, lest

$$1 > \frac{1}{m_i} = 2 - \frac{2}{n} \geq 1.$$

And since $1 - 1/m_i \geq 1/2$, we have

$$\frac{r}{2} \leq 2 \left( 1 - \frac{1}{n} \right),$$

implying $r \leq 3$. Hence $r = 2$ or $r = 3$.

If $r = 2$ we have

$$\frac{1}{m_1} + \frac{1}{m_2} = \frac{1}{n} + \frac{1}{n},$$

which means that $m_1 = m_2 = n$, so $X$ has just two elements and $G$ acts trivially on $X$.

We arrive at $r = 3$, and

$$\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} = 1 + \frac{2}{n}.$$

Index so that $m_1 \leq m_2 \leq m_3$. We cannot have $m_1 \geq 3$, lest the left side be $\leq 1$. So $m_1 = 2$ and

$$\frac{1}{m_2} + \frac{1}{m_3} = \frac{1}{2} + \frac{2}{n}.$$

We cannot have $m_2 \geq 4$, lest the left side be $\leq 1/2$. If $m_2 = 2$ then $n = 2m_3$. If $m_2 = 3$ we have

$$\frac{1}{m_3} = \frac{1}{6} + \frac{2}{n},$$

so that $m_3 = 3, 4, 5$ with $n = 12, 24, 60$, respectively. To summarize, we have the following possibilities:

| $r$ | $m_1$ | $m_2$ | $m_3$ | $n$ |
|---|---|---|---|---|
| 2 | $n$ | $n$ | $-$ | $n$ |
| 3 | 2 | 2 | $m$ | $2m$ |
| 3 | 2 | 3 | 3 | 12 |
| 3 | 2 | 3 | 4 | 24 |
| 3 | 2 | 3 | 5 | 60 |

Now assume that $G$ is a finite group acting by by rotations on the two-dimensional sphere $S^2$. Let $X = \{x \in S^2 : \ G_x \neq 1\}$. Then $X$ consists of antipodal pairs $\{x, -x\}$ on the axes of rotation of the non-trivial elements of $G$. For the first two rows of the table above we have $G$ cyclic or dihedral, respectively.

For $(m_1, m_2, m_3) = (2, 3, 3)$, $G$ has 3 elements of order 2 and 8 elements of order three. Since a 2-Sylow subgroup of $G$ has order four and $G$ has no elements of order four, the 2-Sylow must be $K_4$, and is unique, hence normal in $G$. But the 3-Sylows are not unique, hence are not normal. It follows that $G \simeq A_4$. A 3-Sylow is the stabilizer $G_x$ of a $G$-orbit $\{x, y, z, w\}$ in $S^2$ and permutes $\{y, z, w\}$ transitively. Hence each of $y, z, w$ have the same distance from $x$. Likewise $G_y$ permutes $x, z, w$ transitively, so these points all have the same distance from $y$. It follows that $x, y, z, w$ are the vertices of a tetrahedron, whose symmetry group is $G$.

For $(m_1, m_2, m_3) = (2, 3, 4)$, $G$ has $6 + 3$ elements of order two, 8 elements of order three and 6 elements of order four. Hence $G$ has four 3-Sylow subgroups and we have a homomorphism $\pi : G \to S_4$. If $P$ and $Q$ are distinct 3-Sylows then $|N(P) \cap N(Q)| \leq 2$, so $|\ker \pi| \leq 2$. If $|\ker \pi| = 2$ then $\ker \pi$ is central in $G$ and $\operatorname{im} \pi = A_4$. Since there are eight involutions outside $\ker \pi$ we would have at least 4 involutions in $A_4$, which is not the case. So $\ker \pi = 1$ and $\pi : G \to S_4$ is an isomorphism. As above, one can show that the six points in $S^2$ with stablizer $C_4$ form the vertices of an octahedron whose symmetry group is $G$.

For $(m_1, m_2, m_3) = (2, 3, 5)$, we have $|G| = 60$. We show that $G$ is simple. There are 24 elements of order five, hence $G$ has six Sylow 5-subgroups. Let $N$ be a non-trivial normal subgroup of $G$. If $|N|$ is divisible by 5 then all six 5-Sylows are in $N$, so $|N| \geq 1 + 24$, so $|N| \geq 30$. Therefore $N$ contains an element of order two. But $G$ has fifteen conjugate elements of order two, so $|N| \geq 25 + 15 > 30$, hence $N = G$, and we have proved that $G$ is simple. By Cor. 10.20 it follows that $G \simeq A_5$. There is a $G$-orbit of 12 points in $S^2$ whose stabilizers have order 5. One can show that these are the vertices of an icosahedron.

# 14 Building new groups from old

## 14.1 Automorphisms

Recall that an automorphism of a group $G$ is an isomorphism $f : G \to G$ from $G$ to itself. The set $\operatorname{Aut}(G)$ of automorphisms of $G$ forms a group under composition, with identity element $I_G$, given by $I_G(g) = g$ for all $g \in G$.

There are various kinds of automorphisms; some automorphisms come from $G$ itself: For each $g \in G$, let $c_g : G \to G$ be the function given by $c_g(x) = gxg^{-1}$. It is easy to check that $c_g \in \operatorname{Aut}(G)$ and that

$$c : G \to \operatorname{Aut}(G)$$

is a group homomorphism. In general, the homomorphism $c$ is neither injective nor surjective (see examples below). The image $\operatorname{Inn}(G) = \{c_g : \ g \in G\}$ of $c$ is the group **inner automorphisms** of $G$.

In general, the kernel of $c$ is the center $Z(G)$ of $G$, and $c$ induces an isomorphism

$$G/Z(G) \simeq \mathrm{Inn}(G) \subset \mathrm{Aut}(G).$$

You can check that if $\alpha \in \mathrm{Aut}(G)$, then

$$\alpha \circ c_g \circ \alpha^{-1} = c_{\alpha(g)} \qquad \forall\, g \in G.$$

Therefore $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$; the quotient

$$\mathrm{Out}(G) := \mathrm{Aut}(G)/\,\mathrm{Inn}(G)$$

is the **outer automorphism group** of $G$. All of these groups fit into the exact sequence

$$1 \longrightarrow Z(G) \longrightarrow G \xrightarrow{c} \mathrm{Aut}(G) \longrightarrow \mathrm{Out}(G) \longrightarrow 1.$$

Typically, outer automorphisms of $G$ arise from conjugation in a larger group $\widetilde{G}$, in which $G \triangleleft \widetilde{G}$. This is why

$$\mathrm{Aut}(A_n) = S_n,$$

for $n \neq 6$ (see table below). Often one needs to know which subgroups of $G$ are normalized by $\widetilde{G}$. This leads to the notion of characteristic subgroup: We say that a subgroup $H \leq G$ is *characteristic in* $G$ if $\alpha(H) = H$ for every $\alpha \in \mathrm{Aut}(G)$. The center $Z(G)$ and commutator $[G, G]$ are examples of characteristic subgroups in any group $G$.

If $H$ is characteristic in $G$ then $H$ is normal in $G$, but not conversely. For example, if $G = C_2 \times C_2$ then every subgroup is normal, but $\mathrm{Aut}(G) = GL_2(2)$ moves the subgroups of order two $G$, so these are not characteristic. In $G = Q_8$ the subgroups $\langle i\rangle$, $\langle j\rangle$, $\langle k\rangle$ have index two, hence are normal in $G$, but there is an automorphism $\alpha \in \mathrm{Aut}(Q_8)$ of order three, sending $i \mapsto j \mapsto k \mapsto i$. Hence none of these subgroups are characteristic.

**Examples of Automorphism groups**

| $G$ | $Z(G)$ | $\mathrm{Aut}(G)$ | $\mathrm{Inn}(G)$ | $\mathrm{Out}(G)$ |
|---|---|---|---|---|
| $\mathbb{Z}$ | $\mathbb{Z}$ | $C_2$ | $1$ | $C_2$ |
| $\mathbb{Z}^n$ | $\mathbb{Z}^n$ | $GL_n(\mathbb{Z})$ | $1$ | $GL_n(\mathbb{Z})$ |
| $C_n$ | $C_n$ | $(\mathbb{Z}/n\mathbb{Z})^\times$ | $1$ | $(\mathbb{Z}/n\mathbb{Z})^\times$ |
| $C_p^n$ | $C_p^n$ | $GL_n(p)$ | $1$ | $GL_n(p)$ |
| $S_n, n \neq 2, 6$ | $1$ | $S_n$ | $S_n$ | $1$ |
| $S_6$ | $1$ | $S_6 \cdot 2$ | $S_6$ | $C_2$ |
| $A_n, n \neq 2, 3, 6$ | $1$ | $S_n$ | $A_n$ | $C_2$ |
| $A_6$ | $1$ | $S_6 \cdot 2$ | $A_6$ | $C_2 \times C_2$ |
| $D_4$ | $C_2$ | $D_4$ | $D_2$ | $C_2$ |
| $Q_8$ | $C_2$ | $S_4$ | $D_2$ | $S_3$ |

The notation $\mathrm{Aut}(S_6) \simeq S_6 \cdot 2$ means that $\mathrm{Aut}(S_6)$ fits into an exact sequence

$$1 \longrightarrow S_6 \xrightarrow{c} \mathrm{Aut}(S_6) \longrightarrow C_2 \longrightarrow 1,$$

and similarly for $A_6$. We will examine this exceptional case in the next section.

### 14.1.1 Automorphisms of $S_n$

An automorphism of a group $G$ permutes the conjugacy classes in $G$, and the inner automorphisms preserve each conjugacy class. If $\alpha \in \mathrm{Aut}(G)$ and $X, Y$ are conjugacy classes in $G$ such that $\alpha(X) = Y$, then $|X| = |Y|$ and the elements in $Y$ have the same order as the elements in $X$.

Suppose $\alpha$ is an automorphism of the symmetric group $S_n$, for $n \geq 2$. Then $\alpha$ sends the class $X$ of 2-cycles in $S_n$ to another class $Y$ of elements of order two such that $|Y| = |X| = n(n-1)/2$. There is $1 \leq k \leq n/2$ such that the elements in $Y$ have cycle type $[2^k 1^{n-2k}]$. One possibility is $k = 1$, which means $Y = X$, as occurs for the inner automorphisms.

Suppose that $k \geq 2$. There are $n!/(k!2^k(n-2k)!)$ elements in $S_n$ with cycle type $[2^k 1^{n-2k}]$, so we must have

$$\frac{n(n-1)}{2} = |X| = |Y| = \frac{n!}{k!2^k(n-2k)!}.$$

We rewrite this equation as

$$k(2k-2)(2k-3)\cdots 2\cdot 1 = (n-2)(n-3)\cdot(n-4)(n-5)\cdots(n-2k+2)(n-2k+1).$$

As $2k-2 \le n-2$ and $2k-4 \le n-4$ etc, we must have $n=2k$ and find that

$$n = 2(n-3)(n-5)\cdots 3\cdot 1 \ge 2(n-3),$$

which implies that $n=6$ and $k=3$. We note that the classes $[21111]$ and $[222]$ in $S_6$ both have $15$ elements. We have proved the following.

**Lemma 14.1** *If $S_n$ has an automorphism $\alpha$ which does not preserve the class of 2-cycles, then $n=6$ and $\alpha$ sends the class of 2-cycles to the class of 222-cycles.*

We next investigate the case $k=1$.

**Lemma 14.2** *Suppose $\alpha \in S_n$ preserves the class of 2-cycles. Then $\alpha$ is inner.*

**Proof:** [22] For each $2 \le r \le n$ there are $a_r, b_r \in \{1,\ldots,n\}$ such that $\alpha(1\ r) = (a_r\ b_r)$. The order of $a_r$ and $b_r$ is not determined, and we will exploit this ambiguity.

We single out $r=2$, and set $a=a_2$, $b=b_2$, so that $\alpha(1\ 2) = (a\ b)$. Let $r \ge 3$. Since $(1\ r)(2\ r) = (1\ 2\ r)$ has order three, we must have

$$\alpha(1\ r)\cdot\alpha(1\ 2) = (a_r\ b_r)(a\ b)$$

also of order three. This means the intersection $\{a_r,\ b_r\} \cap \{a,\ b\}$ consists of a single element. Hence either $a_r \in \{a,\ b\}$ and $b_r \notin \{a,\ b\}$ or vice-versa. Let us switch $a_r$ and $b_r$ if necessary so that $a_r \in \{a,\ b\}$ and $b_r \notin \{a,\ b\}$ for all $r \ge 3$.

It appears that whether $a_r = a$ or $a_r = b$ could depend on $r$. Suppose that for some $r, s \ge 3$ we have $a_r = a$ and $a_s = b$. Then

$$\alpha(1\ 2\ r) = \alpha(1\ r)\cdot\alpha(1\ 2) = (a\ b_r)\cdot(a\ b) = (a\ b\ b_r),$$

and

$$\alpha(1\ 2\ s) = \alpha(1\ s)\cdot\alpha(1\ 2) = (b\ b_s)\cdot(a\ b) = (a\ b_s\ b).$$

Now $(1\ 2\ r)(1\ 2\ s) = (1\ r)(2\ s)$ has order two, so $(a\ b\ b_r)(a\ b_s\ b)$ must also have order two. But this is impossible, for if $b_r = b_s$ then $(a\ b\ b_r)(a\ b_s\ b) = e$, while if $b_r \ne b_s$ then $(a\ b\ b_r)(a\ b_s\ b) = (a\ b_s\ b_r)$ has order three.

This contradiction shows that either $a_r = a$ for all $r \ge 3$ or $a_r = b$ for all $r \ge 3$. We now switch $a$ and $b$, if necessary, so that $a_r = a$ for all $r \ge 3$. Now $\alpha$ is conjugation by the permutation $\sigma$ sending $1 \mapsto a$, $2 \mapsto b$, and $r \mapsto b_r$ for all $r \ge 3$. ■

[22] This is a rewrite of the proof by I. Segal, Bull. AMS 1940, vol **46**, p. 565.

## 14.2 Semidirect Products (external view)

Let $G$ and $H$ be groups, and suppose we are given a homomorphism $\varphi : G \to \mathrm{Aut}(H)$, sending $g \in G$ to the automorphism $\varphi_g \in \mathrm{Aut}(H)$. This is called an *action of $G$ on $H$ via $\varphi$*. We can then form a new group $H \rtimes_\varphi G$, as follows. As a set, $H \rtimes_\varphi G = H \times G$ is the direct product of the two sets $G$ and $H$. The multiplication is given by

$$(h, g) \cdot (h', g') = (h \cdot \varphi_g(h'), gg'), \qquad \forall h \in H, g \in G.$$

Note that $H \rtimes_\varphi G = H \times G$ as groups exactly when $\varphi$ is the trivial homomorphism.

We have injective homomorphisms

$$\lambda : H \to H \rtimes_\varphi G, \qquad \rho : G \to H \rtimes_\varphi G,$$

given by $\lambda(h) = (h, 1)$ and $\rho(g) = (1, g)$. It is common to identify $H = \lambda(H)$, and $G = \rho(G)$, but for clarity and brevity at this stage, we write $H' = \lambda(H)$ and $G' = \rho(G)$. Please check that the following hold:

1. $H \rtimes_\varphi G = H'G'$;
2. $H' \cap G' = \{1\}$;
3. $H' \trianglelefteq (H \rtimes_\varphi G)$ and $(H \rtimes_\varphi G)/H' \simeq G$.
4. For $g \in G$ and $h \in H$, we have $\rho(g) \cdot \lambda(h) \cdot \rho(g)^{-1} = \lambda(\varphi_g(h))$.

These formulas spell everything out completely, but they are cumbersome to use in practice, so one resorts to a more compact notation, such as the following. We identify $H = \lambda(H)$ and $G = \rho(G)$, we suppress $\varphi$, and we write $HG$ instead of $H \rtimes_\varphi G$, with multiplication rule

$$hg \cdot h'g' = h\varphi_g(h') \cdot gg'.$$

Thus, the semidirect product construction makes it so that "conjugation by $g$" on $H$ is the given automorphism $\varphi_g$. This makes the multiplication rule easy to remember, and is shows how to recognize a semidirect product.

**Theorem 14.3** *Let $G$ be a group with subgroups $H, K \leq G$ having the following properties:*

1. *$H \trianglelefteq G$;*
2. *$G = HK$;*
3. *$H \cap K = \{1\}$.*

*Then $G \simeq H \rtimes_\varphi K$, where $\varphi : K \to \mathrm{Aut}(H)$ is given by $\varphi_k(h) = khk^{-1}$ for all $k \in K$ and $h \in H$.*

**Proof:** The product map $H \times K \to G$, given by $(h,k) \mapsto hk$, is a homomorphism from $H \times_\varphi K$ to $G$, which is surjective by part 2 and injective by part 1. ■

**Example 1: The groups $D_4$, $A_4$ and $S_4$**

The group $D_2 = C_2 \times C_2$ has automorphism group

$$\mathrm{Aut}(D_2) = GL_2(2) = S_3.$$

The subgroups of $S_3$ are isomorphic to $C_1, C_2, C_3$ and $S_3$ itself. Hence we have semidirect products of $D_2$ with each of these subgroups of $S_3$, where $\varphi$ is the inclusion map. In fact, we have

$$\begin{aligned} D_2 \rtimes C_1 &\simeq D_2 \\ D_2 \rtimes C_2 &\simeq D_4 \\ D_2 \rtimes C_3 &\simeq A_4 \\ D_2 \rtimes S_3 &\simeq S_4. \end{aligned}$$

As the right side is a chain of subgroups of $S_4$, it suffices to verify the last line. Let $K < S_4$ be the subgroup fixing 4. Then $K \simeq S_3$ and $K$ does not contain any $22-cycle$, so $K \cap D_2 = \{1\}$. Hence $S_4 = D_2 \rtimes K$.

**Example 2: Dihedral groups**

In the dihedral group $D_n$ of order $2n$, let $r$ be a rotation of order $n$, and let $s$ be a reflection. Then

$$D_n = \langle r \rangle \rtimes_\varphi \langle s \rangle \simeq C_n \rtimes_\varphi C_2,$$

where $\varphi_s(r) = r^{-1}$. In particular, we have $D_4 \simeq C_4 \rtimes C_2$. We have also seen in example 1 that $D_4 \simeq D_2 \rtimes C_2$. This shows that a semidirect product decomposition need not be unique.

**Example 3: Nonabelian groups of order $p^3$**

Let $p$ be a prime. The group $C_p \times C_p$ has automorphism group

$$\mathrm{Aut}(C_p \times C_p) = GL_2(p).$$

In $GL_2(p)$ we have the subgroup

$$U_2(p) = \left\{ \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} : \ y \in \mathbb{Z}/p\mathbb{Z} \right\} \simeq C_p$$

so we can form the semidirect product $(C_p \times C_p) \rtimes U_2(p)$, which is nonabelian of order $p^3$. On the other hand the group

$$U_3(p) = \left\{ \begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} : \ x, y, z \in \mathbb{Z}/p\mathbb{Z} \right\}$$

has the subgroup with $y = 0$ isomorphic to $C_p \times C_p$, the subgroup with $x = z = 0$ isomorphic to $U_2(p)$, and we have

$$U_3(p) \simeq (C_p \times C_p) \rtimes U_2(p).$$

This group is called the **Heisenberg group** over $\mathbb{Z}/p\mathbb{Z}$, because its commutator relations mimic the Uncertainty Principle.

If $p = 2$, then $U_3(2) \simeq D_4$. The quaternion group $Q_8$ also has order $2^3$, but it cannot be expressed as a nontrivial semidirect product, because every nontrivial subgroup of $Q_8$ contains the center $Z(Q_8) = \{\pm 1\}$, so condition 3 above is never satisfied.

**Example 4: Affine transformations**

Let $V$ be a vector space over a field $k$. An *affine space over* $V$ is a set $X$ on which $V$ acts freely and transitively. We write the action as $(v, x) \mapsto x + v$, where $v \in V$ and $x \in X$. If we choose any point $x_0 \in X$, we get a bijection $V \to X$ sending $v \mapsto x_0 + v$. However, there is no canonical point, or "origin" in $X$, so we cannot identify $X$ with $V$ in any canonical way. This means we cannot add points in $X$, because that requires an origin. We can *subtract* points in $X$, but the result is a vector in $V$. Namely, for $x, y$ in $X$, we define $x - y$ to be the unique vector $v \in V$ such that $x = y + v$.

An *affine transformation* of $X$ is a mapping $f : X \to X$ for which there exists $\dot{f} \in GL(V)$ such that

$$f(x) - f(y) = \dot{f}(x - y), \qquad \forall\, x, y \in X.$$

Under composition, the set of affine transformations of $X$ forms a group $\mathrm{Aff}(X)$.

Each $v \in V$ corresponds to the translation $t_v(x) = x + v$, which is an affine transformation with $\dot{t}_v = I_V$. One can check that $f \circ t_v \circ f^{-1} = t_{f(v)}$ for all $f \in \mathrm{Aff}(X)$. Hence $V$ is a normal subgroup of $\mathrm{Aff}(X)$. Now choose an arbitrary point $x_0 \in X$, and let $G_{x_0} = \{f \in \mathrm{Aff}(X) :\ f(x_0) = x_0\}$. I claim that

$$\mathrm{Aff}(X) = V \rtimes_\varphi G_{x_0}, \tag{58}$$

where $\varphi(g) = \dot{g}$ for $g \in G_{x_0}$. We have already observed that part 1 of Thm. 14.3 holds. Part 3 holds because $V$ acts freely on $X$. For part 2, let $f \in \mathrm{Aff}(X)$ be any affine transformation. Then $f(x_0)$ is some point in $X$, so we can write it as $f(x_0) = x_0 + v$ for a unique $v \in V$. Then the affine transformation $g = t_v^{-1} f$ fixes $x_0$, and we have $f = t_v \circ g$ with $g \in G_{x_0}$, as required by part 2. This proves the claim (58). Finally, I claim that we have an isomorphism

$$G_{x_0} \simeq GL(V), \qquad g \mapsto \dot{g} \in GL(V).$$

For if $g \in G_{x_0}$ then $g(x_0 + v) = x_0 + \dot{g}(v)$, which implies that $g \mapsto \dot{g}$ is an injective homomorphism. Finally, if $g_0 \in GL(V)$, then the mapping $x_0 + v \mapsto x_0 + g_0(v)$ is an affine transformation, proving the claim. We have thus shown that

$$\mathrm{Aff}(X) \simeq V \rtimes GL(V).$$

Note, however, that the subgroup of $\mathrm{Aff}(X)$ which is isomorphic to $GL(V)$ is non-canonical: it depends on the choice of $x_0$. If $V$ is finite dimensional and we choose a basis of $V$ and use it to identify

$$V = F^n \simeq \left\{ \begin{bmatrix} 1 & 0 \\ v & I_n \end{bmatrix} : v \in F^n \right\}$$

and $GL(V) = GL_n(F)$, we can write more explicitly:

$$\mathrm{Aff}(X) \simeq \left\{ \begin{bmatrix} 1 & 0 \\ v & g \end{bmatrix} : v \in F^n,\ g \in GL_n(F) \right\}.$$

**Example 5: Parabolic subgroups**

Let $V$ be a finite dimensional vector space over a field $F$. Fix a subspace $U \subset V$. In the group $GL(V)$ the subgroup

$$G_U = \{g \in GL(V) : \ gU = U\}$$

stabilizing $U$ is called a *parabolic subgroup*. We will show that the parabolic subgroup $G_U$ is a semidirect product.

Each $g \in G_U$ induces a linear transformation on the quotient vector space $V/U$, namely $\bar{g} \cdot (v + U) = (g\dot{v}) + U$. Let $R_U = \{g \in G_U : \bar{g} = I_{V/U}\}$ be the subgroup of $G_U$ acting trivially on $V/U$. Note that $g \in R_U$ if and only if $gv - v \in U$ for all $v \in V$. One checks that $R_U$ is normal in $G_U$. To find the complement, choose a subspace $W \subset V$ complementary to $U$, so that $V = U \oplus W$, and let $L_U = \{g \in G_U : \ gW = W\}$ be the subgroup of $GL(V)$ stabilizing both $U$ and $W$. Then $L_U$ acts on $R_U$ by conjugation, and we have

$$G_U = R_U \rtimes L_U.$$

**Example 6: Frobenius groups**

The essence of the proof of above is the following fact:

*If a group $G$ acts transitively on a set $X$ and $G$ has a normal subgroup $K$ acting freely and transitively on $X$, then $G = K \rtimes_\varphi G_x$, where $x$ is any point in $X$ and $\varphi_g(k) = gkg^{-1}$ for all $g \in G_x$, and $k \in K$.*

This is a weak result, because the existence of the marvellous subgroup $K$ is a strong hypothesis, which we would like to avoid. It is easy to check that the nontrivial elements of $K$ are exactly those elements of $G$ which have no fixed-points in $X$. So the essential question is: when do these elements form a subgroup of $G$?

A finite group $G$ is called a *Frobenius group* if $G$ acts transitively on a finite set $X$ and the following two properties hold:

- Every nontrivial element of $G$ fixes at most one point in $X$.
- Some nontrivial element of $G$ fixes at least one point in $X$.

Equivalently, every stabilizer $G_x$ is nontrivial and any two stabilizers $G_x, G_y$ intersect trivially.

**Theorem 14.4 (Frobenius)** *If $G$ is a Frobenius group then the set*

$$K = \{k \in G : \ k \cdot x \neq x \quad \forall x \in X\} \cup \{1\}$$

*is a subgroup of $G$ and for any $x \in X$ we have $G \simeq K \rtimes G_x$.*

This only known proof of this theorem uses character theory, which you will learn next semester.

### 14.2.1 Groups of order $p^2q$

Let $p$ and $q$ be distinct primes. In this section our aim is to classify groups $G$ of order $p^2q$, where $p$ and $q$ are distinct primes. We begin with a more general situation.

A $pq$**-group** is a group $G$ whose order is of the form $p^aq^b$ for some positive integers $a, b$. Such a group factors as $G = PQ$, where $P$ and $Q$ are Sylow $p$- and $q$-subgroups of $G$. Indeed, the sets $P \times Q$ and $G$ have the same cardinality, and the product map $P \times Q \to G$, sending $(x, y) \mapsto xy$ is injective since $P \cap Q = \{1\}$.

We now make the additional assumption that some Sylow subgroup is normal in $G$. If $P \lhd G$ then $G$ is a semidirect product $G \simeq P \rtimes Q$, with respect to some action of $Q$ on $P$. It may happen that different actions of $Q$ on $P$ give isomorphic groups $P \rtimes Q$.

**Lemma 14.5** *If $\varphi, \psi : Q \to \mathrm{Aut}(P)$ are two homomorphisms, then we have*

$$P \rtimes_\varphi Q \simeq P \rtimes_\psi Q$$

*if and only if there is $g \in \mathrm{Aut}(Q)$ such that $\varphi$ is conjugate to $\psi \circ g$ in $\mathrm{Aut}(P)$.*

**Proof:** Let $F_0 : P \rtimes_\varphi Q \simeq P \rtimes_\psi Q$ be an isomorphism. Since $P$ is the unique Sylow $p$-subgroup of both sides, we have $F_0(P) = P$. Since $F_0(Q)$ is another Sylow $q$-subgroup of $P \rtimes_\psi Q$, we may compose $F_0$ with an inner automorphism of $P \rtimes_\psi Q$ to obtain another isomorphism $F : P \rtimes_\varphi Q \simeq P \rtimes_\psi Q$ with the property that $F(P) = P$ and $F(Q) = Q$. Thus we have restrictions $f = F|_P \in \mathrm{Aut}(P)$ and $g = F|_Q \in \mathrm{Aut}(Q)$.

Let $x \in P$ and $y \in Q$ and consider the conjugation $yxy^{-1}$ in $P \rtimes_\varphi Q$. On one hand, $yxy^{-1} = \varphi_y(x) \in P$, so

$$F(yxy^{-1}) = f(\varphi_y(x)).$$

On the other hand, we have

$$F(yxy^{-1}) = F(y)F(x)F(y)^{-1} = g(y)f(x)g(y)^{-1} = \psi_{g(y)}(f(x))$$

in $P \rtimes_\psi Q$. Hence $f \circ \varphi_y = \psi_{g(y)} \circ f$, or

$$f \circ \varphi_y \circ f^{-1} = \psi \circ g(y) \tag{59}$$

so that $\varphi$ and $\psi \circ g$ are conjugate in $\mathrm{Aut}(P)$, as claimed.

Conversely, if $f \in \mathrm{Aut}(P)$ and $g \in \mathrm{Aut}(Q)$ satisfy (59) then one checks that The map $F : P \rtimes_\varphi Q \simeq P \rtimes_\psi Q$ given by $F(xy) = f(x)g(y)$, for $x \in P$ and $y \in Q$, is a group isomorphism. ■

Let $\mathrm{Hom}(Q, \mathrm{Aut}(P))$ be the set of all homomorphisms $\varphi : Q \to \mathrm{Aut}(P)$. The group $\mathrm{Aut}(P) \times \mathrm{Aut}(Q)$ acts on $\mathrm{Hom}(Q, \mathrm{Aut}(P))$ as follows. Given $\alpha \in \mathrm{Aut}(P), \beta \in \mathrm{Aut}(Q)$, the transform $(\alpha, \beta)\cdot\varphi$ of a homomorphism $\varphi \in \mathrm{Hom}(Q, \mathrm{Aut}(P))$ is the new homomorphism $Q \to \mathrm{Aut}(P)$ given by

$$[(\alpha, \beta) \cdot \varphi]_y = \alpha \circ \varphi_{\beta^{-1}(y)} \circ \alpha^{-1}, \qquad \text{for all} \quad y \in Q.$$

Here we take $\beta^{-1}$ to make this a left group action. The Lemma may now be rephrased as follows.

**Corollary 14.6** *The isomorphism classes of groups of the form $G = P \rtimes Q$ are in bijection with the orbits of $\mathrm{Aut}(P) \times \mathrm{Aut}(Q)$ on $\mathrm{Hom}(Q, \mathrm{Aut}(P))$ under the action just described.*

Assume now that $Q$ is cyclic. If we choose a generator $y$ of $Q$, a nontrivial homomorphism $\varphi : Q \to \mathrm{Aut}(P)$ is determined by the automorphism $\varphi_y \in \mathrm{Aut}(P)$ generating a subgroup $Q_y := \langle \varphi_y \rangle \leq \mathrm{Aut}(P)$ of order dividing $|Q|$. An automorphism of $Q$ changes $y$ to some power $y^j$ where $q \nmid j$ and $Q_{y^j} = Q_y^j = Q_y$. Hence we have

**Corollary 14.7** *If $Q$ is cyclic , the isomorphism classes of groups of the form $G = P \rtimes Q$ are in bijection with the conjugacy-classes in $\mathrm{Aut}(P)$ of subgroups of order dividing $|Q|$.*

Now suppose $|G| = p^2 q$ and as above let $P, Q$ be Sylow $p-$ and $q-$ subgroups of $G$ respectively. Recall the $p$-factorization is the expression $|G| = p^2 \cdot \nu \cdot n_p$, where $\nu = [N_G(P) : P]$ and $n_p = [G : N_G(P)]$ is the number of Sylow $p$-subgroups of $G$. If $\nu = 1$ then $Q \trianglelefteq G$, by the Burnside Transfer Theorem. In this case the $q$-factorization is $q \cdot p^2 \cdot 1$. The possible $p$ and $q$-factorizations are tabulated below, where "none" means no such combination is possible.

| | $q \cdot p^2 \cdot 1$ | $q \cdot p \cdot p$ | $q \cdot 1 \cdot p^2$ | conditions |
|---|---|---|---|---|
| $p^2 \cdot q \cdot 1$ | $P \times Q$ | $P \rtimes Q$ | $P \rtimes Q$ | – |
| $p^2 \cdot 1 \cdot q$ | $Q \rtimes P$ | none | none | $p \mid q-1$ |
| conditions | – | $q \mid p-1$ | $q \mid p^2-1$ | |

We see that some Sylow subgroup of $G$ is normal. Hence we may apply Cor. 14.6, after possibly interchanging $P$ and $Q$. The case $G = P \times Q$ is equivalent to $G$ being abelian, for which there are two possible groups: $G \simeq C_{p^2} \times C_q$ or $G \simeq C_p^2 \times C_q$ according as $P \simeq C_{p^2}$ or $C_p^2 = C_p \times C_p$, respectively. The group $G$ must be abelian unless $p \mid q-1$ or $q \mid p^2-1$. From now on we assume one of these conditions holds.

*Case 1:* $p \mid q-1$. Then $G \simeq Q \rtimes P$, so we calculate the orbits of $\mathrm{Aut}(Q) \times \mathrm{Aut}(P)$ on $\mathrm{Hom}(P, \mathrm{Aut}(Q))$. Since $\mathrm{Aut}(Q) \simeq C_{q-1}$ is abelian, these are just the orbits of $\mathrm{Aut}(P)$ on $\mathrm{Hom}(P, C_{q-1})$.

If $P = C_{p^2}$ we may apply Cor. 14.7. The groups $G$ in this case correspond to subgroups of $C_{q-1}$ of order $1, p$ or $p^2$, the latter occuring only if $p^2 \mid q-1$.

If $P = C_p^2$ then $\mathrm{Aut}(P) = \mathrm{GL}_2(p)$ and $C_{q-1}$ has a unique subgroup of order $p$, so the groups $G$ in this case correspond to $\mathrm{GL}_2(p)$-orbits in $\mathrm{Hom}(C_p^2, C_p)$, of which there are two: zero and nonzero.

Combining the two possibilities for $P$, we see that when $p \mid q-1$ the number of groups of order $p^2 q$ is five if $q^2 \mid p-1$ and four otherwise.

*Case 2:* $q \mid p^2-1$. Here we have $G = P \rtimes Q$. Since $Q$ is cyclic, we may apply Cor. 14.7 to see that the groups of order $p^2 q$ correspond to conjugacy-classes of subgroups of $\mathrm{Aut}(P)$ of order $1$ or $q$.

If $P = C_{p^2}$ then $\mathrm{Aut}(P) = \mathbb{Z}/p^2\mathbb{Z}^\times \simeq C_p \times C_{p-1}$. If $q \mid p-1$ then $\mathrm{Aut}(P)$ has exactly one subgroup of order $q$, giving two groups in this case, one abelian, one nonabelian. If $q \nmid p-1$ then there is only the abelian group $C_{p^2} \times C_q$.

| $P = C_{p^2}$ | $P = C_p^2$ | condition |
|---|---|---|
| 1 | 1 | $p \nmid q-1$ and $q \nmid p^2-1$ |
| 2 | 2 | $p \mid q-1$ and $p^2 \nmid q-1$ |
| 3 | 2 | $p^2 \mid q-1$ |
| 2 | 3 | $q = 2$ |
| 1 | 2 | $2 < q \mid p+1$ |
| 2 | $\frac{q+5}{2}$ | $2 < q \mid p-1$. |

Figure 1: The number of groups of order $p^2q$

If $P = C_p^2$ then $\mathrm{Aut}(P) = \mathrm{GL}_2(p)$. This breaks into three subcases.

*i)* $q = 2$. In this case $p$ is odd and $\mathrm{GL}_2(p)$ has three conjugacy classes of subgroups of order dividing two, generated by

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The three groups are respectively

$$C_p \times C_p \times C_2, \qquad D_p \times C_p, \qquad S[D_p \times D_p],$$

where the latter group is the subgroup of $D_p \times D_p$ generated by $C_p \times C_p$ and an involution inverting both factors under conjugation.

*ii)* $2 < q \mid p+1$. In this case $q \nmid p-1$ and $\mathrm{GL}_2(p)$ has a unique subgroup of order $q$, up to conjugacy (see 5.1.1), whence two groups in this case.

*iii)* $2 < q \mid p-1$. In this case we have a subgroup $V = C_q \times C_q$ of the diagonal matrices and all subgroups of $\mathrm{GL}_2(p)$ of order $q$ can be conjugated into $V$. Moreover, two such subgroups of $V$ are conjugate if and only if one is transformed into the other by switching the factors in $V$. Regarding $V$ additively, the groups $G$ in this case correspond to lines $[x, y]$ in the projectivization of $V$, modulo the involution $[x, y] \leftrightarrow [y, x]$. This involution fixes the lines $[1, 1]$ and $[1, -1]$ and acts freely on the remaining lines. Counting the abelian case, we get $1 + 2 + \frac{1}{2}(q-1) = \frac{1}{5}(q+5)$ isomorphism classes of groups in this case.

All cases are summarized in Figure 1. For each condition on $p, q$ we write the number of groups of order $p^2q$ in the form $N' + N''$, where $N'$ (resp. $N''$) is the number of groups with the given $p, q$ condition having $P = C_{p^2}$ (resp. $P = C_p \times C_p$).

## 14.3 Extensions

The essential problem of extension theory is:

*Given two groups $A, B$, to find all groups $G$ having $A$ as a normal subgroup with quotient $G/A \simeq B$.*

Informally, we are asking how many groups we can build with $A$ at the bottom and $B$ at the top.

For example, if $A = C_4$ and $B = C_2$, then $C_2 \times C_4, C_8, D_4$ and $Q_8$ are all the groups $G$ containing a normal subgroup isomorphic to $C_4$ with cyclic quotient isomorphic to $C_2$.

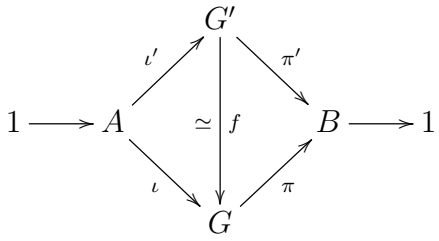
This is a very difficult problem. It becomes easier if we specify the maps involved.

**Definition 14.8** *Let $A$ and $B$ be groups. An* **extension of $B$ by $A$** *is a triple $(G, \iota, \pi)$ where $G$ is a group, $\iota : A \to G$ is an injective homomorphism and $\pi : G \to B$ is a surjective homomorphism with $\operatorname{im}\iota = ker\pi$. Two extensions $(G, \iota, \pi)$ and $(G', \iota', \pi')$ are* **equivalent** *if there exists an isomorphism $f : G' \to G$ such that $f \circ \iota' = \iota$ and $\pi \circ f = \pi'$.*

Thus, an extension of $B$ by $A$ is given by an exact sequence

$$1 \longrightarrow A \xrightarrow{\iota} G \xrightarrow{\pi} B \longrightarrow 1, \tag{60}$$

and two extensions $(G, \iota, \pi), (G', \iota', \pi')$ of $B$ by $A$ are equivalent if there is an isomorphism $f : G' \xrightarrow{\sim} G$ making the following diagram commutative:




It is possible for $G$ and $G'$ to be isomorphic for inequivalent extensions $(G, \iota, \pi), (G', \iota', \pi')$ (see exercise...).

We say the extension $(G, \iota, \pi)$ of $B$ by $A$ is **split** if there exists a homomorphism $s : B \to G$ such that $\pi \circ s = \mathrm{id}_B$ is the identity map on $B$. The map $s$, if it exists, is called a **section**, or a **splitting** of the extension.

If $(G', \iota', \pi')$ is an extension of $B$ by $A$ equivalent to $(G, \iota, \pi)$ via an isomorphism $f : G' \to G$ and $s : B \to A$ is a splitting of $(G', \iota', \pi')$, then $f \circ s$ is a splitting of $(G, \iota, \pi)$. Hence the quality of being split depends only on the equivalence class of the extension.

**Proposition 14.9** *For an extension $(G, \iota, \pi)$ of $B$ by $A$, the following are equivalent.*

1. *The extension $(G, \iota, \pi)$ is split.*
2. *There is a subgroup $B' \leq G$ which is mapped isomorphically onto $B$ via $\pi$.*
3. [23] *There is a homomorphism $\varphi : B \to \mathrm{Aut}(A)$ such that the extension $(G, \iota, \pi)$ is equivalent to $(A \rtimes_\varphi B, \iota', \pi')$, where $\iota'(a) = (a, 1)$ and $\pi'(b) = (1, b)$.*

[23] I thank Andew Yarmola for suggesting this formulation.

**Proof:**

$(1 \Rightarrow 2$:) Assume $(G, \iota, \pi)$ is split, and let $s : B \to G$ be a section. Then $s$ is injective, since $\pi \circ s = I_B$, so $s$ is an isomorphism from $B$ onto the subgroup $B' = s(B) \leq G$, and it is easy to check that $\pi$ maps $B'$ isomorphically onto $B$.

$(2 \Rightarrow 1$:) Assume there is a subgroup $B' \leq G$ which is mapped isomorphically onto $B$ via $\pi$. Let $s : B \to B'$ be the inverse of the isomorphism $\pi|_{B'} : B' \to B$. It is easy to check that $s$ is a section, so the extension $(G, \pi)$ is split.

$(3 \Rightarrow 1$:) Suppose $(G, \iota, \pi)$ is equivalent to $(A \rtimes_\varphi B, \iota', \pi')$ as in 3, via an isomorphism $f : A \rtimes_\varphi B \xrightarrow{\sim} G$. Then $s(b) = f(1, b)$ defines a section of $(G, \iota, \pi)$.

$(1, 2 \Rightarrow 3$:) Assume $(G, \iota, \pi)$ is split, and let $s : B \to G$ be a section. Since both $\iota$ and $s$ are injective, there is a unique homomorphism $\varphi : B \to \mathrm{Aut}(A)$ such that by $\iota(\varphi_b(a)) = s(b) \cdot \iota(a) \cdot s(b)^{-1}$. The map $f : A \rtimes_\varphi B \xrightarrow{\sim} G$ given by $f(a, b) = \iota(a) \cdot s(b)$ is an isomorphism giving the equivalence asserted in 3. ■

There is one situation where an extension is guaranteed to split.

**Theorem 14.10** *Suppose $A$ and $B$ are finite groups with relatively prime orders. Then any extension of $B$ by $A$ is split.*

**Proof:** See [Isaacs *Finite Group Theory* p.79 Theorem 3.8]. ■

The simplest example of a non-split extension is given by

$$1 \longrightarrow C_2 \longrightarrow C_4 \xrightarrow{\pi} C_2 \longrightarrow 1,$$

where $\pi$ is the squaring map and $C_2$ is viewed as the subgroup of squares in $C_4$. Note that $\pi$ is the unique surjection $C_4 \twoheadrightarrow C_2$. To see that this extension is nonsplit, note that $C_2$ is the unique subgroup of order two in $C_4$. Thus, both groups of order four are extensions of $C_2$ by $C_2$. One of them, $C_2 \times C_2$, is a split extension, while the other $C_4$, is nonsplit.

Something similar happens with non-abelian groups of order eight: both $D_4$ and $Q_8$ are extensions of $C_2$ by $C_4$. The former is split and the latter is nonsplit.

## 14.4 Metacyclic groups and extensions

A *metacyclic group* is a group $G$ having a cyclic normal subgroup $A$ with cyclic quotient $B = G/A$. Any cyclic group $C$ is metacyclic. Indeed, we can take $A$ to be any subgroup of $C$. Then $A$ is cyclic and so is $B = C/A$.

If $p$ is a prime then the Borel subgroups of $\mathrm{SL}_2(p)$ and $\mathrm{PGL}_2(p)$ are metacyclic: They have normal subgroups of order $p$ with cyclic quotients of order $p - 1$.

If $p$ and $q$ are primes then any group $G$ of order $pq$ is metacyclic. Indeed we have seen in section 14.6 that if $p \leq q$ and $P, Q$ are the corresponding Sylow subgroups then $Q \triangleleft G$ and $G/Q \simeq P$. In fact (more advanced), if $G$ is a finite group in which every Sylow subgroup is cyclic then $G$ is metacyclic.

The classification of metacyclic groups is simpler if we specify the groups $A$ and $B$ in advance. For this we use the language of extensions: A **metacyclic extension** is an extension

$$1 \longrightarrow A \xrightarrow{\iota} G \xrightarrow{\pi} B \longrightarrow 1. \tag{61}$$

where $A$ and $B$ are cyclic. In this section we classify metacyclic extensions with $G$ finite. So we fix cyclic groups $A \simeq C_m$ and $B \simeq C_n$, as well as generators $\alpha, \beta$ of $A$ and $B$, respectively.

**Proposition 14.11** *Let $(G, \iota, \pi)$ be a metacyclic extension of $B$ by $A$. Let $a = \iota(\alpha)$ and choose an element $b \in G$ such that $\pi(b) = \beta$. Then*

1. *Every element of $G$ can be written uniquely as as $a^i b^j$, for $i \in \mathbb{Z}/m\mathbb{Z}$ and some integer $0 \leq j < n$.* [24]

2. *The group $G$ has the presentation*

$$G \simeq \langle a, b \mid a^m = e, \quad bab^{-1} = a^q, \quad b^n = a^r \rangle \tag{62}$$

   *for some elements $q, r$ in $\mathbb{Z}/m\mathbb{Z}$ such that*

$$q^n = 1, \qquad \text{and} \qquad qr = r. \tag{63}$$

3. *Let $(G_1, \iota_1, \pi_1)$ be another extension of $B$ by $A$, let $a_1 = \iota_1(\alpha)$ and choose $b_1 \in G_1$ such that $\pi_1(b_1) = \beta$. Let $q_1, r_1$ be as in part 2, for $a_1, b_1$. Then the extensions $(G_1, \iota_1, \pi_1)$ and $(G, \iota, \pi)$ are equivalent if and only if $q_1 = q$ and $r_1 = r + (1 + q + \cdots + q^{n-1})k$, for some $k \in \mathbb{Z}/m\mathbb{Z}$.*

**Proof:** For part 1, let $x \in G$ is an arbitrary element, we have $\pi(x) = \beta^j$ for some $j \in \mathbb{Z}$, and also $\pi(b^j) = \beta^j$, so $xb^{-j} \in \ker \pi = \langle a \rangle$, which means that $x = a^i b^j$ for some $i \in \mathbb{Z}/m\mathbb{Z}$ and integer $j$. Since $\pi(b^n) = \pi(b)^n = \beta^n = 1$, we have $b^n \in \ker \pi = \langle a \rangle$, so $b^n = a^r$, for some $r \in \mathbb{Z}/m\mathbb{Z}$. Hence in the expression $x = a^i b^j$ we may replace $j$ by its remainder when divided by $n$.

We are given that $\alpha$ has order $m$ and $\beta$ has order $n$. Since $\iota$ is injective this means $a$ has order $m$. And since $\langle a \rangle \trianglelefteq G$ we have $bab^{-1} = a^q$ for some $q \in (\mathbb{Z}/m\mathbb{Z})^\times$. We have proved that $G$ satisfies the relations (62). These calculations also show that the group $\langle a, b \mid a^m = e, \quad bab^{-1} = a^q, \quad b^n = a^r \rangle$ has order at most $nm$, hence is isomorphic to $G$.

To see that $q, r$ satisfy (63), note that $b^n = a^r$ commutes with $a$. Hence $a = b^n a b^{-n} = a^{(q^n)}$, which implies $q^n = 1$. Also $b$ commutes with $b^n = a^r$, so we have $a^r = ba^r b^{-1} = (bab^{-1})^r = a^{qr}$, so that $r = qr$, proving (63).

[24] Note that $b$ need not have order $n$, so we cannot write $j \in \mathbb{Z}/n\mathbb{Z}$.

For part 3, let $(G_1, \iota_1, \pi_1)$ be another extension of $B$ by $A$, set $\iota_1(\alpha) = a_1$ and choose $b_1 \in G_1$ such that $\pi_1(b_1) = \beta$. Applying part 2 to this extension, we get relations analogous to (62) and (63), namely

$$a_1^m = e, \quad b_1 a_1 b_1^{-1} = a_1^{q_1}, \quad b_1^n = a_1^{r_1}, \tag{64}$$

along with

$$q_1^n = 1, \qquad \text{and} \qquad q_1 r_1 = r_1. \tag{65}$$

Suppose the extensions $(G, \iota, \pi)$ and $(G_1, \iota_1, \pi_1)$ are equivalent. This means there is an isomorphism $f : G_1 \to G$ such that $f\iota_1 = \iota$ and $\pi f = \pi_1$. The former relation means that $f(a_1) = a$ while the second implies that $f(b_1)$ is another lift of $\beta$ in $G$. Hence we have

$$f(b_1) = a^k b,$$

for some $k \in \mathbb{Z}/m\mathbb{Z}$. And since $f(a_1) = a$, we have

$$a^{r_1} = f(a_1^{r_1}) = f(b_1)^n = (a^k b)^n = a^{(1+q+\cdots+q^{n-1})k+r},$$

where the last equality follows by induction from the relations $bab^{-1} = a^q$ and $b^n = a^r$. Hence we have $r_1 = (1 + q + \cdots + q^{n-1})k$ in $\mathbb{Z}/m\mathbb{Z}$, as claimed.

Finally, we have

$$a^{q_1} = f(a_1^{q_1}) = f(b_1 a_1 b_1^{-1}) = f(b_1) \cdot a \cdot f(b_1)^{-1} = a^k b \cdot a \cdot b^{-1} a^{-k} = a^k \cdot a^q \cdot a^{-k} = a^q,$$

so $q_1 = q$ in $\mathbb{Z}/m\mathbb{Z}$.

Conversely, if $r_1 = (1 + q + \cdots + q^{n-1})k$ in $\mathbb{Z}/m\mathbb{Z}$ then the above calculations show that $a$ and $a^k b$ satisfy the relations of $a_1$ and $b_1$, so there is a surjective homomorphism $f : G_1 \to G$ such that $f(a_1) = a$ and $f(b_1) = a^k b$. These equations imply that $f\iota_1 = \iota$ and $\pi f = \pi_1$. Finally, $f$ is an isomorphism since $|G| = mn = |G_1|$.

■

We next prove that such extensions exist, whenever the conditions (63) are satisfied.

**Proposition 14.12** *Suppose $q, r$ are elements of $\mathbb{Z}/m\mathbb{Z}$ satisfying $q^n = 1$ and $qr = r$. Then there exists an extension*

$$1 \longrightarrow A \xrightarrow{\iota} G \xrightarrow{\pi} B \longrightarrow 1$$

*and an element $b \in G$ with $\pi(b) = \beta$, such that*

$$bab^{-1} = a^q, \qquad \text{and} \qquad b^n = a^r.$$

**Proof:** We will construct $G$ as a quotient of a split extension. Let $C$ be a cyclic group of order $mn$, choose a surjective homomorphism $\psi : C \to B$, and let $\gamma$ be a generator of $C$ such that $f(\gamma) = \beta$.

Since $q^n = 1$, we have $q^{mn} = 1$, so there is a homomorphism

$$\varphi : C \to (\mathbb{Z}/m\mathbb{Z})^\times = \mathrm{Aut}(A), \qquad \text{such that} \qquad \varphi(\gamma) = q.$$

Form the semidirect product $\widetilde{G} = A \rtimes_\varphi C$, where we have the relation $\gamma\alpha\gamma^{-1} = \alpha^q$. We observe that $\gamma^n\alpha\gamma^{-n} = \alpha^{(q^n)} = \alpha$ and $\gamma\alpha^r\gamma^{-1} = \alpha^{qr} = \alpha^r$. Thus, $\alpha$ commutes with $\gamma^n$ and $\gamma$ commutes with $\alpha^r$. Since $\widetilde{G}$ is generated by $\alpha$ and $\gamma$, this implies that the cyclic subgroup $H_r = \langle \alpha^{-r}\gamma^n \rangle$ is contained in the center of $\widetilde{G}$. In particular, $H_r \trianglelefteq \widetilde{G}$, so we can form the quotient group

$$G_r := \widetilde{G}/H_r.$$

Let $\iota_r : A \to G_r$ be the projection of $A \subset \widetilde{G}$ to $G_r$. This is injective since $A \cap H_r = \{1\}$. Set $a = \iota_r(\alpha) = \alpha H_r$ and $b = \gamma H_r$, both elements of $G_r$. Then $a$ and $b$ satisfy the relations

$$a^m = 1, \qquad bab^{-1} = a^q, \qquad b^n = a^r.$$

Let $\tilde{\pi} : \widetilde{G} \to B$ be the composition

$$\tilde{\pi} : \widetilde{G} \xrightarrow{p} C \xrightarrow{\psi} B,$$

where $p$ is the natural projection $G = A \rtimes C \to C$. We have $\tilde{\pi}(\alpha^i\gamma^j) = \beta^j$. In particular, $\pi(\alpha^{-r}\gamma^n) = \beta^n = 1$. Thus, $\tilde{\pi}$ induces a surjective map $\pi_r : G_r \to B$ such that $\pi_r(a^ib^j) = \beta^j$. We see that $\pi_r(b) = \beta$ and that $\iota_r(A) \leq \ker \pi_r$. On the other hand, if $\pi_r(a^ib^j) = 1$ then $n \mid j$, say $j = nk$, and we have $a^ib^j = a^ia^{rk} \in \iota_r(A)$. This shows that $\ker \pi_r = \iota_r(A)$ and completes the proof that $(G_r, \iota_r, \pi_r)$ is the desired extension. ■

The conditions on $r$ and $q$ can be understood more simply if we regard "$q$" as the endomorphism of $\mathbb{Z}/m\mathbb{Z}$ given by multiplication by $q$. Likewise we view $q - 1$ and $q_n := 1 + q + \cdots + q^{n-1}$ as endomorphisms of $\mathbb{Z}/m\mathbb{Z}$. The condition $rq = r$ means that $r \in \ker(q-1)$. The condition $q^n = 1$ means that $\operatorname{im} q_n \subset \ker(q-1)$. Part 3 of the proposition means that the equivalence class of the extension $(G, \pi)$ depends only on the class of $r$ in $\ker(q-1)/\operatorname{im} N_q$. In this language, the two propositions may be then summarized as follows.

**Theorem 14.13** *Fix generators $\alpha$ of $A \simeq C_m$ and $\beta$ of $B \simeq C_n$ and let $q \in (\mathbb{Z}/m\mathbb{Z})^\times$ satisfy $q^n = 1$. Then there is a bijection from the subquotient $\ker(q-1)/\operatorname{im} q_n$ of $\mathbb{Z}/m\mathbb{Z}$ to the set of equivalence classes of extensions $(G, \iota, \pi)$ of $B$ by $A$ such that any lift of $\beta$ in $G$ acts on $\iota(A)$ by the power $q$. To the class of $r \in \ker(q-1)/\operatorname{im} q_n$ corresponds the equivalence class of the extension $(G_r, \iota_r, \pi_r)$ where*

$$G_r = \langle a, b \mid a^m = e, \quad bab^{-1} = a^q, \quad b^n = a^r \rangle,$$

*$\iota_r(\alpha) = a$ and $\pi_r(b) = \beta$. This extension splits iff the class of $r$ in $\ker(q-1)/\operatorname{im} q_n$ is zero.*

We have now classified all metacyclic extensions, and have shown that every metacyclic group is isomorphic to one of the groups

$$G(m, n, q, r) = \langle a, b \mid a^n = e,\ bab^{-1} = a^q, b^n = a^r \rangle,$$

where $q, r \in \mathbb{Z}/m$ satisfy $q^n = 1$ and $(q-1)r = 0$. However, the same group can appear in different extensions. For example, if $\gcd(j, n) = 1$ then $\ker(q^j - 1) = \ker(q-1)$ on $\mathbb{Z}/m\mathbb{Z}$

$$G(m, n, q^j, r) \simeq G(m, n, q, r)$$

via $a \mapsto a, b \mapsto b^j$. Hence the group $G(m, n, q, r)$ depends only on the subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ generated by $q$.

**Application:** Metacyclic groups arise naturally in the Galois Theory of $p$-adic fields. A simple case is as follows: Let $p$ be a prime and let $L$ is a finite Galois extension of the field $\mathbb{Q}_p$ of $p$-adic numbers. There is a canonical intermediate field $\mathbb{Q}_p \subset K \subset L$, obtained by adjoining to $\mathbb{Q}_p$ all roots of unity in $L$ of order prime to $p$. In the above discussion take $q = p$ and let $n = [K : \mathbb{Q}_p]$ and $m = [L : K]$. Assume that $p \nmid m$. Then $G = \mathrm{Gal}(L/\mathbb{Q}_p)$ is a metacyclic group with quotient $B = \mathrm{Gal}(K/\mathbb{Q}_p)$ and kernel $A = \mathrm{Gal}(L/K)$. The generator $b$ corresponds to a *Frobenius automorphism*, and $a$ corresponds to an automorphism fixing $K$, of order $m$. See Serre's *Local Fields* for more details.