**ALGEBRA 3 (MATH 456)**
**COURSE NOTES**
**FALL 2020**
**VERSION: June 28, 2020**

EYAL Z. GOREN,
MCGILL UNIVERSITY

Contents

# Part 1. Basic Concepts and Key Examples

Groups are among the most basic of algebraic structures. Because of their simplicity, in terms of their definition, their complexity is large. For example, vector spaces, which have a very complex definition, are easy to classify; once the field and dimension are known, the vector space is unique up to isomorphism. In contrast, it is difficult to list all groups of a given order, or even obtain an asymptotic formula for that number.

In the study of vector spaces the objects are well understood and so one focuses on the study of maps between them. One studies canonical forms (e.g., the Jordan canonical form), diagonalization, and other special properties of linear transformations (normal, unitary, nilpotent, etc.). In contrast, at least in the theory of finite groups on which this course focuses, there is no comparable theory of maps. A theory exists mostly for maps into matrix groups; such maps are called linear representations and we will make initial steps in this theory towards the end of the course.

While we shall define such maps (called homomorphisms) between groups in general, there will be a large set of so-called simple groups for which there are essentially no such maps: the image of a simple group under a homomorphism is for all practical purposes just the group itself. To an extent, the simple groups serve as basic building blocks, or "atoms", from which all other finite groups are composed. The set of atoms is large, infinite in fact. The classification of all simple groups was completed in the second half of the 20-th century and has required thousands of pages of difficult math. There will be little we will be able to say about simple groups in this course, besides their existence and some key examples. Thus, our focus - apart from the three isomorphism theorems - will be on the structure of the objects, that is the groups, themselves. We will occupy ourselves with understanding the structure of subgroups of a finite group, with groups acting as symmetries of a given set and with special classes of groups – cyclic, simple, abelian, solvable, etc.

## 1. First definitions

### 1.1. Group.

A **group** $G$ is a non-empty set with a function

$$m\colon G \times G \to G,$$

where we usually abbreviate $m(g,h)$ to $g * h$ or simply $gh$, such that the following hold:

(1) (**Associativity**) $f(gh) = (fg)h$ for all $f, g, h \in G$. [1]
(2) (**Identity**) There is an element $e \in G$ such that for all $g \in G$ we have $eg = ge = g$.
(3) (**Inverse**) For every $g \in G$ there is an element $h \in G$ such that $gh = hg = e$.

We call $m(g,h)$ the product of $g$ and $h$. It follows quite easily from associativity that given any $n$ elements $g_1, \dots, g_n$ of $G$ we can put parentheses as we like in $g_1 * \cdots * g_n$ without changing the final outcome. For that reason we allow ourselves to write simply $g_1 \cdots g_n$, though the actual computation of such product is done by successively by multiplying two elements at the time, e.g. $(((g_1g_2)(g_3g_4))g_5)$ is a way to compute $g_1g_2g_3g_4g_5$.

[1] In full notation $m(f, m(g,h)) = m(m(f,g),h)$.

The **identity** element is unique: if $e'$ has the same property then $e' = ee' = e$. Often we will denote the identity element by 1 (or by 0 is the group is commutative - see below). When confusion is possible, we will write $e_G$ or $1_G$ to indicate that the corresponding element is the identity of the group $G$.

The element $h$ provided in axiom (3) is unique as well: if $h'$ has the same property then $hg = e = gh'$ and so $h = he = h(gh') = (hg)h' = eh' = h'$. We may therefore denote this $h$ unambiguously by $g^{-1}$ and call it the **inverse** of $g$. Note that if $h$ is the inverse of $g$ then $g$ is the inverse of $h$ and so $(g^{-1})^{-1} = g$. Another useful identity is $(fg)^{-1} = g^{-1}f^{-1}$. It is verified just by checking that $g^{-1}f^{-1}$ indeed functions as $(fg)^{-1}$. And it does: $(g^{-1}f^{-1})(fg) = g^{-1}(f^{-1}f)g = g^{-1}eg = g^{-1}g = e$, and a similar calculation gives $(fg)(g^{-1}f^{-1}) = e$.

We define by induction $g^n = g^{n-1}g$ for $n > 0$ and $g^n = (g^{-n})^{-1}$ for $n < 0$. Also $g^0 = e$, by definition. One proves that $g^{n+m} = g^n g^m$ for any $n, m \in \mathbb{Z}$.

A group is called of **finite order** if it has finitely many elements. It is called **abelian** if it is **commutative**: $gh = hg$ for all $g, h \in G$. The term "abelian" comes from the name of Niels Henrik Abel (1802 – 1829), a Norwegian mathematician who made fundamental contributions to Algebra; the Abel prize is named after him.

1.2. **Subgroup and order.** A **subgroup** $H$ of a group $G$ is a subset of $G$ such that: (i) $e \in H$, (ii) if $g, h \in H$ then $gh \in H$, and (iii) if $g \in H$ then also $g^{-1} \in H$. One readily checks that in fact $H$ is a group. One checks that $\{e\}$ and $G$ are always subgroups, called the **trivial subgroups**. Any other subgroup is called **proper**. We will use the notation

$$H < G$$

to indicate that $H$ is a subgroup of $G$. This notation allows $H = G$.

One calls a subgroup $H$ **cyclic** if there is an element $h \in H$ such that $H = \{h^n : n \in \mathbb{Z}\}$. Note that for $h \in G$, $\{h^n : n \in \mathbb{Z}\}$ is always a cyclic subgroup of $G$. We denote it by $\langle h \rangle$. The **order** of an element $h \in G$, $\mathrm{ord}(h)$, is defined to be the minimal positive integer $n$ such that $h^n = e$. If no such $n$ exists, we say $h$ has infinite order.

**Lemma 1.2.1.** *For every $h \in G$ we have* $\mathrm{ord}(h) = \sharp\langle h \rangle$.

In words the Lemma says that the order of an element is the order of the (cyclic) subgroup it generates.

*Proof.* Assume first that $\mathrm{ord}(h)$ is finite. Since for every $n$ we have $h^{n+\mathrm{ord}(h)} = h^n h^{\mathrm{ord}(h)} = h^n$ we see that $\langle h \rangle = \{e, h, h^2, \dots, h^{\mathrm{ord}(h)-1}\}$. Thus, also $\sharp\langle h \rangle$ is finite and is at most $\mathrm{ord}(h)$.

Suppose conversely that $\sharp\langle h \rangle$ is finite, say of order $n$. Then the elements of $\langle h \rangle$ given by $\{e = h^0, h, \dots, h^n\}$ cannot be distinct and thus for some $0 \le i < j \le n$ we have $h^i = h^j$. Therefore, $h^{j-i} = e$ and we conclude that $\mathrm{ord}(h)$ is finite and $\mathrm{ord}(h)$ is at most $\sharp\langle h \rangle$. This concludes the proof. □

**Corollary 1.2.2.** *If $h$ has a finite order $n$ then $\langle h \rangle = \{e, h, \dots, h^{n-1}\}$ and consists of precisely $n$ elements (that is, there are no repetitions in this list.)*

It is ease to check that if $\{H_\alpha : \alpha \in J\}$ is a non-empty set of subgroups of $G$ then $\cap_{\alpha \in J} H_\alpha$ is a subgroup as well. Let $\{g_\alpha : \alpha \in I\}$ be a set consisting of elements of $G$ (here $I$ is some index set). We denote by $\langle \{g_\alpha : \alpha \in I\} \rangle$ the minimal subgroup of $G$ containing $\{g_\alpha : \alpha \in I\}$. It is clearly the intersection of all subgroups of $G$ containing the set $\{g_\alpha : \alpha \in I\}$.

The next lemma provides a more concrete description of the subgroup $\langle \{g_\alpha : \alpha \in I\} \rangle$ generated by the set $\{g_\alpha : \alpha \in I\}$.

**Lemma 1.2.3.** *The subgroup $\langle\{g_\alpha : \alpha \in I\}\rangle$ is the set of all finite expressions $h_1 \cdots h_t$ where each $h_i$ is some $g_\alpha$ or $g_\alpha^{-1}$.*

*Proof.* Clearly $\langle\{g_\alpha : \alpha \in I\}\rangle$ contains each $g_\alpha$ hence all the expressions $h_1 \cdots h_t$ where each $h_i$ is some $g_\alpha$ or $g_\alpha^{-1}$. Thus, from the characterization of $\langle\{g_\alpha : \alpha \in I\}\rangle$ as the minimal subgroup containing the set $\{g_\alpha : \alpha \in I\}$, it is enough to show that the set of all finite expressions $h_1 \cdots h_t$, where each $h_i$ is some $g_\alpha$ or $g_\alpha^{-1}$, is a subgroup. Clearly $e$ (equal to the empty product, or to $g_\alpha g_\alpha^{-1}$ if you prefer) is in it. Also, from the definition it is clear that this set is closed under multiplication. Finally, since $(h_1 \cdots h_t)^{-1} = h_t^{-1} \cdots h_1^{-1}$, it is also closed under taking inverses. □

We call $\langle\{g_\alpha : \alpha \in I\}\rangle$ **the subgroup of** $G$ **generated by** $\{g_\alpha : \alpha \in I\}$; if it is equal to $G$, we say that $\{g_\alpha : \alpha \in I\}$ are **generators** for $G$.

## 2. Main examples

It is critical to familiarize ourselves with the fundamental examples. This is the only way one can build intuition for the subject and realize its vast applicability.

### 2.1. $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^\times$.

The set of integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$, with the addition operation, is an infinite abelian group whose identity element is 0. It is cyclic; both 1 and $-1$ are generators and, in fact, the only generators. But note that we also have $\mathbb{Z} = \langle 2, 3\rangle$ and so on. So $\mathbb{Z}$ has many generating sets. However, if we wish to generate it just by a single element, the only choices are either 1, or $-1$.

The group $\mathbb{Z}/n\mathbb{Z}$of integers modulo $n$, $\{0, 1, 2, \dots, n-1\}$, with addition modulo $n$, is a finite abelian group. The group $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group with generator 1. In fact (see the section on cyclic groups), an element $x$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $(x, n) := \gcd(x, n) = 1$.

Consider $(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} : (a, n) = 1\}$ with multiplication. Its order is denoted by $\varphi(n)$ (the function $n \mapsto \varphi(n)$ is call **Euler's phi function**; See the exercises for further properties of this function). To see it is a group, note that multiplication is associative and if $(a, n) = (b, n) = 1$ then also $(ab, n) = 1$ and so indeed we get an operation on $\mathbb{Z}/n\mathbb{Z}^\times$. The congruence class 1 is the identity and the existence of inverse follows from finiteness: given $a \in \mathbb{Z}/n\mathbb{Z}^\times$ consider the function $x \mapsto ax$. It is injective: if $ax = ay$ then $a(x - y) = 0 \pmod n$, that is (using the same letters to denote integers in these congruence classes), $n | a(x - y)$. Since $(a, n) = 1$, we conclude that $n | (x - y)$, that is, $x = y$ in $\mathbb{Z}/n\mathbb{Z}$. It follows that $x \mapsto ax$ is also surjective and thus there is an element $x$ such that $ax = 1$.

The Euclidean algorithm gives another proof that inverses exists. Since $(a, n) = 1$, there are $x, y$ such that $ax + ny = 1$, and the algorithm allows us to find $x$ and $y$. Note that $ax \equiv 1 \pmod n$ and so $x$ is the multiplicative inverse to $a$ modulo $n$.

### 2.2. Fields.

Let $\mathbb{F}$ be a field. This structure was introduced in the course MATH 235. Then $(\mathbb{F}, +)$, the set $\mathbb{F}$ with the addition operation, is a commutative group. As well, $(\mathbb{F}^\times, \times)$, the non-zero elements with the product operation, is a commutative group. Thus, for example, $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ ($p$ prime) are groups with respect to addition. The sets $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}, \mathbb{Z}/p\mathbb{Z} - \{0\}$ ($p$ prime) are groups with respect to multiplication. The unit circle $\{z \in \mathbb{C} : |z| = 1\}$ is a subgroup of $\mathbb{C}^\times$.

2.3. **The dihedral group $D_n$.** Let $n \geq 3$. Consider the linear transformations of the plane that take a regular polygon with $n$ sides, symmetric about zero, onto itself. One easily sees that every such symmetry is determine by its action of the vertices $1, 2$ (thought of as vectors, they form a basis) and that it takes these vertices to the vertices $i, i+1$ or $i+1, i$, where $1 \leq i \leq n$ (and the labels of the vertices are read modulo $n$). One concludes that every such symmetry is of the form $y^a x^b$ for suitable and unique $a \in \{0, 1\}, b \in \{1, \dots, n\}$, where $y$ is the reflection fixing 1 (so takes $n, 2$ to $2, n$) and $x$ is the rotation taking $1, 2$ to $2, 3$. One finds that $y^2 = e = x^n$ and that $yxy = x^{-1}$. All other relations are consequences of these.

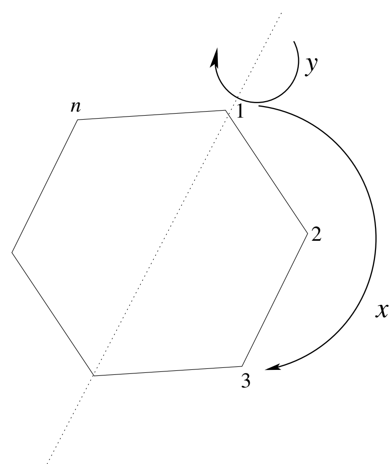



FIGURE 1. Symmetries of a regular Polygon with $n$ vertices.

The **Dihedral group** $D_n$, the group of all these symmetries, is thus a group of order $2n$ generated by a reflection $y$ and a rotation $x$ satisfying $y^2 = x^n = xyxy = e$. Expressing the group $D_n$ by means of $x$ and $y$ satisfying these relations makes sense also for $n = 1, 2$, but one loses the geometric interpretation. Therefore, we will typically consider only $n \geq 3$.

The elements $\{1, x, x^2, \dots, x^{n-1}\}$ are clock-wise rotations by the angles $\{0, \frac{2\pi}{n}, \frac{4\pi}{n}, \dots, \frac{2(n-1)\pi}{n}\}$, respectively. The elements $\{y, xy, x^2y, \dots, x^{n-1}y\}$ are all reflections.

2.4. **The symmetric group $S_n$.** Consider the set $S_n$ consisting of all injective (hence bijective) functions, called **permutations**,

$$\sigma\colon \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}.$$

We define

$$m(\sigma, \tau) = \sigma \circ \tau.$$

This makes $S_n$ into a group, whose identity $e$ is the identity function $e(i) = i, \forall i$.

We may describe the elements of $S_n$ in the form of a table:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}.$$

This defines a permutation $\sigma$ by the rule $\sigma(a) = i_a$.

Another device is to use the notation $(n_1\, n_2 \dots n_s)$, where the $n_j$ are distinct elements of $\{1, 2, \dots, n\}$. This defines a permutation $\sigma$ according to the following convention: $\sigma(n_a) = n_{a+1}$ for $1 \leq a < s$, $\sigma(n_s) = n_1$, and for any other element $x$ of $\{1, 2, \dots, n\}$ we let $\sigma(x) = x$. Such a permutation is called a **cycle**. A cycle of length 2 is called a **transposition**. One can easily prove the following facts:

(1) Disjoint cycles commute.

(2) Every permutation is a product of disjoint cycles (uniquely up to permuting the cycles and omitting cycles of length one).
(3) The order of $(n_1\, n_2 \dots n_s)$ is $s$.
(4) If $\sigma_1, \dots, \sigma_t$ are disjoint cycles of orders $r_1, \dots, r_t$ then the order of $\sigma_1 \circ \cdots \circ \sigma_t$ is the least common multiple of $r_1, \dots, r_t$.
(5) The symmetric group has order $n!$.

More generally, given any non-empty set $T$, we let $\Sigma_T$ denote the group whose elements are bijections $\sigma\colon T \to T$; the group operation is composition $m(\sigma, \tau) = \sigma \circ \tau$, the identity element is the identity function $1\colon T \to T$ (the function given by $1(t) = t, \forall t \in T$) and, finally, the inverse of $\sigma$ is just the inverse function $\sigma^{-1}$. If $T = \{1, 2, \dots, n\}$ we have $\Sigma_T = S_n$. If $T$ has $n$ elements, then there is a natural identification of $\Sigma_T$ with $S_n$.

**Example 2.4.1.** The order of the permutation $(1\,2\,3\,4)$ is 4. Indeed, it is not trivial and $(1\,2\,3\,4)^2 = (1\,3)(2\,4)$, $(1\,2\,3\,4)^3 = (4\,3\,2\,1)$, $(1\,2\,3\,4)^4 = 1$.

The permutation $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 5 & 4 & 2 \end{smallmatrix}\right)$ is equal to the product of cycles $(1\,6\,2)(4\,5)$. It is of order 6.

The problem with the notation $\left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{smallmatrix}\right)$ is that it's long. On the other hand, any permutation in $S_n$ can be written this way. A compromise is achieved by the notation $[i_1\ i_2\ \cdots\ i_n]$ for $\left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{smallmatrix}\right)$. This notation appears in many textbooks and articles. Note, however, that we will never use it in this course.

The reason we will never use it after the end of this paragraph is that it's potentially very confusing. Note, for example, that $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 5 & 4 & 2 \end{smallmatrix}\right)$ is written $[6\ 1\ 3\ 5\ 4\ 2]$ in this notation. However, this is very different from the cycle permutation $(6\,1\,3\,5\,4\,2)$ – for example, the first takes 1 to 6 and 2 to 1, but the second takes 1 to 3 and 2 to 6. Thus, confusing the type of parentheses could be disastrous.

2.4.1. *Sign; permutations as linear transformations.*

**Lemma 2.4.2.** *Let $n \geq 2$. Let $S_n$ be the group of permutations of $\{1, 2, \dots, n\}$. There exists a surjective function*

$$\mathrm{sgn}\colon S_n \to \{\pm 1\}$$

*(called the **sign**). It has the property that for every $i \neq j$,*

$$\mathrm{sgn}(\ (ij)\ ) = -1,$$

*and for any two permutations $\sigma, \tau$,*

$$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma) \cdot \mathrm{sgn}(\tau).$$

**Terminology**: We will refer to the property $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma) \cdot \mathrm{sgn}(\tau)$ by saying sgn is a **homomorphism**. The terminology will be justified later.

*Proof.* Consider the polynomial in $n$-variables[2]

$$p(x_1, \dots, x_n) = \prod_{i<j} (x_i - x_j).$$

Given a permutation $\sigma$, we may define a new polynomial

$$\prod_{i<j} (x_{\sigma(i)} - x_{\sigma(j)}).$$

[2]For $n = 2$ we get $x_1 - x_2$. For $n = 3$ we get $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$.

Note that $\sigma(i) \neq \sigma(j)$ and for any pair $k < \ell$ we obtain in the new product either $(x_k - x_\ell)$ or $(x_\ell - x_k)$. Thus, for a suitable choice of a sign $\mathrm{sgn}(\sigma) \in \{\pm 1\}$, we have[3]

$$\prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)}) = \mathrm{sgn}(\sigma)\prod_{i<j}(x_i - x_j).$$

We obtain a function

$$\mathrm{sgn}\colon S_n \to \{\pm 1\}.$$

This function satisfies, for $k < \ell$, $\mathrm{sgn}(\ (k\ell)\ ) = -1$: Let $\sigma = (k\ell)$ and consider the product

$$\prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)}) = (x_\ell - x_k) \prod_{\substack{i<j \\ i\neq k, j\neq \ell}} (x_{\sigma(i)} - x_{\sigma(j)}) \prod_{\substack{k<j \\ j\neq \ell}}(x_\ell - x_j) \prod_{\substack{i<\ell \\ i\neq k}}(x_i - x_k).$$

(This corresponds to the cases (i) $i = k, j = \ell$; (ii) $i \neq k, j \neq \ell$; (iii) $i = k, j \neq \ell (\Rightarrow j > k)$; (iv) $i \neq k, j = \ell (\Rightarrow i < \ell)$.) Counting the number of signs changes (note that case (ii) doesn't contribute at all!), we find that

$$\prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)}) = (-1)(-1)^{\sharp\{j:k<j<\ell\}}(-1)^{\sharp\{i:k<i<\ell\}}\prod_{i<j}(x_i - x_j) = -\prod_{i<j}(x_i - x_j).$$

It remains to show that sgn satisfies $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\cdot\mathrm{sgn}(\tau)$. We first make the seemingly innocuous observation that for *any* variables $y_1, \dots, y_n$ and for *any* permutation $\sigma$ we have

$$\prod_{i<j}(y_{\sigma(i)} - y_{\sigma(j)}) = \mathrm{sgn}(\sigma)\prod_{i<j}(y_i - y_j).$$

Let $\tau$ be a permutation. We apply this observation for the variables $y_i := x_{\tau(i)}$. We get

$$\begin{aligned}
\mathrm{sgn}(\tau\sigma)\cdot p(x_1, \dots, x_n) &= p(x_{\tau\sigma(1)}, \dots, x_{\tau\sigma(n)}) \\
&= p(y_{\sigma(1)}, \dots, y_{\sigma(n)}) \\
&= \mathrm{sgn}(\sigma)\cdot (y_1, \dots, y_n) \\
&= \mathrm{sgn}(\sigma)\cdot p(x_{\tau(1)}, \dots, x_{\tau(n)}) \\
&= \mathrm{sgn}(\sigma)\cdot\mathrm{sgn}(\tau)\cdot p(x_1, \dots, x_n).
\end{aligned}$$

This gives

$$\mathrm{sgn}(\tau\sigma) = \mathrm{sgn}(\tau)\cdot\mathrm{sgn}(\sigma).$$

□

**Calculating** sgn **in practice.** Recall that every permutation $\sigma$ can be written as a product of disjoint cycles

$$\sigma = (a_1 \dots a_\ell)(b_1 \dots b_m)\dots(f_1 \dots f_n).$$

**Lemma 2.4.3.** $\mathrm{sgn}(a_1 \dots a_\ell) = (-1)^{\ell-1}$.

*Proof.* We write

$$(a_1 \dots a_\ell) = \underbrace{(a_1 a_\ell)\dots(a_1 a_3)(a_1 a_2)}_{\ell-1 \text{ transpositions}}.$$

Since a transposition has sign $-1$ and sgn is a homomorphism, the claim follows. □

**Corollary 2.4.4.** $\mathrm{sgn}(\sigma) = (-1)^{\sharp\text{ even length cycles}}$.

[3]For example, if $n = 3$ and $\sigma$ is the cycle $(123)$ we have

$$(x_{\sigma(1)} - x_{\sigma(2)})(x_{\sigma(1)} - x_{\sigma(3)})(x_{\sigma(2)} - x_{\sigma(3)}) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3).$$

Hence, $\mathrm{sgn}(\ (1\,2\,3)\ ) = 1$.

**A Numerical example.** Let $n = 11$ and

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 5 & 4 & 3 & 1 & 7 & 8 & 10 & 6 & 9 \end{pmatrix}.$$

Then

$$\sigma = (1\,2\,5)(3\,4)(6\,7\,8\,10\,9).$$

Now,

$$\mathrm{sgn}(\ (1\,2\,5)\ ) = 1, \quad \mathrm{sgn}(\ (3\,4)\ ) = -1, \quad \mathrm{sgn}(\ (6\,7\,8\,10\,9)\ ) = 1.$$

We conclude that $\mathrm{sgn}(\sigma) = -1$.

**Realizing $S_n$ as linear transformations.** Let $\mathbb{F}$ be any field. Let $\sigma \in S_n$. There is a unique linear transformation

$$T_\sigma \colon \mathbb{F}^n \to \mathbb{F}^n,$$

such that

$$T_\sigma(e_i) = e_{\sigma(i)}, \quad i = 1, \dots n,$$

where, as usual, $e_1, \dots, e_n$ are the standard basis of $\mathbb{F}^n$. Note that

$$T_\sigma \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma^{-1}(1)} \\ x_{\sigma^{-1}(2)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{pmatrix}.$$

(For example, because $T_\sigma x_1 e_1 = x_1 e_{\sigma(1)}$, the $\sigma(1)$ coordinate is $x_1$, namely, in the $\sigma(1)$ place we have the entry $x_{\sigma^{-1}(\sigma(1))}$.) Since for every $i$ we have $T_\sigma T_\tau(e_i) = T_\sigma e_{\tau(i)} = e_{\sigma\tau(i)} = T_{\sigma\tau} e_i$, we have the relation

$$T_\sigma T_\tau = T_{\sigma\tau}.$$

The matrix representing $T_\sigma$ is the matrix $(a_{ij})$ with $a_{ij} = 0$ unless $i = \sigma(j)$. For example, for $n = 4$ the matrices representing the permutations $(12)(34)$ and $(1\,2\,3\,4)$ are, respectively

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Otherwise said,[4]

$$T_\sigma = \left(e_{\sigma(1)} \mid e_{\sigma(2)} \mid \dots \mid e_{\sigma(n)}\right) = \begin{pmatrix} e_{\sigma^{-1}(1)} \\ \hline e_{\sigma^{-1}(2)} \\ \hline \vdots \\ \hline e_{\sigma^{-1}(n)} \end{pmatrix}.$$

From the matrix representation of $T_\sigma$ we get

$$\det(T_\sigma) = \det\left(e_{\sigma(1)} \mid e_{\sigma(2)} \mid \cdots \mid e_{\sigma(n)}\right) = \mathrm{sgn}(\sigma) \det\left(e_1 \mid e_2 \mid \cdots \mid e_n\right) =$$
$$\mathrm{sgn}(\sigma) \det(I_n) = \mathrm{sgn}(\sigma).$$

[4]This gives the interesting relation $T_{\sigma^{-1}} = T_\sigma^t$. Because $\sigma \mapsto T_\sigma$ is a group homomorphism we may conclude that $T_\sigma^{-1} = T_\sigma^t$. Of course, for a general invertible matrix this doesn't hold – there is no reason for the inverse to be given by the transpose.

2.4.2. *Transpositions and generators for $S_n$.* For $1 \leq i < j \leq n$ we have the transposition $\sigma = (ij)$. Let $T$ be the set of all transpositions in $S_n$. $T$ has $n(n-1)/2$ elements and it generates $S_n$. In fact, the transpositions $(12), (23), \dots, (n-1\ n)$ alone generate $S_n$. We leave these facts as an exercise.

2.4.3. *The alternating group $A_n$.* Consider the set $A_n$ of all permutations in $S_n$ whose sign is 1. They are called the **even** permutations (those with sign $-1$ are called **odd**). We see that $e \in A_n$ and that if $\sigma, \tau \in A_n$ also $\sigma\tau$ and $\sigma^{-1}$ are in $A_n$. This follows from $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)$ and $\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)^{-1}$.

Thus, $A_n$ is a group. It is called the **alternating group**. For $n > 1$, it has $n!/2$ elements (use multiplication by $(12)$ to create a bijection between the odd and even permutations). Here are some examples

| $n$ | $A_n$ |
|---|---|
| 2 | $\{1\}$ |
| 3 | $\{1, (123), (132)\}$ |
| 4 | $\{1, (123), (132), (124), (142), (134), (143), (234), (243),$ $(12)(34), (13)(24), (14)(23)\}$ |

2.4.4. *A useful formula for conjugation.* Let $\sigma, \tau \in S_n$. There is a nice formula for $\tau\sigma\tau^{-1}$ (this is called conjugating $\sigma$ by $\tau$). If $\sigma$ is written as a product of cycles then the permutation $\tau\sigma\tau^{-1}$ is obtained by applying $\tau$ to the numbers appearing in the cycles of $\sigma$. That is, if $\sigma$ takes $i$ to $j$ then $\tau\sigma\tau^{-1}$ takes $\tau(i)$ to $\tau(j)$. Indeed,

$$\tau\sigma\tau^{-1}(\tau(i)) = \tau(\sigma(i)) = \tau(j).$$

Here is an example: say $\sigma = (1\ 4)(2\ 5)(3\ 7\ 6)$ and $\tau = (1\ 2\ 3\ 4)(6\ 7)$ then $\tau\sigma\tau^{-1} = (\tau(1)\ \tau(4))\ (\tau(2)\ \tau(5))\ (\tau(3)\ \tau(7)\ \tau(6)) = (2\,1)(3\,5)(4\,6\,7)$.

2.4.5. *The dihedral group as a subgroup of the symmetric group.* . Let $n \geq 3$. By encoding the action of the elements of $D_n$ on the $n$ vertices of the $n$-gon, we may view $D_n$ as a subgroup of $S_n$; indeed, every symmetry is completely determined by its action on the vertices. Thus,

$$x \mapsto (1\,2\ \cdots\ n),$$

and, if $n$ is even

$$y \mapsto (2\ n)(3\ n-1)\cdots(\frac{n}{2}\ \frac{n}{2}+2),$$

while if $n$ is odd

$$y \mapsto (2\ n)(3\ n-1)\cdots(\frac{n+1}{2}\ \frac{n+3}{2}).$$

2.5. **Matrix groups and the quaternions.** Let $R$ be a commutative ring with 1. We let $\mathrm{GL}_n(R)$ denote the $n \times n$ matrices with entries with $R$, whose determinant is a unit in $R$.

**Proposition 2.5.1.** $\mathrm{GL}_n(R)$ *is a group under matrix multiplication.*

For the proof we will use properties of the determinant, in particular that it is multiplicative. When you have proved it in MATH 251 you most likely assumed that the entries of the matrices belong to some field $R$. If you go back to your notes you will find that the proof applies whenever $R$ is a commutative ring. Similarly, for the adjoint matrix.

*Proof.* Multiplication of matrices is associative and the identity matrix is in $\mathrm{GL}_n(R)$. If $A, B \in \mathrm{GL}_n(R)$ then $\det(AB) = \det(A)\det(B)$ gives that $\det(AB)$ is a unit of $R$ and so $AB \in \mathrm{GL}_n(R)$. The adjoint matrix satisfies $\mathrm{Adj(A)}A = \det(A)I_n$ and so every matrix $A$ in $\mathrm{GL}_n(R)$ has an inverse equal to $\det(A)^{-1}\mathrm{Adj(A)}$. Note that $A^{-1}A = \mathrm{Id}$ implies that $\det(A^{-1}) = \det(A)^{-1}$, hence $\det(A^{-1})$ is an invertible element of $R$. Thus, $A^{-1}$ is in $\mathrm{GL}_n(R)$. □

**Proposition 2.5.2.** *Let $\mathbb{F}$ is a finite field of $q$ elements. The group $\mathrm{GL}_n(\mathbb{F})$ is a finite group of cardinality $(q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})$.*

*Proof.* To give a matrix in $\mathrm{GL}_n(\mathbb{F})$ is to give a basis of $\mathbb{F}^n$ (consisting of the columns of the matrix). The first vector $v_1$ in a basis can be chosen to be any non-zero vector in $\mathbb{F}^n$, and there are $q^n - 1$ such vectors. The second vector $v_2$ can be chosen to be any vector not in $\mathrm{Span}(v_1)$; there are $q^n - q$ such vectors. The third vector $v_3$ can be chosen to be any vector not in $\mathrm{Span}(v_1, v_2)$; there are $q^n - q^2$ such vectors. And so on. □

*Exercise* 2.5.3. Prove that the set of upper triangular matrices in $\mathrm{GL}_n(\mathbb{F})$, where $\mathbb{F}$ is any field, forms a subgroup of $\mathrm{GL}_n(F)$. It is also called a **Borel subgroup**. Prove that the set of upper triangular matrices in $\mathrm{GL}_n(\mathbb{F})$ with 1 on the diagonal, where $\mathbb{F}$ is any field, forms a subgroup of $\mathrm{GL}_n(F)$. It is also called a **unipotent subgroup**. Calculate the cardinality of these groups when $\mathbb{F}$ is a finite field of $q$ elements.

Let us change gears and consider the case $R = \mathbb{C}$, the complex numbers, and the set of eight matrices

$$\left\{\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \pm\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}, \pm\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}, \pm\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}\right\}.$$

One verifies that this is a subgroup of $\mathrm{GL}_2(\mathbb{C})$, called the **Quaternion group**. One can use the notation

$$\pm 1, \pm i, \pm j, \pm k$$

for the matrices, respectively. Then we have

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = i,\ ki = j.$$

Note that $Q$ is a non-abelian group of order 8.

2.6. **Direct product.** Let $G, H$ be two groups. Define on the cartesian product $G \times H$ multiplication by

$$m\colon (G \times H) \times (G \times H) \to G \times H, \quad m((a,x),(b,y)) = (ab, xy).$$

This makes $G \times H$ into a group, called the **direct product** (also direct sum) of $G$ and $H$.

One checks that $G \times H$ is abelian if and only if both $G$ and $H$ are abelian. The following relation among orders hold: $\mathrm{ord}((x,y)) = \mathrm{lcm}(\mathrm{ord}(x), \mathrm{ord}(y))$. It follows that if $G, H$ are cyclic groups whose orders are co-prime then $G \times H$ is also a cyclic group.

The construction generalizes easily to a product of finitely many groups $G_1 \times \cdots \times G_n$; the elements are vectors with coordinate-wise group operation. As a matter of notation, we write $G^2$ for $G \times G$ and, more generally, $G^n$ for $G \times \cdots \times G$ ($n$-times).

**Example 2.6.1.** If $H_1 < H, G_1 < G$ are subgroups then $H_1 \times G_1$ is a subgroup of $H \times G$. However, not every subgroup of $H \times G$ is of this form. For example, the subgroups of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are $\{0\} \times \{0\}, \{0\} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \{0\}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the subgroup $\{(0,0),(1,1)\}$ which is *not* a product of subgroups.

2.7. **Groups of small order.** One can show that in a suitable sense (namely, "up to isomorphism"; see § 7.1) the following is a complete list of groups for the given orders. In the middle column we give the abelian groups and in the right column the non-abelian groups. These groups are all familiar to us, except $T$, which will be discussed later.

| order | abelian groups | non-abelian groups |
|---|---|---|
| 1 | $\{1\}$ | |
| 2 | $\mathbb{Z}/2\mathbb{Z}$ | |
| 3 | $\mathbb{Z}/3\mathbb{Z}$ | |
| 4 | $(\mathbb{Z}/2\mathbb{Z})^2, \mathbb{Z}/4\mathbb{Z}$ | |
| 5 | $\mathbb{Z}/5\mathbb{Z}$ | |
| 6 | $\mathbb{Z}/6\mathbb{Z}$ | $S_3$ |
| 7 | $\mathbb{Z}/7\mathbb{Z}$ | |
| 8 | $(\mathbb{Z}/2\mathbb{Z})^3, \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}$ | $D_4, Q$ |
| 9 | $(\mathbb{Z}/3\mathbb{Z})^2, \mathbb{Z}/9\mathbb{Z}$ | |
| 10 | $\mathbb{Z}/10\mathbb{Z}$ | $D_5$ |
| 11 | $\mathbb{Z}/11\mathbb{Z}$ | |
| 12 | $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}$ | $D_6, A_4, T$ |

In the following table we list for every $n$ the number $G(n)$ of groups of order $n$ (this is taken from J. Rotman/*An introduction to the theory of groups*):

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $G(n)$ | 1 | 1 | 1 | 2 | 1 | 2 | 1 | 5 | 2 | 2 | 1 | 5 | 1 | 2 | 1 | 14 | 1 | 5 | 1 |

| $n$ | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $G(n)$ | 5 | 2 | 2 | 1 | 15 | 2 | 2 | 5 | 4 | 1 | 4 | 1 | 51 |

You may wish to consider the number of groups of order $n$ when $n$ is prime and form a conjecture. We will prove it shortly, in fact. Can you also make a conjecture when $n$ is a product of two primes? It may help you to know a few more values: $G(33) = G(35) = 1$ but $G(55) = 2$.

Asymptotically, the number of groups of order $p^n$, where $p$ is prime, is

$$p^{\frac{2}{27}n^3 + O(n^{8/3})}.$$

This is an asymptotic formula and it takes a while until it reflects the truth. For $n = 10$ it predicts that there should be about $2^{74} \sim 10^{22}$ groups of order 1024. The true number seems to be $49,487,365,422$, which is still very large! Here is the number of subgroups of order $2^n$ for small values of $n$ (from Wikipedia and Groupprops, June 2020)

| exponent $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| order $2^n$ | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 2018 |
| no. of groups | 1 | 1 | 2 | 5 | 14 | 51 | 267 | 2328 | 56092 | 10494213 | 49487365422 | unknown (!) |

## 3. Cosets and Lagrange's theorem

3.1. **Cosets.** Let $G$ be a group and $H$ a subgroup of $G$. A **left coset** of $H$ in $G$ is a subset $S$ of $G$ of the form

$$gH := \{gh : h \in H\},$$

for some $g \in G$. A **right coset** is a subset of $G$ of the form

$$Hg := \{hg : h \in H\},$$

for some $g \in G$. For brevity, we shall discuss only left cosets but the discussion with minor changes applies to right cosets as well.

**Example 3.1.1.** Consider the group $S_3$ and the subgroup $H = \{1, (12)\}$. The following table lists the left cosets of $H$. For an element $g$, we list the coset $gH$ in the middle column, and the coset $Hg$ in the last column.

| $g$ | $gH$ | $Hg$ |
|---|---|---|
| 1 | $\{1, (12)\}$ | $\{1, (12)\}$ |
| (12) | $\{(12), 1\}$ | $\{(12), 1\}$ |
| (13) | $\{(13), (123)\}$ | $\{(13), (132)\}$ |
| (23) | $\{(23), (132))\}$ | $\{(23), (123))\}$ |
| (123) | $\{(123), (13)\}$ | $\{(123), (23)\}$ |
| (132) | $\{(132), (23)\}$ | $\{(132), (13)\}$ |

TABLE 1. Cosets of $\langle (12) \rangle$

The first observation is that the element $g$ such that $S = gH$ is not unique. In fact, as the following lemma implies, $gH = kH$ if and only if $g^{-1}k \in H$. The second observation is that two left cosets are either equal or disjoint (but a left coset can intersect a right coset in a more complicated way); this is a consequence of the following lemma.

**Lemma 3.1.2.** *Define a relation $g \sim k$ if $\exists h \in H$ such that $gh = k$. This is an equivalence relation such that the equivalence class of $g$ is precisely $gH$.*

*Proof.* Since $g = ge$ and $e \in H$ the relation is reflexive. If $gh = k$ for some $h \in H$ then $kh^{-1} = g$ and $h^{-1} \in H$. Thus, the relation is symmetric. Finally, if $g \sim k \sim \ell$ then $gh = k, kh' = \ell$ for some $h, h' \in H$ and so $g(hh') = \ell$. Since $hh' \in H$ we conclude that $g \sim \ell$ and the relation is transitive. □

Thus, pictorially the cosets look like that:

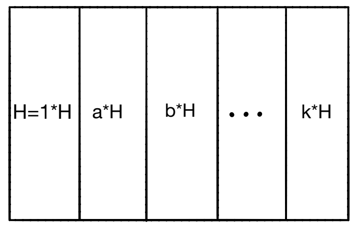



FIGURE 2. Cosets of a subgroup H.

*Remark* 3.1.3. One should note that in general $gH \neq Hg$; The table above provides an example. Moreover, $(13)H$ is not a right coset of $H$ at all. A difficult theorem of P. Hall asserts that given a finite group $G$ and a subgroup $H$ one can find a set $\{g_1, \dots, g_d\}$ of elements of $G$ such that $g_1H, \dots, g_dH$ are precisely the lest cosets of $H$, and $Hg_1, \dots, Hg_d$ are precisely the right cosets of $H$.

### 3.2. **Lagrange's theorem.**

**Theorem 3.2.1.** *Let $H < G$. The group $G$ is a disjoint union of left cosets of $H$. If $G$ is of finite order then the number of left cosets of $H$ in $G$ is $|G|/|H|$. We call the number of left cosets the* **index** *of $H$ in $G$ and denote it by $[G : H]$.*

*Proof.* We have seen that there is an equivalence relation whose equivalence classes are the cosets of $H$. Recall that different equivalence classes are always disjoint. Thus,

$$G = \dot\cup_{i=1}^{s} g_iH,$$

a disjoint union of $s$ cosets, where the $g_i$ are chosen appropriately. We next show that for every $x, y \in G$ the cosets $xH, yH$ have the same cardinality by producing a bijection between them.

Define a function

$$f : xH \to yH, \qquad f(g) = yx^{-1}g.$$

Note that $f$ is well defined: since $g = xh$ for some $h \in H$, $f(g) = yh$, which is an element of $yH$. Similarly, the function $f' : yH \to xH$, $f'(g) = xy^{-1}g$ is well-defined. Clearly, $f \circ f'$ and $f' \circ f$ are the identity functions of $yH$ and $xH$, respectively. This shows that $f$ is bijective and so $|xH| = |yH|$ for any $x, y \in G$. Thus, $|G| = s \cdot |H|$ and $s = [G : H] = |G|/|H|$. □

**Corollary 3.2.2.** *If $G$ is a finite group then $|H|$ divides $|G|$.*

*Remark* 3.2.3. The converse does not hold. The group $A_4$, which is of order 12, does not have a subgroup of order 6.

**Corollary 3.2.4.** *If $G$ is a finite group then* $\text{ord}(g) \mid |G|$ *for all $g \in G$.*

*Proof.* We saw that $\text{ord}(g) = |\langle g \rangle|$, so we may use Corollary 3.2.2. □

*Remark* 3.2.5. The converse does not hold. That is, if $n \mid |G|$ it does not follow that $G$ has an element of order $n$. In fact, if $G$ is not a cyclic group then there is no element $g \in G$ such that $\text{ord}(g) = |G|$.

**Corollary 3.2.6.** *If the order of $G$ is a prime number then $G$ is cyclic.*

*Proof.* From Corollary 3.2.4 we deduce that every element different from the identity has order equal to $|G|$. Thus, every such element generates the group. $\square$

**Example 3.2.7.** Consider the group $S_4$ and its subgroup $D_4$. There is no subgroup $J$ of $S_4$ such that $S_4 \supsetneq J \supsetneq D_4$. Indeed, from Lagrange's theorem we get

$$[S_4 : J][J : D_4] = [S_4 : D_4] = 3.$$

Thus, either $[S_4 : J] = 1$, in which case $J = S_4$, or $[J : D_4] = 1$, in which case $J = D_4$.

## 4. Cyclic groups

Let $G$ be a finite cyclic group of order $n$, $G = \langle g \rangle$.

### 4.1. Order of elements and subgroups.

**Lemma 4.1.1.** *We have* $\mathrm{ord}(g^a) = n/\gcd(a, n)$.

*Proof.* Note that $g^t = g^{t-n}$ and so $g^t = e$ if and only if $n|t$ (cf. Corollary 1.2.2). Thus, the order of $g^a$ is the minimal $r$ such that $ar$ is divisible by $n$. Clearly $a \cdot n/\gcd(a, n)$ is divisible by $n$ so the order of $g^a$ is less or equal to $n/\gcd(a, n)$. On the other hand if $ar$ is divisible by $n$ then, because $n = \gcd(a, n) \cdot n/\gcd(a, n)$ and $n/\gcd(a, n)$ is relatively prime to $a$, $r$ is divisible by $n/\gcd(a, n)$. $\square$

**Corollary 4.1.2.** *The element $g^a$ generates G, i.e. $\langle g^a \rangle = G$, if and only if $(a, n) = 1$. Thus, the number of generators of G is $\varphi(n) := \sharp\{1 \le a \le n : (a, n) = 1\}$, where $\varphi$ is Euler's function.*

**Proposition 4.1.3.** *For every $h|n$ the group G has a unique subgroup of order h. This subgroup is cyclic.*

*Proof.* We first show that every subgroup of $G$ is cyclic. Let $H$ be a non trivial subgroup. Then there is a minimal $0 < a < n$ such that $g^a \in H$ and hence $H \supseteq \langle g^a \rangle$. Let $g^r \in H$. We may assume that $r > 0$. Write $r = ka + k'$ for $0 \le k' < a$. Note that $g^{r-ka} \in H$. The choice of $a$ then implies that $k' = 0$. Thus, $H = \langle g^a \rangle$.

Since $\gcd(a, n) = \alpha a + \beta n$ for some integers $\alpha, \beta$, we have $g^{\gcd(a,n)} = (g^n)^\beta (g^a)^\alpha \in H$. Thus, $g^{a-\gcd(a,n)} \in H$. Therefore, by the choice of $a$, $a = \gcd(a, n)$; that is, $a|n$. Thus, every subgroup is cyclic and of the form $\langle g^a \rangle$ for an appropriate $a|n$. Its order is $n/a$. We conclude that for every $b|n$ there is a unique subgroup of order $b$ and it is cyclic, generated by $g^{n/b}$. $\square$

### 4.2. $\mathbb{F}^\times$ is cyclic.

**Lemma 4.2.1.** *Let n be a positive integer. We have the following identity for Euler's $\varphi$ function:*

$$n = \sum_{d|n} \varphi(d).$$

*(The summation is over positive divisors of n, including* 1 *and n.)*

*Proof.* Let $G$ be a cyclic group of order $n$. Then we have

$$\begin{aligned} n &= |G| \\ &= \sum_{1 \le d \le n} \sharp\{g \in G : \mathrm{ord}(g) = d\} \\ &= \sum_{d|n} \sharp\{g \in G : \mathrm{ord}(g) = d\}, \end{aligned}$$

where we have used that the order of an element divides the order of the group.

Now, if $h \in G$ has order $d$ it generates a subgroup of order $d$, which is in fact the unique subgroup of $G$ of that order. Therefore, it follows that all the elements of $G$ of order $d$ generate the same subgroup. That subgroup is a cyclic group of order $d$ and thus has $\varphi(d)$ generators (that are exactly the elements of $G$ of order $d$). The formula follows. ☐

**Proposition 4.2.2.** *Let $G$ be a finite group of order $n$ such that for $h|n$ the group $G$ has at most one subgroup of order $h$ then $G$ is cyclic.*

*Proof.* Consider an element $g \in G$ of order $h$. The subgroup $\langle g \rangle$ it generates is of order $h$ and has $\varphi(h)$ generators. We conclude that every element of order $h$ must belong to this subgroup (because there is a unique subgroup of order $h$ in $G$) and that there are exactly $\varphi(h)$ elements of order $h$ in $G$.

On the one hand $n = \sum_{d|n} \{\text{num. elts. of order } d\} = \sum_{d|n} \varphi(d)\epsilon_d$, where $\epsilon_d$ is 1 if there is an element of order $d$ in $G$ and is zero otherwise. But, by Lemma 4.2.1, $n = \sum_{d|n} \varphi(d)$. We conclude that $\epsilon_d = 1$ for all $d|n$ and, in particular, $\epsilon_n = 1$ and so there is an element of order $n$ in $G$. This element is a generator of $G$. ☐

**Corollary 4.2.3.** *Let $\mathbb{F}$ be a finite field then $\mathbb{F}^\times$ is a cyclic group.*

*Proof.* Let $q$ be the number of elements of $\mathbb{F}$. To show that for every $h$ dividing $q-1$ there is at most one subgroup of order $h$, we note that every element in that subgroup - call it $H$ - will have order dividing $h$ and hence will solve the polynomial $x^h - 1$. As a polynomial of degree $h$ in a field cannot have more than $h$ roots, the $h$ elements in that subgroup must be exactly the $h$ solutions of the polynomial $x^h - 1$. In particular, this subgroup is unique. ☐

The proof shows an interesting fact. If $\mathbb{F}$ is a field of $q$ elements, then $\mathbb{F}$ is the union of $\{0\}$ and the $q-1$ roots of $x^{q-1} - 1$, equivalently $\mathbb{F}$ is the solutions to the polynomial $x^q - x$. It's a general fact that $\mathbb{F}$ has some finite characteristic $p$, which is a prime, and that therefore $q$ is a power of $p$. Conversely, suppose that $L$ is a field of characteristic $p$ and the polynomial $x^q - x$ splits completely in $L$. Then $\mathbb{F} := \{a \in L : a^q - a = 0\}$ is a field with $q$ elements. Indeed, one only need to verify that this set is closed under addition, multiplication and inverse (multiplicative and additive). The only tricky one to check is addition. However, since for $p$ prime, $p | \binom{p}{i}$, $1 < i < p$, one concludes from the binomial theorem that $(x+y)^p = x^p + y^p$ in $L$ and, by iteration, that $(x+y)^q = x^q + y^q$ in $L$. This gives immediately that $\mathbb{F}$ is closed under addition.

*Remark* 4.2.4. Although the groups $(\mathbb{Z}/p\mathbb{Z})^\times$ are cyclic for every prime $p$, that doesn't mean we know an explicit generator. **Artin's primitive root conjecture** states that 2 is a generator for infinitely many primes $p$ (the conjecture is the same for any prime number instead of 2). Work starting with R. Murty and R. Gupta, and continued with K. Murty and Heath-Brown, had shown that for infinitely many primes $p$ either $2, 3$ or 5 are a primitive root.

# 5. Constructing subgroups

5.1. **Commutator subgroup.** Let $G$ be a group. Define its **commutator subgroup** $G'$, or $[G, G]$, to be the subgroup generated by $\{xyx^{-1}y^{-1}; x, y \in G\}$. An element of the form $xyx^{-1}y^{-1}$ is called a **commutator**. We use the notation $[x, y] = xyx^{-1}y^{-1}$. It is not true, in general, that every element in $G'$ is a commutator, though every element is a product of commutators, by definition.

**Example 5.1.1.** We calculate the commutator subgroup of $S_3$. First, note that every commutator is an even permutation, hence contained in $A_3$. Thus, $S_3' < A_3$. Next, $[(12),(13)] = (12)(13)(12)(13) = (123)$ is in $S_3'$. It follows that $S_3' = A_3$.

5.2. **Centralizer subgroup.** Let $H$ be a subgroup of $G$. We define its **centralizer** $\text{Cent}_G(H)$ to be the set $\{g \in G : gh = hg, \forall h \in H\}$. One checks that it is a subgroup of $G$ called **the centralizer of** $H$ **in** $G$.

Given an element $h \in G$ we may define $\text{Cent}_G(h) = \{g \in G : gh = hg\}$. It is a subgroup of $G$ called the **centralizer of** $h$ in $G$. One checks that $\text{Cent}_G(h) = \text{Cent}_G(\langle h \rangle)$ and that $\text{Cent}_G(H) = \cap_{h\in H}\text{Cent}_G(h)$.

Taking $H = G$, the subgroup $\text{Cent}_G(G)$ is the set of elements of $G$ such that each of them commutes with every other element of $G$. It has a special name; it is called the **center** of $G$ and denoted $Z(G)$. In this course we will not be using the centralizer of a proper subgroup much, but the centralizer of $G$, namely, its centre, will be often used.

**Example 5.2.1.** If $G$ is abelian then $G = Z(G) = \text{Cent}_G(H)$ for any subgroup $H < G$. If $H_1 \subseteq H_2 \subset G$ then $\text{Cent}_G(H_2) \subseteq \text{Cent}_G(H_1)$. If $G = G_1 \times G_2$ then $\text{Cent}_{G_1\times G_2}(G_1 \times \{1\}) = Z(G_1) \times G_2$ and, more generaly, $\text{Cent}_{G_1\times G_2}(H_1 \times H_2) = \text{Cent}_{G_1}(H_1) \times \text{Cent}_{G_2}(H_2)$.

**Example 5.2.2.** We calculate the centralizer of $(12)$ in $S_5$. First recall the useful observation from §2.4.4: $\tau\sigma\tau^{-1}$ is the permutation obtained from $\sigma$ by changing its entries according to $\tau$. For example: $(1234)[(12)(35)](1234)^{-1} = (1234)[(12)(35)](1432) = (1234)(1453) = (23)(45)$ and $(23)(45)$ is indeed obtained from $(12)(35)$ by changing the labels $1,2,3,4,5$ according to the rule $(1234)$.

Using this, we see that the centralizer of $(12)$ in $S_5$ is just $S_2 \times S_3$ – here $S_2$ are the permutations of $1,2$ and $S_3$ are the permutations of $3,4,5$. Viewed this way they are subgroups of $S_5$.

5.3. **Normalizer subgroup.** Let $H$ be a subgroup of $G$. Define the **normalizer** of $H$ in $G$, $N_G(H)$, to be the set $\{g \in G : gHg^{-1} = H\}$. It is a subgroup of $G$. Note that $H \subset N_G(H), \text{Cent}_G(H) \subset N_G(H)$ and $H \cap \text{Cent}_G(H) = Z(H)$.

**Example 5.3.1.** Consider $S_3 < S_4$. If $\tau \in N_{S_4}(S_3)$ then $\tau(123)\tau^{-1} \in S_3$ and so $\tau$ takes $1,2$ and $3$ to $1,2$ and $3$ (perhaps scrambling their order). Thus, $\tau \in S_3$. That is, $N_{S_4}(S_3) = S_3$.

## 6. Normal subgroups and quotient groups

Let $N < G$. We say that $N$ is a **normal** subgroup if for all $g \in G$ we have $gN = Ng$; equivalently, $gNg^{-1} = N$ for all $g \in G$; equivalently, $gN \subset Ng$ for all $g \in G$; equivalently, $gNg^{-1} \subset N$ for all $g \in G$. For example, if $gN \subset Ng$ for all $g$, then also $g^{-1}N \subset Ng^{-1}$, which gives $Ng \subset gN$. So it follows that $gN = Ng$.

We will use the notation $N \lhd G$ to signify that $N$ is a normal subgroup of $G$. Note that an equivalent way to say that $N \lhd G$ is to say that $N < G$ and $N_G(N) = G$.

**Example 6.0.1.** The group $A_3$ is normal in $S_3$. If $\sigma \in A_3$ and $\tau \in S_3$ then $\tau\sigma\tau^{-1}$ is an even permutation because its sign is $\text{sgn}(\tau)\text{sgn}(\sigma)\text{sgn}(\tau^{-1}) = \text{sgn}(\tau)^2\text{sgn}(\sigma) = 1$. Thus, $\tau A_3\tau^{-1} \subset A_3$. The same argument gives that $A_n \lhd S_n$.

The subgroup $H = \{1, (12)\}$ is not a normal subgroup of $S_3$. One can use Table 3.1.1 above to see that $(13)H \neq H(13)$. Or, use that $(13)(12)(13)^{-1} = (32)$.

**Construction of a quotient group:** Let $N \lhd G$. Let $G/N$ denote the set of left cosets of $N$ in $G$. We show that $G/N$ has a natural structure of a group; it is called the **quotient group** of $G$ by $N$.

Given two cosets $aN$ and $bN$ we define

$$aN * bN = abN.$$

We need to show this is well defined, because the formula seems to depend on the choice of representatives $a$ and $b$ to represent the cosets $aN, bN$. Suppose then that $aN = a'N$ and $bN = b'N$ then we must prove that $abN = a'b'N$. Now, we know that for suitable $\alpha, \beta \in N$ we have $a\alpha = a', b\beta = b'$. Thus, $a'b'N = a\alpha b\beta N = abb^{-1}\alpha b\beta N = ab(b^{-1}\alpha b)N$. Note that since $N \lhd G$ and $\alpha \in N$ also $b^{-1}\alpha b \in N$ and so $ab(b^{-1}\alpha b)N = abN$. This innocuous step – noting that $b^{-1}\alpha b \in N$ because $N$ is normal – is crucial. Indeed, if $N$ is not a normal subgroup the collection of cosets $G/N$ has no natural group structure.

One checks easily that $N = eN$ is the identity of $G/N$ and that $(gN)^{-1} = g^{-1}N$. (Note that $(gN)^{-1}$ - the inverse of the element $gN$ in the group $G/N$ is also the set $\{(gn)^{-1} : n \in N\} = Ng^{-1} = g^{-1}N$.)

**Definition 6.0.2.** A non-trivial group $G$ is called **simple** if its only normal subgroups are the trivial ones: $\{e\}$ and $G$.

*Remark* 6.0.3. We shall later prove that $A_n$ is a simple group for $n \geq 5$. By inspection, one finds that also $A_2$ and $A_3$ are simple. On the other hand $A_4$ is not simple. The "Klein 4 group" $V := \{1, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of $A_4$. The notation $V$ is customary, coming from the word "vier" (four, in German), but we will usually denote it $K$, for Klein.

**Abelianization.** Recall the definition of the commutator subgroup $G'$ of $G$ from §5.1. In particular, the notation $[x, y] = xyx^{-1}y^{-1}$. One easily checks that $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$ and that $[x, y]^{-1} = [y, x]$. Hence, also $g[x, y]^{-1}g^{-1} = [gxg^{-1}, gyg^{-1}]^{-1}$.

**Proposition 6.0.4.** *The subgroup $G'$ is normal in $G$. The group $G^{\mathrm{ab}} := G/G'$ is abelian (it is called the* **abelianization** *of $G$). Furthermore, if $N$ is a normal subgroup of $G$ and $G/N$ is abelian then $N \supseteq G'$.*

*Proof.* We know that $G' = \{[x_1, y_1]^{\epsilon_1} \cdots [x_r, y_r]^{\epsilon_r} : x_i, y_i \in G, \epsilon_i = \pm 1\}$. It follows that

$$gG'g^{-1} = \{[gx_1g^{-1}, gy_1g^{-1}]^{\epsilon_1} \cdots [gx_rg^{-1}, gy_rg^{-1}]^{\epsilon_r} : x_i, y_i \in G, \epsilon_i = \pm 1\} \subseteq G',$$

hence $G' \lhd G$.

For every $x, y \in G$ we have $xG' \cdot yG' = xyG' = xy(y^{-1}x^{-1}yx)G' = yxG' = yG' \cdot xG'$. Thus, $G/G'$ is abelian. If $G/N$ is abelian then for every $x, y \in G$ we have $xN \cdot yN = yN \cdot xN$. That is, $xyN = yxN$; equivalently, $x^{-1}y^{-1}xyN = N$. Thus, for every $x, y \in G$ we have $xyx^{-1}y^{-1} \in N$. So $N$ contains all the generators of $G'$ and therefore $N \supseteq G'$. □

**Example 6.0.5.** *Abelianization of $D_n$.* Recall that the dihedral group $D_n$ – the symmetries of a regular $n$-gon – is generated by $x, y$ subject to the relations $y^2 = x^n = yxyx = 1$. Let $H = \langle x^2 \rangle$. Note that if $n$ is odd, $H = \langle x \rangle$, while for $n$ even $H$ has index 2 in $\langle x \rangle$. We check first that $H$ is normal. Since $D_n$ is generated by $x, y$, it is enough to check that $H$ is closed under conjugation by these elements. Clearly $xHx^{-1} = H$, and the identity $yx^2y^{-1} = (yxy)^2 = x^{-2}$ implies that $yHy^{-1} = H$ too.

We next claim that in fact $H = D_n'$. First, since $x^2 = [y, x]^{-1}$ we have $H \subseteq D_n'$. To show equality it is enough to show that $D_n/H$ is abelian. Since $D_n/H$ is generated by the images $\bar{x}, \bar{y}$ of the elements $x, y$, it is enough to show that $\bar{x}$ and $\bar{y}$ commute. That is, that $[\bar{y}, \bar{x}]$ is the identity element; otherwise said, that $[y, x] \in H$. But $[y, x] = x^{-2} \in H$.

Note that for $n$ odd, the group $D_n^{\mathrm{ab}}$ has order 2 and so is isomorphic[5] to $\mathbb{Z}/2\mathbb{Z}$. For $n$ even, the group $D_n^{\mathrm{ab}}$ has order 4, and it is not hard to check that it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (under $\bar{x} \mapsto (1,0)$, $\bar{y} \mapsto (0,1)$, say).

**Example 6.0.6.** *Abelianization of the unipotent group.* Let $\mathbb{F}$ be a field and $n \geq 2$ an integer. Consider the unipotent group $N$ in $\mathrm{GL}_n(\mathbb{F})$ comprised all upper-triangular matrices with 1's along the diagonal. Let $H$ be the collection of matrices in $N$ that have 0's in all the $(i, i+1)$ entries. For example, for $n = 4$ we are talking about the groups

$$\begin{pmatrix} 1 & * & * & * \\ & 1 & * & * \\ & & 1 & * \\ & & & 1 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 1 & 0 & * & * \\ & 1 & 0 & * \\ & & 1 & 0 \\ & & & 1 \end{pmatrix}$$

We claim that $H = N'$. First we check that $H$ is normal in $N$. This is easily checked because, for instance,

$$\begin{pmatrix} 1 & a & * & * \\ & 1 & b & * \\ & & 1 & c \\ & & & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & * & * \\ & 1 & b' & * \\ & & 1 & c' \\ & & & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & * & * \\ & 1 & b+b' & * \\ & & 1 & c+c' \\ & & & 1 \end{pmatrix},$$

from which we deduce that also

$$\begin{pmatrix} 1 & a & * & * \\ & 1 & b & * \\ & & 1 & c \\ & & & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & * & * \\ & 1 & -b & * \\ & & 1 & -c \\ & & & 1 \end{pmatrix}.$$

Then, we quickly see that $H$ is normal and even that each commutator lies in $H$. To show that $H = N'$ more work is needed. I leave it as a (somewhat challenging) exercise. At the very least, I suggest you verify that for $n = 3$ (and that's not hard).

**Some lemmas about product and intersection of subgroups.**

**Lemma 6.0.7.** *Let $B$ and $N$ be subgroups of $G$, $N \lhd G$.*

1. *(1) $B \cap N$ is a normal subgroup of $B$.*
2. *(2) $BN := \{bn : b \in B, n \in N\}$ is a subgroup of $G$. Also, $NB$ is a subgroup of $G$. In fact, $BN = NB$.*
3. *(3) If $B \lhd G$ then $BN \lhd G$ and $B \cap N \lhd G$.*
4. *(4) If $B$ and $N$ are finite then $|BN| = |B||N|/|B \cap N|$. The same holds for $NB$.*

*Proof.* (1) $B \cap N$ is a normal subgroup of $B$: First $B \cap N$ is a subgroup of $G$, hence of $B$. Let $b \in B$ and $n \in B \cap N$. Then $bnb^{-1} \in B$ because $b, n \in B$ and $bnb^{-1} \in N$ because $N \lhd G$.

(2) $BN := \{bn : b \in B, n \in N\}$ is a subgroup of $G$: Note that $ee = e \in BN$. If $bn, b'n' \in BN$ then $bnb'n' = (bb') \cdot ((b')^{-1}nb')n' \in BN$. Finally, if $bn \in BN$ then $(bn)^{-1} = n^{-1}b^{-1} = b^{-1} \cdot bn^{-1}b^{-1} \in BN$.

Note that $BN = \cup_{b \in B} bN = \cup_{b \in B} Nb = NB$.

[5]For now think of "isomorphic" as "can be identified with".

(3) If $B \lhd G$ then $BN \lhd G$: We saw that $BN$ is a subgroup. Let $g \in G$ and $bn \in BN$ then $gbng^{-1} = (gbg^{-1})(gng^{-1}) \in BN$, using the normality of both $B$ and $N$. If $x \in B \cap N, g \in G$ then $gxg^{-1} \in B$ and $gxg^{-1} \in N$, because both are normal. Thus, $gxg^{-1} \in B \cap N$, which shows $B \cap N$ is a normal subgroup of $G$.

(4) If $B$ and $N$ are finite then $|BN| = |B||N|/|B \cap N|$: Define a map of *sets,*

$$f\colon B \times N \to BN, \qquad (b,n) \overset{f}{\mapsto} bn.$$

*to prove the assertion it is enough to prove that the fibre* $f^{-1}(x)$ *of any element* $x \in BN$ *has cardinality* $|B \cap N|$.

*Suppose that* $x = bn$, *then for every* $y \in B \cap N$ *we have* $(by)(y^{-1}n) = bn$. *This shows that* $f^{-1}(x) \supseteq \{(by, y^{-1}n) : y \in B \cap N\}$, *a set of* $|B \cap N|$ *elements. On the other hand, if* $bn = b_1 n_1$ *then* $y := b^{-1}b_1 = nn_1^{-1}$ *is in* $B \cap N$. *Note that* $b_1 = by$ *and* $n_1 = y^{-1}n$. *Thus,* $f^{-1}(x) = \{(by, y^{-1}n) : y \in B \cap N\}$. [6]

□

*Remark* 6.0.8. In general, if $B, N$ are subgroups of $G$ (that are not normal) then $BN$ need not be a subgroup of $G$. Indeed, consider the case of $G = S_3$, $B = \{1, (12)\}, N = \{1, (13)\}$ then $BN = \{1, (12), (13), (132)\}$ which is not a subgroup of $S_3$. Thus, in general $< B, N > \supset BN$ and equality does not hold. We can deduce though that

$$| < B, N > | \geq \frac{|B| \cdot |N|}{|B \cap N|}.$$

This is a very useful formula. Suppose, for example, that $(|B|, |N|) = 1$ then $|B \cap N| = 1$ because $B \cap N$ is a subgroup of both $B$ and $N$ and so by Lagrange's theorem $|B \cap N|$ divides both $|B|$ and $|N|$. In this case then $| < B, N > | \geq |B| \cdot |N|$. For example, we can conclude, with no computations at all, that any subgroup of order 3 of $A_4$ together with the Klein group $V$ generates $A_4$.

Recall that a group $G$ is called simple if it has no non-trivial normal subgroups. It follows from Lagrange's theorem that every group of prime order is simple. A group of odd order, which is not prime, is not simple (a very difficult theorem of Feit and Thompson). We shall later prove that the alternating group $A_n$ is a simple group for $n \geq 5$.

The classification of all finite simple groups is known. Most simple groups follows into a rather small number of families (such as the groups $A_n$ for $n \geq 5$). Outside those families there are finitely many simple groups, called the sporadic groups. John Conway, who passed away this year (2020) form COVID-19 complications, discovered several of them. The examples he found were obtained from symmetry groups of lattices in 24 dimensional space.

Another family of simple groups is the following: Let $\mathbb{F}$ be a finite field and let $\mathrm{SL}_n(\mathbb{F})$ be the group of $n \times n$ matrices with determinant 1. Let $T$ be the diagonal matrices with all elements on the diagonal being equal (hence the elements of $T$ are in bijection with solutions of $x^n = 1$ in $\mathbb{F}$); $T$ is the center of $\mathrm{SL}_n(\mathbb{F})$. Let $\mathrm{PSL}_n(\mathbb{F}) = \mathrm{SL}_n(\mathbb{F})/T$. This is almost always a simple group for $n \geq 2$ and any $\mathbb{F}$, the only exceptions being $n = 2$ and $\mathbb{F} \cong \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$. (See Rotman, op. cit., §8).

One can gain some understanding of the structure of a group from its normal subgroups. If $N \lhd G$ then we have a **short exact sequence**

$$1 \to N \to G \to G/N \to 1.$$

(That means that all the arrows are group homomorphisms and the image of an arrow is exactly the kernel of the next one.) Thus, one might hope that the knowledge of $N$ and $G/N$ allows one

[6] Note that we do not need to assume $BN$ is a subgroup. In particular, we do not need to assume that $B$ or $N$ are normal subgroups, only that they are subgroups.

to find the properties of $G$. This works best when the map $G \to G/N$ has a section, i.e., there is a homomorphism $f \colon G/N \to N$ such that $\pi_N \circ f = Id$. Then $G$ is a semi-direct product. We will come back to these ideas later on in the course.

# Part 2. The Isomorphism Theorems

## 7. HOMOMORPHISMS

It is a general principle in mathematics that when studying a particular class of objects one also considers maps between the objects and one requires the maps to respect the main properties of the objects. For example, maps between vector spaces are required to be *linear* – to respect addition of vectors and multiplication by scalar, two properties that are directly linked to the definition of vector spaces. Similarly, when studying posets (partially ordered sets) it is natural to look at maps $f\colon S \to T$ such that $s_1 < s_2$ implies $f(s_1) < f(s_2)$. As said, this is a general principle that is respected when studying rings, fields, modules, differential manifolds, graphs, etc.

7.1. **Basic definitions.** Let $G$ and $H$ be two groups. A **homomorphism**

$$f\colon G \to H$$

is a function satisfying

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

It is a consequence of the definition that $f(e_G) = e_H$ and that $f(a^{-1}) = f(a)^{-1}$.

A homomorphism is called an **isomorphism** if it is $1\colon 1$ and surjective. In that case, the set theoretic inverse function $f^{-1}$ is automatically a homomorphism too. Thus, $f$ is an isomorphism if and only if there exists a homomorphism $g\colon H \to G$ such that $h \circ g = id_G, g \circ h = id_H$.

Two groups, $G$ and $H$, are called **isomorphic** if there exists an isomorphism $f\colon G \to H$. We use the notation $G \cong H$. For all practical purposes two isomorphic groups should be considered as the same group. Being isomorphic is an equivalence relation on groups.

**Example 7.1.1.** Let $n \geq 2$. The sign map $\mathrm{sgn}\colon S_n \to \{\pm 1\}$ is a surjective group homomorphism.

**Example 7.1.2.** Let $G$ be a cyclic group of order $n$, say $G = \langle g \rangle$. The group $G$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$: Indeed, define a function $f\colon G \to \mathbb{Z}/n\mathbb{Z}$ by $f(g^a) = a$. Note that $f$ is well defined because if $g^a = g^b$ then $n|(b-a)$. It is a homomorphism: $g^a g^b = g^{a+b}$. It is easy to check that $f$ is surjective. It is injective, because $f(g^a) = 0$ implies that $n|a$ and so $g^a = g^0 = e$ in the group $G$.

**Example 7.1.3.** We have an isomorphism $S_3 \cong D_3$ coming from the fact that a symmetry of a triangle (an element of $D_3$) is completely determined by its action on the vertices.

**Example 7.1.4.** The Klein four group $V = \{1, (12)(34), (13)(24), (14)(23)\}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ by $(12)(34) \mapsto (0,1),\ (13)(24) \mapsto (1,0),\ (14)(23) \mapsto (1,1)$.

The **kernel** $\mathrm{Ker}(f)$ of a homomorphism $f\colon G \to H$ is by definition the set

$$\mathrm{Ker}(f) = \{g \in G : f(g) = e_H\}.$$

For example, the kernel of the sign homomorphism $S_n \to \{\pm 1\}$ is the alternating group $A_n$.

**Lemma 7.1.5.** *The set* $\mathrm{Ker}(f)$ *is a normal subgroup of* $G$; $f$ *is injective if and only if* $\mathrm{Ker}(f) = \{e\}$. *For every* $h \in H$, *the preimage* $f^{-1}(h) := \{g \in G : f(g) = h\}$ *is a coset of* $\mathrm{Ker}(f)$.

*Proof.* First, since $f(e) = e$ we have $e \in \mathrm{Ker}(f)$. If $x, y \in \mathrm{Ker}(f)$ then $f(xy) = f(x)f(y) = ee = e$ so $xy \in \mathrm{Ker}(f)$ and $f(x^{-1}) = f(x)^{-1} = e^{-1} = e$ so $x^{-1} \in \mathrm{Ker}(f)$. That shows that $\mathrm{Ker}(f)$ is a subgroup. If $g \in G, x \in \mathrm{Ker}(f)$ then $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)ef(g)^{-1} = e$. Thus, $\mathrm{Ker}(f) \lhd G$.

If $f$ is injective then there is a unique element $x$ such that $f(x) = e$. Thus, $\mathrm{Ker}(f) = \{e\}$. Suppose that $\mathrm{Ker}(f) = \{e\}$ and $f(x) = f(y)$. Then $e = f(x)f(y)^{-1} = f(xy^{-1})$ so $xy^{-1} = e$. That is $x = y$ and $f$ is injective.

More generally, note that $f(x) = f(y)$ iff $f(x^{-1}y) = e$ iff $x^{-1}y \in \mathrm{Ker}(f)$ iff $y \in x\mathrm{Ker}(f)$. Thus, if $h \in H$ and $f(x) = h$ then the fibre $f^{-1}(h)$ is precisely $x\mathrm{Ker}(f)$. □

**Lemma 7.1.6.** *If $N \lhd G$ then the canonical map $\pi_N \colon G \to G/N$, given by $\pi_N(a) = aN$, is a surjective homomorphism with kernel $N$.*

*Proof.* We first check that $\pi = \pi_N$ is a homomorphism: $\pi(ab) = abN = aNbN = \pi(a)\pi(b)$. Since every element of $G/N$ is of the form $aN$ for some $a \in G$, $\pi$ is surjective. Finally, $a \in \mathrm{Ker}(\pi)$ iff $\pi(a) = aN = N$ (the identity element of $G/N$) iff $a \in N$. □

**Corollary 7.1.7.** *A subgroup $N < G$ is normal if and only if it is the kernel of a homomorphism.*

**Example 7.1.8.** Let $\mathbb{F}$ be a field and $n \geq 1$ an integer. The determinant map

$$\det \colon \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}^\times,$$

is a surjective homomorphism. Its kernel, called $\mathrm{SL}_n(\mathbb{F})$ (GL stands for General Linear and SL for Special Linear), namely the matrices of determinant 1, is a normal subgroup.

**Example 7.1.9.** We construct a surjective homomorphism

$$f \colon S_4 \to S_3.$$

Let $T = \{(12)(34), (13)(24), (14)(23)\}$. For every $\sigma \in S_4$ we have $\sigma(ij)(kl)\sigma^{-1} = (\sigma(i)\,\sigma(j))(\sigma(k)\,\sigma(l))$ and so $S_4$ acts on $T$ by conjugation. As such, every $\sigma$ induces a permutation of the elements in $T$. As $T$ has three elements, we therefore get a homomorphism

$$f \colon S_4 \to S_3.$$

We claim that this homomorphism is surjective. For this, test the effect of permutations of the form $(abc)$ on $T$, as well as permutations of the form $(ab)$, to see that we get all the permutations in $S_3$. The kernel $K$ of this homomorphism consists of permutations $\sigma$ such that

$$\sigma(ij)(kl)\sigma^{-1} = (\sigma(i)\,\sigma(j))(\sigma(k)\,\sigma(l)) = (ij)(kl).$$

One can check by hand that the Klein group $V = \{1\} \cup T$ acts trivially on the elements of $T$ and so $V \subset K$. It will follow from the first isomorphism theorem that $K$ has 4 elements and so one concludes that $V = K$.

7.2. **Behavior of subgroups under homomorphisms.** The following proposition describes the behaviour of subgroups under homomorphisms.

**Proposition 7.2.1.** *Let*

$$f \colon G \to H$$

*be a group homomorphism. The following holds*

(1) *If $A < G$ then $f(A) < H$, in particular $f(G) < H$.*
(2) *If $B < H$ then $f^{-1}(B) < G$. Furthermore, if $B \lhd H$ then $f^{-1}(B) \lhd G$.*
(3) *If, moreover, $f$ is surjective, then $A \lhd G$ implies $f(A) \lhd H$.*

*Proof.* Since $f(e) = e$ we have $e \in f(A)$. Furthermore, the identities $f(x)f(y) = f(xy)$, $f(x)^{-1} = f(x^{-1})$ show that $f(A)$ is closed under multiplication and inverses. Thus, $f(A)$ is a subgroup.

Let $B < H$. Since $f(e) = e$ we see that $e \in f^{-1}(B)$. Let $x, y \in f^{-1}(B)$ then $f(xy) = f(x)f(y) \in B$ because both $f(x)$ and $f(y)$ are in $B$. Thus, $xy \in f^{-1}(B)$. Also, $f(x^{-1}) = f(x)^{-1} \in B$ and so $x^{-1} \in f^{-1}(B)$. This shows that $f^{-1}(B) < G$.

Suppose now that $B \lhd H$. Let $x \in f^{-1}(B), g \in G$. Then $f(gxg^{-1}) = f(g)f(x)f(g)^{-1}$. Since $f(x) \in B$ and $B \lhd H$ it follows that $f(g)f(x)f(g)^{-1} \in B$ and so $gxg^{-1} \in f^{-1}(B)$. Thus, $f^{-1}(B) \lhd G$.

The last claim follows with similar arguments. $\square$

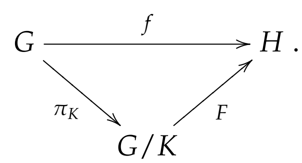
*Remark* 7.2.2. It is not necessarily true that if $A \lhd G$ then $f(A) \lhd H$. For example, consider $G = \{1, (12)\}$ with its embedding into $S_3$.

## 8. The first isomorphism theorem

There are several isomorphism theorems, or so they are called, but a better way to understand this material is to understand really well the first isomorphism theorem and think about the other isomorphism theorems as applications, or consequences.

**Theorem 8.0.1.** *(***The First Isomorphism Theorem***) Let $f\colon G \to H$ be a homomorphism of groups. Let $N$ be the kernel of $f$ and $K$ a normal subgroup of $G$ that is contained in $N$.*

*There is a unique homomorphism $F\colon G/K \to H$ such that the following diagram commutes:*[7]




*Furthermore,* $\mathrm{Ker}(F) = N/K$*.*

*Proof.* Define

$$F\colon G/K \to H, \qquad F(bK) = f(b).$$

This is a well-defined function: If $bK = cK$ then $b = ck$ for some $k \in K \subset N = \mathrm{Ker}(f)$ and so $f(b) = f(ck) = f(c)f(k) = f(c)$. The map $F$ is a homomorphism as $F(bK \cdot dK) = F(bdK) = f(bd) = f(b)f(d) = F(bK)F(dK)$. By construction, we have

$$F(\pi_K(b)) = F(bK) = f(b),$$

and the diagram is therefore commutative. Note, that since the map $\pi_K$ is surjective, there is a unique function $F$ that could make the diagram commutative; that is, $F$ is a unique.

Finally, $bK \in \mathrm{Ker}(F)$ if and only if $f(b) = 1_H$; namely, if and only if $b \in N$. Thus, the kernel are cosets of the form $bK$, where $b \in N$; otherwise said, $\mathrm{Ker}(F) = N/K$. $\square$

**Corollary 8.0.2.** *Let $f\colon G \to H$ be a homomorphism of groups. Then*

$$G/\mathrm{Ker}(f) \cong H.$$

*Proof.* Indeed, from the commutativity of the diagram we conclude that $F\colon G/\mathrm{Ker}(f) \cong H$ is surjective. On the other hand, its kernel is $\mathrm{Ker}(f)/\mathrm{Ker}(f)$, which is just the identity element of $G/\mathrm{Ker}(f)$. Thus, $F$ is a bijective homomorphism. $\square$

**Example 8.0.3.** Let $m, n$ be positive integers such that $(m, n) = 1$. Consider the homomorphism

$$f\colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \qquad f(x) = (x \mod m, x \mod n).$$

The kernel of $f$ is $mn\mathbb{Z}$ and by the first isomorphism theorem we get an injective map

$$F\colon \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

As both sides have cardinality $mn$, the homomorphism $F$ is also surjective. We get the familiar **Chinese Remainder Theorem**:

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \quad (m, n) = 1.$$

[7] That means that $F \circ \pi_K = f$.

**Example 8.0.4.** Let $\mathbb{F}$ be a field and consider the $3 \times 3$ unipotent group

$$N = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{F} \right\}.$$

The function

$$f \colon N \to \mathbb{F} \times \mathbb{F},$$

where $\mathbb{F} \times \mathbb{F}$ is considered as an abelian group with coordinate-wise addition, is a surjective homomorphism whose kernel are the matrices

$$K = \left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : c \in \mathbb{F} \right\}.$$

In fact $K$ is the commutator subgroup of $N$ (cf. Example 6.0.6). At any rate, we find that

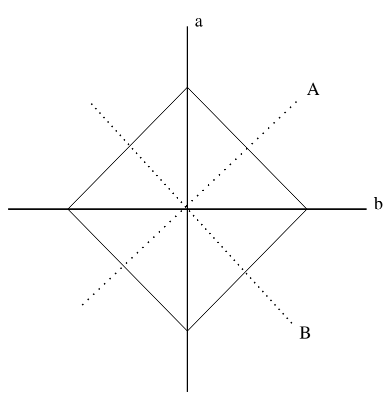
$$N/K \cong \mathbb{F} \times \mathbb{F}.$$

**Example 8.0.5.** We complete Example 7.1.9. As the homomorphism $f$ constructed there is surjective, we have $S_4/\mathrm{Ker}(f) \cong S_3$. As $S_3$ has 6 elements, it follows that $\mathrm{Ker}(f)$ has 4 elements and, as we have already observed, it contains the Klein group. Thus, $\mathrm{Ker}(f) = V$.

**Example 8.0.6.** Let us construct two homomorphisms

$$f_i \colon D_4 \to S_2.$$

We get the first homomorphism $f_1$ be looking at the action of the symmetries on the axes $\{a, b\}$.




Thus, $f_1(x) = (ab), f_1(y) = 1$ ($x$ permutes the axes, while $y$ fixes the axes – though not pointwise). Similarly, if we let $A, B$ be the lines whose equation is $a = b$ and $a = -b$, then $D_4$ acts as permutations on $\{A, B\}$ and we get a homomorphism $f_2 \colon D_4 \to S_2$ such that $f_2(x) = (AB), f_2(y) = (AB)$.

The homomorphism $f_i$, for $i = 1, 2$, is surjective and therefore the kernel $N_i = \mathrm{Ker}(f_i)$ has 4 elements. We find that $N_1 = \{1, x^2, y, x^2y\}$ and $N_2 = \{1, x^2, xy, x^3y\}$. By the first isomorphism theorem we have $D_4/N_i \cong S_2$.

Now, quite generally, if $g_i \colon G \to H_i$ are group homomorphisms then $g \colon G \to H_1 \times H_2$, defined by $g(r) = (g_1(r), g_2(r))$ is a group homomorphism with kernel $\mathrm{Ker}(g_1) \cap \mathrm{Ker}(g_2)$. One uses the notation $g = (g_1, g_2)$. Applying this to our situation, we get a homomorphism

$$f = (f_1, f_2) \colon D_4 \to S_2 \times S_2,$$

whose kernel is $\{1, x^2\}$. It follows that the image of $f$ has 4 elements and hence $f$ is surjective. That is,

$$D_4/\langle x^2\rangle \cong S_2 \times S_2.$$

**Example 8.0.7.** A homomorphism, especially if it is injective, could serve to realize more concretely a group that is initially defined rather abstractly. We have already done so, without making a big deal of it. Recall that $D_n$ was defined as the group of symmetries of a regular $n$-gon. By enumerating the vertices we realized $D_n$ as a subgroup of $S_n$. In effect, we have constructed an injective homomorphism $D_n \to S_n$ under which

$$y \mapsto (1)(2\ n)(3\ n-1)\cdots, \quad x \mapsto (1\ 2\ 3\cdots n).$$

**Example 8.0.8.** Consider the group $G = \mathrm{GL}_3(\mathbb{F}_2)$, a group with $168 = (8-1)(8-2)(8-4)$ elements. This is a famous group in fact, being the only simple group (namely a group with no non-trivial normal subgroups) of order 168; All other simple groups of order less than 168 are either the cyclic abelian groups of prime order or the alternating group $A_5$ of order 60. By considering the action of $G$ on $\mathbb{F}_2^3$ – the vector space of dimension 3 over $\mathbb{F}_2$ – or more precisely, just its action on the 7 non-zero vectors $\mathbb{F}_2^3 - \{0\}$ we get an injective group homomorphism $\mathrm{GL}_3(\mathbb{F}_2) \hookrightarrow S_7$, where $S_7$ is interpreted as the permutations of $\mathbb{F}_2^3 - \{0\}$.

Now, the only element of order 7 of $S_7$ up to conjugation is a cycle of length 7 and, clearly, it acts transitively on $\mathbb{F}_2^3 - \{0\}$. It will follow from theorems we shall prove later that since $7|168$ the group $G$ must have an element of order 7. We can therefore conclude that there is a matrix in $\mathrm{GL}_3(\mathbb{F}_2)$ of order 7 and that matrix permutes cyclically the non-zero vectors of the space. Can you find such a matrix??

**Example 8.0.9.** Let $G$ be an abelian group and fix an integer $n$. Consider the two sets

$$G[n] := \{g \in G : g^n = 1_G\}, \quad G^n := \{g^n : g \in G\}.$$

Making use of the fact that $G$ is abelian one easily checks that these are subgroups. If $G$ is not abelian this need not be true. For example, take $G = S_3$ and $n = 2$. Then $S_3[2] = \{1, (12), (13), (23)\}$ which is not a subgroup. In this case $S_3^2 = \{(1), (123), (132)\}$ is a subgroup, but if we take $n = 3$ we find that $S_3^3 = \{1, (12), (13), (23)\}$, which is not a subgroup.

Getting back to the case where $G$ is abelian, we notice that we have a surjective homomorphism:

$$[n]\colon G \to G^n, \quad [n](g) := g^n.$$

The kernel of this homomorphism is $G[n]$ and so, using the first isomorphism theorem, we conclude

$$G/G[n] \cong G^n.$$

Here is a simple application. Suppose that $p \equiv 2 \pmod 3$ then the equation $x^3 - a \equiv 0 \pmod p$ has a unique solution for every non-zero congruence class $a$. Indeed, since $3 \nmid (p-1)$, there are no elements of order 3 in the group $\mathbb{Z}/p\mathbb{Z}^\times$. Thus, $(\mathbb{Z}/p\mathbb{Z}^\times)^3 = \mathbb{Z}/p\mathbb{Z}^\times$, that is, every element is a cube.[8] But more is true; since the kernel of the homomorphism $[3]\colon \mathbb{Z}/p\mathbb{Z}^\times \to \mathbb{Z}/p\mathbb{Z}^\times, g \mapsto g^3$ is trivial in this case, every $a$ is obtained from a unique $g$ as $a = g^3$. That is, we have a unique solution.

[8] We apologize for the confusing notation: here $(\mathbb{Z}/p\mathbb{Z}^\times)^3$ refers to the third powers of elements in $\mathbb{Z}/p\mathbb{Z}^\times$, as in the notation $G^n$, and not to the cartesian product of $\mathbb{Z}/p\mathbb{Z}^\times$ with itself three times.

## 9. The second isomorphism theorem

**Theorem 9.0.1.** *Let $G$ be a group. Let $B < G, N \lhd G$. Then*
$$BN/N \cong B/(B \cap N).$$

*Proof.* Recall from Lemma 6.0.7 that $BN$ is a group and $N$ is a normal subgroup in it. Define a homomorphism $B \to BN/N$ as the composition of the homomorphisms $B \hookrightarrow BN \to BN/N$. That is, we have a homomorphism
$$f\colon B \to BN/N, \quad f(b) = bN.$$
Every element $x$ of $BN/N$ is of the form $bnN$ with some $b \in B, n \in N$. As $bnN = bN$ we find that $f(b) = x$ and therefore $f$ is surjective. We also have $f(b) = bN = e_{BN/N}$ if and only if $b \in N$. But then clearly $b \in B \cap N$. Thus, $\mathrm{Ker}(f) = B \cap N$ and the first isomorphism theorem gives the isomorphism $B/B \cap N \cong BN/N$. □

*Remark* 9.0.2. This is often used as follows: Let $f\colon G \to H$ be a group homomorphism with kernel $N$. Let $B < G$. What can we say about the image of $B$ under $f$? Well $f(B) = f(BN)$ and $f\colon BN \to H$ has kernel $N$. We conclude that $f(B) \cong BN/N \cong B/(B \cap N)$.

As a concrete example, consider $B = S_3 \subset S_4$ (realized as the permutations fixing 4) and the homomorphism $f\colon S_4 \to S_3$ constructed in Examples 7.1.9, 8.0.5. We have $f(S_3) \cong S_3/V \cap S_3$ where $V$ is the Klein group and equal to the kernel of $f$. As every non-trivial element of $V$ moves 4, we have $S_3 \cap V = \{1\}$. We conclude that under the isomorphism $f$ we have $f(S_3) \cong S_3$.

## 10. The third isomorphism theorem

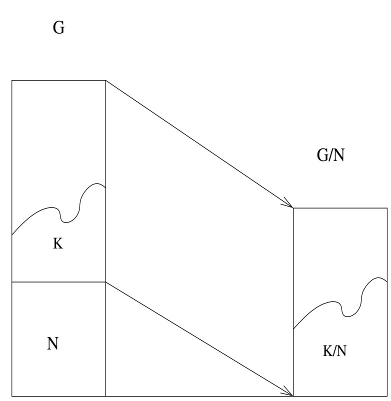
In the following theorem we have put together statements that are sometimes divided into two theorems, called the Third Isomorphism Theorem and the Correspondence Theorem.

**Theorem 10.0.1.** *Let $f\colon G \to H$ be a surjective homomorphism of groups.*

*(1) $f$ induces a bijection:*
$$\{\text{subgps of } G \text{ containing } \mathrm{Ker}(f)\} \quad \leftrightarrow \quad \{\text{subgps of } H\}.$$
*Given by $G_1 \mapsto f(G_1)$, $G_1 < G$, and in the other direction by $H_1 \mapsto f^{-1}(H_1)$, $H_1 < H$.*

*(2) Suppose that $\mathrm{Ker}(f) < G_1 < G_2$. Then $G_1 \lhd G_2$ if and only if $f(G_1) \lhd f(G_2)$. Moreover, in that case,*
$$G_2/G_1 \cong f(G_2)/f(G_1).$$

*(3) Let $N < K < G$ be groups, such that $N \lhd G, K \lhd G$. Then*
$$(G/N)/(K/N) \cong G/K.$$



*Proof.* We proved in general (Prop. 7.2.1) that if $G_1 < G$ then $f(G_1) < H$ and if $H_1 < H$ then $f^{-1}(H_1) < G$. Since $f$ is a surjective map we have $f(f^{-1}(H_1)) = H_1$. We need to show that if $\mathrm{Ker}(f) < G_1$ then $f^{-1}(f(G_1)) = G_1$. Clearly $f^{-1}(f(G_1)) \supseteq G_1$. Let $x \in f^{-1}(f(G_1))$ then $f(x) \in f(G_1)$. Choose then $g \in G_1$ such that $f(g) = f(x)$ and write $x = g(g^{-1}x)$. Note that $f(g^{-1}x) = e_H$ and so $g^{-1}x \in \mathrm{Ker}(f) \subseteq G_1$. Thus, $x = g(g^{-1}x) \in G_1$.

Consider the restriction of $f$ to $G_2$ as a surjective group homomorphism $f\colon G_2 \to f(G_2)$. We proved under those conditions that if $G_1 \lhd G_2$ then $f(G_1) \lhd f(G_2)$. If $f(G_1) \lhd f(G_2)$ then we also proved that $f^{-1}(f(G_1)) \lhd G_2$. Since $G_1 \supset \mathrm{Ker}(f)$ we have $f^{-1}(f(G_1)) = G_1$.

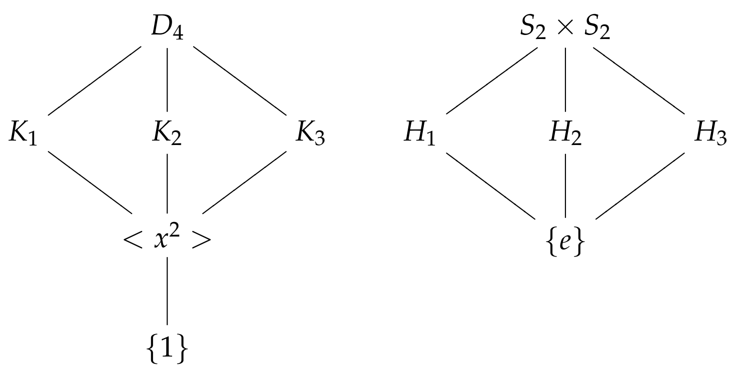
It remains to show that if $\mathrm{Ker}(f) < G_1 \lhd G_2$ then $G_2/G_1 \cong f(G_2)/f(G_1)$. The homomorphism obtained by composition

$$G_2 \to f(G_2) \to f(G_2)/f(G_1),$$

is surjective and has kernel $f^{-1}(f(G_1)) = G_1$. The claim now follows from the First Isomorphism Theorem.

We apply the previous results in the case where $H = G/N$ and $f\colon G \to G/N$ is the canonical map. We consider the case $G_1 = K, G_2 = G$. Then $G/K \cong f(G)/f(K) = (G/N)/(K/N)$. □

**Example 10.0.2.** Consider again the group homomorphism $f\colon D_4 \to S_2 \times S_2$ constructed in Example 8.0.6. Using the Third Isomorphism Theorem we conclude that the graph of the subgroups of $D_4$ containing $< x^2 >$ is exactly that of $S_2 \times S_2$ (analyzed in Example 2.6.1). Hence we have:




We'll see later that this does not exhaust the list of subgroups of $D_4$. Here we have

$K_1 =< x >$,
$K_2 =< y, x^2 >$,
$K_3 =< xy, x^2 >$

and

$H_1 = f(K_1) = \{(1,1), ((ab), (AB))\}$,
$H_2 = f(K_2) = \{(1,1), (1, (AB))\}$,
$H_3 = f(K_3) = \{(1,1), ((ab), 1)\}$.

**Example 10.0.3.** Let $\mathbb{F}$ be a field and let $N = \{\mathrm{diag}[f, f, \dots, f] : f \in \mathbb{F}^\times\}$ be the set of diagonal matrices with the same non-zero element in each diagonal entry. In fact, $N = Z(\mathrm{GL}_n(\mathbb{F}))$ and is therefore a normal subgroup. The quotient group

$$\mathrm{PGL}_n(\mathbb{F}) := \mathrm{GL}_n(\mathbb{F})/N$$

is called the projective linear group.

Let $\mathbb{P}^{n-1}(\mathbb{F})$ be the set of equivalence classes of non-zero vectors in $\mathbb{F}^n$ under the equivalence $v \sim w$ if there is $f \in \mathbb{F}^*$ such that $fv = w$; that is, the set of lines through the origin. The set $\mathbb{P}^{n-1}(\mathbb{F})$ is called the $(n-1)-$**dimensional projective space**. The importance of the group $\mathrm{PGL}_n(\mathbb{F})$ is that it acts as automorphisms on the projective $(n-1)$-space $\mathbb{P}^{n-1}(\mathbb{F})$: If we denote the class of a matrix $A$ in $\mathrm{PGL}_n(\mathbb{F})$ by $[A]$, say, and the class of vector $v$ in $\mathbb{P}^{n-1}(\mathbb{F})$ by $[v]$ then the action is given by $[A][v] = [Av]$. (Check this is well-defined!).

Let

$$\pi\colon \mathrm{GL}_n(\mathbb{F}) \to \mathrm{PGL}_n(\mathbb{F})$$

be the canonical homomorphism. The function

$$\det\colon \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}^*$$

is a group homomorphism, whose kernel, the matrices with determinant one, is denoted $\mathrm{SL}_n(\mathbb{F})$. Consider the image of $\mathrm{SL}_n(\mathbb{F})$ in $\mathrm{PGL}_n(\mathbb{F})$; it is denoted $\mathrm{PSL}_n(\mathbb{F})$. We want to analyze it and the quotient $\mathrm{PGL}_n(\mathbb{F})/\mathrm{PSL}_n(\mathbb{F})$.

The group $\mathrm{PSL}_n(\mathbb{F})$ is equal to $\pi(\mathrm{SL}_n(\mathbb{F})) = \pi(\mathrm{SL}_n(\mathbb{F})N)$ and is therefore isomorphic to $\mathrm{SL}_n(\mathbb{F})N/N \cong \mathrm{SL}_n(\mathbb{F})/\mathrm{SL}_n(\mathbb{F}) \cap N = \mathrm{SL}_n(\mathbb{F})/\mu_n(\mathbb{F})$, where by $\mu_n(\mathbb{F})$ we mean the group $\{f \in \mathbb{F}^\times : f^n = 1\}$ (where we identify $f$ with $\mathrm{diag}[f, f, \dots, f]$). Therefore,

$$\mathrm{PSL}_n(\mathbb{F}) \cong \mathrm{SL}_n(\mathbb{F})/\mu_n(\mathbb{F}).$$

We have $\mathrm{PGL}_n(\mathbb{F})/\mathrm{PSL}_n(\mathbb{F}) \cong (\mathrm{GL}_n(\mathbb{F})/N)/(\mathrm{SL}_n(\mathbb{F})N/N) \cong \mathrm{GL}_n(\mathbb{F})/\mathrm{SL}_n(\mathbb{F})N$. Let $\mathbb{F}^{\times(n)}$ be the subgroup of $\mathbb{F}^\times$ consisting of the elements $\{f^n : f \in \mathbb{F}^\times\}$. Under the isomorphism $\mathrm{GL}_n(\mathbb{F})/\mathrm{SL}_n(\mathbb{F}) \cong \mathbb{F}^\times$ the subgroup $\mathrm{SL}_n(\mathbb{F})N$ corresponds to $\mathbb{F}^{\times(n)}$. We conclude that

$$\mathrm{PGL}_n(\mathbb{F})/\mathrm{PSL}_n(\mathbb{F}) \cong \mathbb{F}^\times/\mathbb{F}^{\times(n)}.$$

**Example 10.0.4.** We return to Example 8.0.4. We constructed a surjective homomorphism

$$f\colon N \to \mathbb{F} \times \mathbb{F},$$

with kernel

$$K = \left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : c \in \mathbb{F} \right\}.$$

Assume that $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$. What are the subgroups of $N$ that contain $K$?

By the Third Isomorphism Theorem, they are in bijection with the subgroups of $\mathbb{F} \times \mathbb{F}$. Besides the trivial subgroups $\{(0,0)\}$ and $\mathbb{F} \times \mathbb{F}$ that correspond to $K$ and $N$, respectively, there are many other subgroups.

Every proper subgroup $W$ of $\mathbb{F} \times \mathbb{F}$ is abelian. We have a definition of $nw$ for $n \in \mathbb{Z}, w \in W$ (this is $g^n$ in multiplicative notation and is familiar to us). Since $pw = 0$, we conclude that we may view $W$ as an $\mathbb{F}$-vector space, where for $\bar{n} \in \mathbb{F}$, represented by an integer $n$, we let $\bar{n}w = nw$ and this is well-defined! The conclusion is that every subgroup of $\mathbb{F} \times \mathbb{F}$ is an $\mathbb{F}$-subspace, and the proper subgroups correspond to 1-dimensional subspace of $\mathbb{F} \times \mathbb{F}$. The converse is true too. Thus, the proper subgroups of $N$ that strictly contain $K$ are in bijection with lines in $\mathbb{F} \times \mathbb{F}$. To describe these lines we use linear functionals: For every $(x, y) \neq 0$ we have the subgroup $\{(a, b) : a, b \in \mathbb{F}, xa + yb = 0\}$ corresponding to the subgroup of $N$ given by

$$B_{(x,y)} := \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{F}, xa + yb = 0 \right\}.$$

In fact, $B_{(x,y)}$ depends on $(x, y)$ up to proportion only. Namely, it depends only on the point $(x : y) \in \mathbb{P}^1(\mathbb{F})$, the one-dimensional projective space (cf. Example 10.0.3). There are $p + 1$ points $(x : y)$ in this space (they are represented for example by $(1, a)$ for $a \in \mathbb{F}$ and $(0, 1)$) and so there are $p + 1$ subgroups of $N$ lying strictly in between $N$ and $K$.

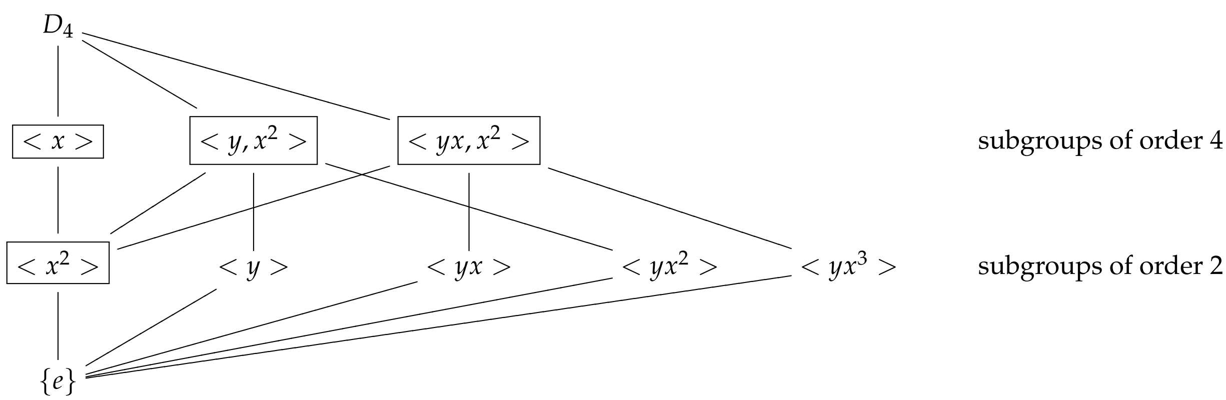
## 11. The lattice of subgroups of a group

Let $G$ be a group. Consider the set $\Lambda(G)$ of all subgroups of $G$. Define an order on this set by $A \leq B$ if $A$ is a subgroup of $B$. This relation is transitive and $A \leq B \leq A$ implies $A = B$. That is, the relation is really an order.

The set $\Lambda(G)$ is a combinatorical lattice: Every two elements $A, B$ have a minimum $A \cap B$ (that is if $C \leq A, C \leq B$ then $C \leq A \cap B$) and a maximum $\langle A, B \rangle$ - the subgroup generated by $A$ and $B$ (that is $C \geq A, C \geq B$ then $C \geq \langle A, B \rangle$). If $A \in \Lambda(G)$ then let $\Lambda_A(G)$ to be the set of all elements in $\Lambda(G)$ that are greater or equal to $A$. It is a lattice in its own right. By the Third Isomorphism Theorem, we have

$$\boxed{\text{If } N \lhd G \text{ then } \Lambda_N(G) \cong \Lambda(G/N) \text{ as lattices.}}$$

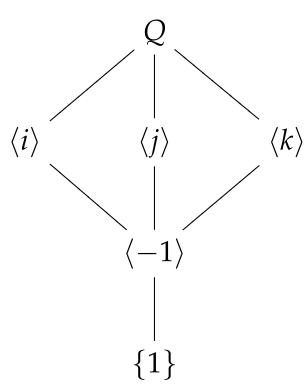
Here is the lattice of subgroups of $D_4$. Normal subgroup are boxed.




How to prove that these are *all* the subgroups of $D_4$? Note that every proper subgroup has order 2 or 4 by Lagrange's theorem. If it is cyclic then it must be one of the above, because the diagram certainly contains all cyclic subgroups. Else, it can only be of order 4 and every element of it different from $e$ has order 2. It is easy to verify that any two distinct elements of order 2 generate one of the subgroups we have listed.

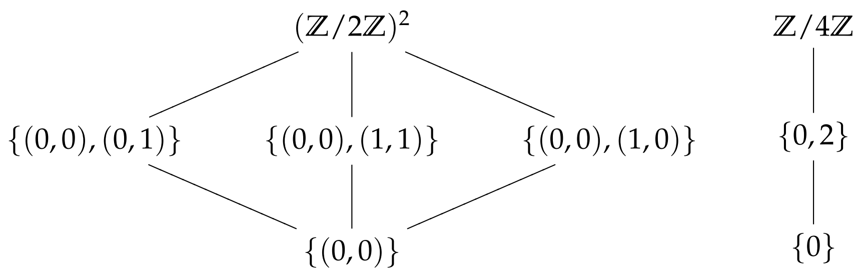
There are at least two ways in which one uses this concept:

- To examine whether two groups could possibly be isomorphic. Isomorphic groups have isomorphic lattices of subgroups. For example, the groups $D_4$ and $Q$ both have 8 elements. The lattice of subgroups of $Q$ is the following:




We conclude that $Q$ and $D_4$ are not isomorphic.

- To recognize quotients. Consider for example $D_4/\langle x^2 \rangle$. This is a group of 4 elements. Let us give ourselves that there are only two groups of order 4 up to isomorphism and those are $(\mathbb{Z}/2\mathbb{Z})^2$ and $\mathbb{Z}/4\mathbb{Z}$. The lattice of subgroups for them are




We conclude that $D_4/\langle x^2 \rangle \cong (\mathbb{Z}/2\mathbb{Z})^2$.

# **Part** 3. **Group Actions on Sets**

Group actions on sets will be revealed to be an extremely powerful method to gain information about the structure of groups.

## 12. Basic definitions

Let $G$ be a group and let $S$ be a non-empty set. We say that $G$ **acts on** $S$ if we are given a function

$$G \times S \to S, \quad (g, s) \longmapsto g * s,$$

such that;

(i) $e * s = s$ for all $s \in S$;

(ii) $(g_1 g_2) * s = g_1 * (g_2 * s)$ for all $g_1, g_2 \in G$ and $s \in S$.

Given an action of $G$ on $S$ we can define the following sets. Let $s \in S$. Define the **orbit** of $s$

$$\mathrm{Orb}(s) = \{g * s : g \in G\}.$$

*Note that* $\mathrm{Orb}(s)$ *is a subset of* $S$, equal to all the images of the element $s$ under the action of the elements of the group $G$. We also define the **stabilizer** of $s$ to be

$$\mathrm{Stab}(s) = \{g \in G : g * s = s\}.$$

*Note that* $\mathrm{Stab}(s)$ *is a subset of* $G$. In fact, it is a subgroup, as the next Lemma states.

One should think of every element of the group as becoming a symmetry of the set $S$. We will make that more precise later. For now, we just note that every element $g \in G$ defines a function $S \to S$ by $s \mapsto gs$. This function will turn out to be bijective.

## 13. Basic properties

**Lemma 13.0.1.** *(1) Let $s_1, s_2 \in S$. We say that $s_1$ is related to $s_2$, i.e., $s_1 \sim s_2$, if there exists $g \in G$ such that*

$$g * s_1 = s_2.$$

*This is an equivalence relation. The equivalence class of $s_1$ is its orbit* $\mathrm{Orb}(s_1)$.

*(2) Let $s \in S$. The set* $\mathrm{Stab}(s)$ *is a subgroup of $G$.*

*(3) Suppose that both $G$ and $S$ have finitely many elements. Then*

$$|\mathrm{Orb}(s)| = \frac{|G|}{|\mathrm{Stab}(s)|}.$$

*Proof.* (1) We need to show reflexive, symmetric and transitive. First, we have $e * s = s$ and hence $s \sim s$, meaning the relation is reflexive. Second, if $s_1 \sim s_2$ then for a suitable $g \in G$ we have $g * s_1 = s_2$. But then, $s_1 = g^{-1} * (g * s_1) = g^{-1} * s_2$ and so the relation is symmetric.

It remains to show transitive. If $s_1 \sim s_2$ and $s_2 \sim s_3$ then for suitable $g_1, g_2 \in G$ we have

$$g_1 * s_1 = s_2, \quad g_2 * s_2 = s_3.$$

Therefore,

$$(g_2 g_1) * s_1 = g_2 * (g_1 * s_1) = g_2 * s_2 = s_3,$$

and hence $s_1 \sim s_3$.

Moreover, by the very definition, the equivalence class of an element $s_1$ of $S$ is all the elements of the form $g * s_1$ for some $g \in G$, namely, $\text{Orb}(s_1)$.

(2) Let $H = \text{Stab}(s)$. We have to show that: (i) $e \in H$; (2) If $g_1, g_2 \in H$ then $g_1 g_2 \in H$; (iii) If $g \in H$ then $g^{-1} \in H$.

First, by definition of group action we have $e * s = s$. Therefore $e \in H$. Next suppose that $g_1, g_2 \in H$, i.e., $g_1 * s = s$ and $g_2 * s = s$. Then, $(g_1 g_2) * s = g_1 * (g_2 * s) = g_1 * s = s$. Thus, $g_1 g_2 \in H$. Finally, if $g \in H$ then $g * s = s$ and so $g^{-1} * g * s = g^{-1} * s$. But, $g^{-1} * g * s = e * s = s$, and therefore $g^{-1} \in H$.

(3) We claim that there exists a bijection between the left cosets of $H$ and the orbit of $s$. If we show that, then by Lagrange's theorem,

$$|\text{Orb}(s)| = \text{no. of left cosets of } H = \text{index of } H = |G|/|H|.$$

Define a function

$$G/H := \{\text{left cosets of } H\} \xrightarrow{\phi} \text{Orb}(s),$$

by

$$\phi(gH) = g * s.$$

We claim that $\phi$ is a well defined bijection. First

Well-defined: Suppose that $g_1 H = g_2 H$. We need to show that the rule $\phi$ would give the same result whether we take the representative $g_1$ or the representative $g_2$ to the coset. That is, we need to show

$$g_1 * s = g_2 * s.$$

Note that $g_1^{-1} g_2 \in H$, i.e., $(g_1^{-1} g_2) * s = s$. We get

$$\begin{aligned} g_1 * s &= g_1 * ((g_1^{-1} g_2) * s) \\ &= (g_1 (g_1^{-1} g_2)) * s \\ &= g_2 * s. \end{aligned}$$

$\phi$ is surjective: Let $t \in \text{Orb}(s)$ then $t = g * s$ for some $g \in G$. Thus,

$$\phi(gH) = g * s = t,$$

and we get that $\phi$ is surjective.

$\phi$ is injective: Suppose that $\phi(g_1 H) = \phi(g_2 H)$. We need to show that $g_1 H = g_2 H$. Indeed,

$$\begin{aligned} & \phi(g_1 H) = \phi(g_2 H) \\ \Rightarrow \quad & g_1 * s = g_2 * s \\ \Rightarrow \quad & g_2^{-1} * (g_1 * s) = g_2^{-1} * (g_2 * s) \\ \Rightarrow \quad & (g_2^{-1} g_1) * s = (g_2^{-1} g_2) * s = s \\ \Rightarrow \quad & g_2^{-1} g_1 \in \text{Stab}(s) = H \\ \Rightarrow \quad & g_1 H = g_2 H. \end{aligned}$$

□

**Corollary 13.0.2.** *The set $S$ is a disjoint union of orbits.*

*Proof.* The orbits are the equivalence classes of the equivalence relation $\sim$ defined in Lemma 13.0.1. Any equivalence relation on a set partitions the set into disjoint equivalence classes. □

We have in fact seen that every orbit is in bijection with the cosets of some group. If $H$ is any subgroup of $G$ let us use the notation $G/H$ for its cosets (note though that if $H$ is not normal this is not a group, but just a set). We saw that if $s \in S$ then there is a natural bijection $G/\text{Stab}(s) \leftrightarrow \text{Orb}(s)$. Thus, the picture of $S$ is as follows

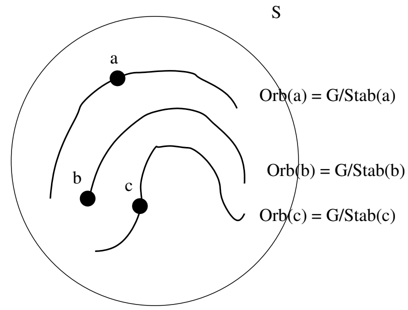



FIGURE 3. $S$ decomposes into disjoint orbits.

## 14. SOME EXAMPLES

**Example 14.0.1.** The group $S_n$ acts on the set $\{1, 2, \dots, n\}$. The action is **transitive**, i.e., there is only one orbit. The stabilizer of $i$ is $S_{\{1,2,\dots,i-1,i+1,\dots,n\}} \cong S_{n-1}$.

**Example 14.0.2.** The group $\mathrm{GL}_n(\mathbb{F})$ acts on $\mathbb{F}^n$, and also $\mathbb{F}^n - \{0\}$. The action is transitive on $\mathbb{F}^n - \{0\}$ and has two orbits on $\mathbb{F}^n$. The stabilizer of 0 is of course $\mathrm{GL}_n(\mathbb{F})$; the stabilizer of a non-zero vector $v_1$ can be written in a basis $w_1, w_2, \dots, w_n$ with $w_1 = v_1$ as the matrices of the shape

$$\begin{pmatrix} 1 & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & \vdots & \dots & \vdots \\ 0 & * & \dots & * \end{pmatrix}.$$

**Example 14.0.3.** Let $H$ be a subgroup of $G$ then we have an action

$$H \times G \to G, \qquad (h, g) \mapsto hg.$$

In this example, $H$ is the "group" and $G$ is the "set". Here the orbits are right cosets of $H$ and the stabilizers are trivial. Since $G = \coprod \mathrm{Orb}(g_i) = \coprod Hg_i$, we conclude that $|G| = \sum_i |\mathrm{Orb}(g_i)| = \sum_i |H|/|\mathrm{Stab}(g_i)| = \sum_i |H|$ and therefore that $|H| \mid |G|$ and that $[G : H]$, the number of cosets, is $|G|/|H|$. We have recovered Lagrange's theorem.

**Example 14.0.4.** Let $H$ be a subgroup of $G$. Let $G/H = \{gH : g \in G\}$ be the set of left cosets of $H$ in $G$. Then we have an action

$$G \times G/H \to G/H, \qquad (a, bH) \mapsto abH.$$

Here there is a unique orbit – $G$ acts transitively. The stabilizer of $gH$ is the subgroup $gHg^{-1}$. We will come back to this important example. It will yield the coset representation of a group.

**Example 14.0.5.** Let $G = \mathbb{R}/2\pi\mathbb{Z}$. It acts on the sphere by rotations: an element $\theta \in G$ rotates the sphere by angle $\theta$ around the north-south axis. The orbits are latitude lines and the stabilizers of every point is trivial, except for the poles whose stabilizer is $G$. See Figure 4.

**Example 14.0.6.** Recall that $D_8$ is the group of symmetries of a regular octagon in the plane.

$$D_8 = \{e, x, x^2, \dots, x^7, y, yx, yx^2, \dots, yx^7\},$$

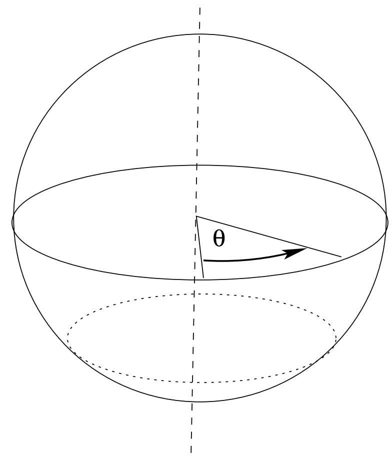



FIGURE 4. Action on the sphere by rotation.

where $x$ is the rotation clockwise by angle $2\pi/8$ and $y$ is the reflection through the $y$-axis. We have the relations

$$x^8 = y^2 = e, \quad yxy = x^{-1}.$$

We let $S$ be the set of colourings of the vertices of the octagon having 4 red vertices and 4 green vertices. We may think about $S$ as the set of necklaces with 8 gems, where four gems are rubies and 4 are sapphires. The cardinality of $S$ is $\binom{8}{4} = 70$. The group $D_8$ acts on $S$ by its action on the octagon.

For example, the colouring $s_0$ in Figure 5 (where the two colours are represented by squares and circles) is certainly preserved under $x^2$ and under $y$. Therefore, the stabilizer of $s_0$ contains at least the set of eight elements

$$\{e, x^2, x^4, x^6, y, yx^2, yx^4, yx^6\}. \tag{1}$$

Remember that the stabilizer is a subgroup and, by Lagrange's theorem, of order dividing

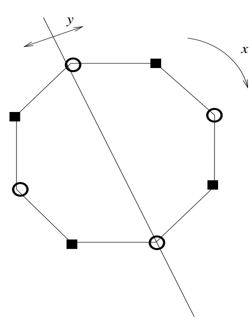



FIGURE 5. A necklace with 4 rubies and 4 sapphires.

$16 = |D_8|$. On the other hand, $\mathrm{Stab}(s_0) \neq D_8$ because $x \notin \mathrm{Stab}(s_0)$. It follows that the stabilizer has exactly 8 elements and is equal to the set in (1).

According to Lemma 13.0.1 the orbit of $s_0$ is in bijection with the left cosets of $\mathrm{Stab}(s_0) = \{e, x^2, x^4, x^6, y, yx^2, yx^4, yx^6\}$. By Lagrange's theorem there are two cosets. For example, $\mathrm{Stab}(s_0)$ and $x\mathrm{Stab}(s_0)$ are distinct cosets. The proof of Lemma 13.0.1 tells us how to find the orbit: it is the set

$$\{s_0, xs_0\},$$

portrayed in Figure 6.

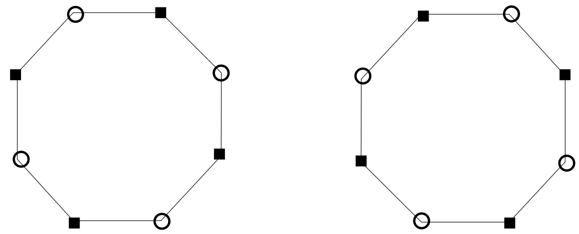
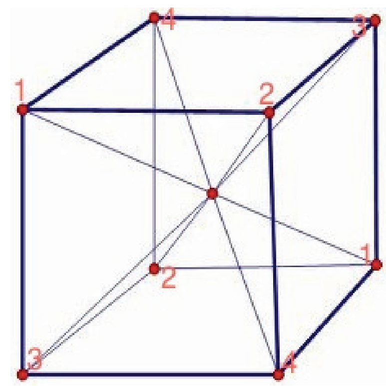


FIGURE 6. The orbit of the necklace.




**Example 14.0.7.** Let $\Gamma$ be the group of symmetries of the cube obtained by rigid motions (so reflections are not allowed). The action of $\Gamma$ on the 8 vertices gives an injective homomorphism $\Gamma \hookrightarrow S_8$. But, as we shall see, there are much more useful realizations of $\Gamma$.

Let's see a clever way to count the number of elements in $\Gamma$: It is easy to see that $\Gamma$ acts transitively on the 6 faces of the cube. The stabilizer of a face is made of the rotations that keep the face but rotate it around its middle point. The orbit-stabilizer formula then gives that

$$\sharp\Gamma = 24.$$

By considering the action of $\Gamma$ on two adjacent faces we see that the homomorphism $\Gamma \to S_6$ must be injective. We obtain that $\Gamma$ can be realized as a **transitive subgroup** of $S_6$ (namely, a subgroup that acts transitively on $\{1, 2 \dots, 6\}$. This is an improvement, but still $\sharp S_6 = 6! = 720$ and $\sharp\Gamma = 24$ which means that $\Gamma$ is a "tiny" subgroup of $S_6$. So consider the action of $\Gamma$ on the 4 long diagonals of the cube which we number $\{1, 2, 3, 4\}$. This gives a homomorphism

$$f \colon \Gamma \to S_4.$$

It is not a priori clear whether $f$ is injective. Since both sides have 24 elements, if we show $f$ is surjective then $f$ is also injective and hence an isomorphism. Here is an argument showing that:

A rotation keeping the front face has the effect $(1243)$, while a rotation keeping the right-facing face has the effect $(2314)$. The cyclic subgroups generated by those two cycles are $\{1, a = (1243), b = (14)(23), (3421)\}$ and $\{1, c = (2314), d = (21)(34), (4132)\}$. We see that the subgroup they generate contains the Klein group (calculate $bd$), and a short calculation shows that it in facts contains a subgroup of order 8 (for instance the subgroup generated by the Klein group and $(1243)$). Thus, the order of the subgroup they generate is divisible by 8. On the other hand, its order is also divisible by 3 because it contains $ac = (132)$. Therefore, the image of $f$ is $S_4$ and we conclude that

$$\Gamma \cong S_4.$$

## 15. Cayley's theorem

**Theorem 15.0.1.** *Every finite group of order $n$ is isomorphic to a subgroup of $S_n$.*

We first prove a lemma that puts group actions in a different context. Let $A$ be a finite set. Recall the group of permutations of $A$, $\Sigma_A$; it is the set of bijective functions $A \to A$. If we let $s_1, \dots, s_n$ be the elements of $A$, we can identify bijective functions $A \to A$ with permutations of $\{1, \dots, n\}$ and we see that $\Sigma_A \cong S_n$.

**Lemma 15.0.2.** *To give an action of a group $G$ on a set $A$ is equivalent to giving a homomorphism $G \to \Sigma_A$. The kernel of this homomorphism is $\cap_{a\in A}\mathrm{Stab}(a)$.*

*Proof.* An element $g$ define a function $\phi_g \colon A \to A$ by $\phi_g(a) = ga$. We have $\phi_e$ being the identity function. Note that $\phi_h\phi_g(a) = \phi_h(ga) = hga = \phi_{hg}(a)$ for every $a$ and hence $\phi_h\phi_g = \phi_{hg}$. In particular, $\phi_g\phi_{g^{-1}} = \phi_{g^{-1}}\phi_g = Id$. This shows that every $\phi_g$ is a bijection and the map

$$\phi\colon G \to \Sigma_A, \qquad g \mapsto \phi_g,$$

is a homomorphism. (Conversely, given such a homomorphism $\phi$, define a group action by $g * a := \phi(g)(a)$.)

The kernel of this homomorphism consists of the elements $g$ such that $\phi_g$ is the identity, i.e., $\phi_g(a) = a$ for all $a \in A$. That is, $g \in \mathrm{Stab}(a)$ for every $a \in A$. The set of such elements $g$ is just $\cap_{a\in A}\mathrm{Stab}(a)$. □

*Proof.* (Cayley's Theorem) Consider the action of $G$ on itself by multiplication (Example 14.0.3), $(g, g') \mapsto gg'$. Recall that all stabilizers are trivial. Thus this action gives an injective homomorphism

$$G \hookrightarrow \Sigma_G \cong S_n,$$

where $n = |G|$. □

## 16. The coset representation

Let $G$ be a group and $H$ a subgroup of finite index $n$. Consider the action of $G$ on the set of cosets $G/H$ of $H$ (Example 14.0.4) and the resulting homomorphism

$$\phi\colon G \to \Sigma_{G/H} \cong S_n,$$

where $n = [G : H]$. We shall refer to it as the **coset representation** of $G$. The kernel $K$ of $\phi$ is

$$K = \cap_{a\in G/H}\mathrm{Stab}(a) = \cap_{g\in G}\mathrm{Stab}(gH) = \cap_{g\in G}gHg^{-1}.$$

Being a kernel of a homomorphism, $K$ is normal in $G$. $K$ is also contained in $H$. Furthermore, since the resulting homomorphism $G/K \to S_n$ is injective we get that $|G/K| = [G : K]$ divides $|S_n| = n!$. In particular, we conclude that every subgroup $H$ of $G$ contains a subgroup $K$ which is normal in $G$ and of index at most $[G : H]!$. Thus, for example, a simple infinite group has no subgroups of finite index – I am not sure if this has a simple proof that doesn't use one way or another group actions.

In fact, the formula $K = \cap_{g\in G}gHg^{-1}$ shows that $K$ is the maximal subgroup of $H$ which is normal in $G$. Indeed, if $K' \lhd G, K' < H$ then for any $g \in G$ we have $K' = gK'g^{-1} \subseteq gHg^{-1}$ and we see that $K' \subseteq K$.

The coset representation reveals an important principle. *To give a subgroup of finite index $n$ of a group $G$ is to give a transitive action of $G$ on a set of $n$ elements.*

Indeed, if $G$ acts transitively on a set $T$ of $n$-elements, pick an element $t \in T$ and let $H = \mathrm{Stab}(t)$. Then, the bijection $G/H \leftrightarrow T$ shows that $H$ is of index $n$. Conversely, if $H$ is a subgroup of $G$ of index $n$, the coset representation of $G$ on $G/H$ is a transitive action on a set of $n$ elements.

**Example 16.0.1.** We construct a surjective homomorphism $S_4 \to S_3$ in a different way than that of Example 8.0.5. Recall that $D_4 < S_4$ is a subgroup of index 3. The coset representation therefore gives a homomorphism

$$S_4 \to S_3.$$

The image is a transitive subgroup of $S_3$ and there are only two such: $A_3$ and $S_3$. Take the element $(12)$ which is not in $D_4$. Then the three cosets of $D_4$ can be written as

$$D_4, (12)D_4, xD_4,$$

for some $x$ whose precise form will not matter to us. As $(12)$ takes $D_4$ to $(12)D_4$ and $(12)D_4$ to $D_4$, it must fix $xD_4$ and therefore the image of $(12)$ in $S_3$ is a transposition. It follows that the image of $S_4$ must be $S_3$. The kernel is a normal subgroup of $S_4$ contained in $D_4$ of cardinality 4. It must therefore be the Klein group $V$.

## 17. The Cauchy-Frobenius formula

The **Cauchy-Frobenius formula** (CFF), sometimes called **Burnside's lemma**, is a very useful formula for combinatorial problems.

### 17.1. A formula for the number of orbits.

**Theorem 17.1.1. (CFF)** *Let $G$ be a finite group acting on a finite set $S$. Let $N$ be the number of orbits of $G$ in $S$. Define*

$$I(g) = |\{s \in S : g * s = s\}|$$

*(the number of elements of $S$ fixed by the action of $g$). Then*

$$N = \frac{1}{|G|} \sum_{g \in G} I(g). \tag{2}$$

*Remark* 17.1.2. To say $N = 1$ is to say that $G$ acts transitively on $S$. It means exactly that: For every $s_1, s_2 \in S$ there exists $g \in G$ such that $g * s_1 = s_2$.

*Remark* 17.1.3. In the proof we will use the following general fact. Let $G$ act on a set $S$ and let $s \in S$. Then, for any element $g \in G$,

$$\mathrm{Stab}_G(gs) = g\mathrm{Stab}_G(s)g^{-1}.$$

In words, the stabilizers of two elements in $S$ that lie in the same orbit are conjugate subgroups of $G$. In particular they all have the same cardinality (the function $\mathrm{Stab}_G(gs) \to \mathrm{Stab}(s)$ given by $h \mapsto g^{-1}hg$ is a bijection).

*Proof.* We define a function

$$T \colon G \times S \to \{0, 1\}, \quad T(g, s) = \begin{cases} 1 & g * s = s \\ 0 & g * s \neq s \end{cases}.$$

Note that for a fixed $g \in G$ we have

$$I(g) = \sum_{s \in S} T(g, s),$$

and that for a fixed $s \in S$ we have

$$|\mathrm{Stab}(s)| = \sum_{g \in G} T(g, s).$$

Let us fix representatives $s_1, \dots, s_N$ for the $N$ disjoint orbits of $G$ in $S$. Now,

$$\begin{aligned}
\sum_{g \in G} I(g) &= \sum_{g \in G} \left( \sum_{s \in S} T(g, s) \right) = \sum_{s \in S} \left( \sum_{g \in G} T(g, s) \right) \\
&= \sum_{s \in S} |\mathrm{Stab}(s)| = \sum_{s \in S} \frac{|G|}{|\mathrm{Orb}(s)|} \\
&= \sum_{i=1}^{N} \sum_{s \in \mathrm{Orb}(s_i)} \frac{|G|}{|\mathrm{Orb}(s)|} = \sum_{i=1}^{N} \sum_{s \in \mathrm{Orb}(s_i)} \frac{|G|}{|\mathrm{Orb}(s_i)|} \\
&= \sum_{i=1}^{N} \frac{|G|}{|\mathrm{Orb}(s_i)|} \cdot |\mathrm{Orb}(s_i)| = \sum_{i=1}^{N} |G| \\
&= N \cdot |G|.
\end{aligned}$$

□

**Corollary 17.1.4.** *Let $G$ be a finite group acting transitively on a finite $S$. Suppose that $|S| > 1$. Then there exists $g \in G$ without fixed points.*

*Proof.* By contradiction. Suppose that every $g \in G$ has a fixed point in $S$. That is, suppose that for every $g \in G$ we have

$$I(g) \geq 1.$$

Since $I(e) = |S| > 1$ we have that

$$\sum_{g \in G} I(g) > |G|.$$

By Cauchy-Frobenius formula, the number of orbits $N$ is greater than 1. Contradiction. □

**Example 17.1.5.** The symmetry group $\Gamma$ of the cube acts transitively on the faces. It follows that there is a symmetry of the cube leaving no face fixed (there are many, in fact). Can you find one?

**Example 17.1.6.** A subgroup $G$ of $S_n$ is called **transitive** if its action on $\{1, 2, \dots, n\}$ is transitive. If $n > 1$, the corollary says that such a subgroup contains a permutation with no fixed points. Moreover, by the orbit-stabilizer formula, $G$ has a subgroup of index $n$ and so $n | \sharp G$. Such results are used in the classification of transitive subgroups of $S_n$ for small values of $n$ – a classification important to Galois theory because the Galois group of an irreducible separable polynomial of degree $n$ is a transitive subgroup of $S_n$. For example, for $S_3$ we find that $A_3$ and $S_3$ are the only transitive subgroups. For $S_4$ we are looking for subgroups of order divisible by 4 (so $4, 8, 12$ and 24) that act transitively and also contain a permutation with no fixed point. After conjugation, we may therefore assume that either $(1234)$ or $(12)(34)$ belongs to the subgroup. Continuing the analysis, one finds that up to conjugation the transitive subgroups are $V$, $\langle (1234) \rangle, D_4, A_4, S_4$.

17.2. **Applications to combinatorics.** In the following examples we will consider roulettes and necklaces. When we are asking about the number of colourings of a roulette with $n$ wedges satisfying some restrictions, we allow rotational symmetries only. When we talk about colourings of necklaces, we allow in addition symmetries obtain from turning the necklace over so that its back side becomes its front side. Thus, for a roulette with $n$ wedges the symmetry group is $\mathbb{Z}/n\mathbb{Z}$, while for a necklace with $n$ stones the symmetry group is $D_n$.

**Example 17.2.1.** How many roulettes with 11 wedges, painted 2 blue, 2 green and 7 red, are there when we allow rotations?

Let $S$ be the set of painted roulettes. Let us enumerate the sectors of a roulette by the numbers $1, \dots, 11$. The set $S$ is a set of $\binom{11}{2}\binom{9}{2} = 1980$ elements (choose which 2 wedges are blue, and then choose out of the remaining 9 wedges which 2 are green).

Let $G$ be the group $\mathbb{Z}/11\mathbb{Z}$. It acts on $S$ by rotations. The element 1 rotates a painted roulette by angle $2\pi/11$ clockwise. The element $n$ rotates a painted roulette by angle $2n\pi/11$ clockwise. We are interested in $N$ – the number of orbits for this action. We use **CFF**.

The identity element always fixes the whole set. Thus $I(0) = 1980$. We claim that if $1 \leq i \leq 10$ then $i$ doesn't fix any element of $S$. Indeed, suppose that $1 \leq i \leq 10$ and $i$ fixes $s$. Then so does $\langle i \rangle = \mathbb{Z}/11\mathbb{Z}$ (the stabilizer is a subgroup). But any colouring fixed under rotation by 1 must be single colored! Contradiction.

Applying **CFF** we get

$$N = \frac{1}{11} \sum_{n=0}^{10} I(n) = \frac{1}{11} \cdot 1980 = 180.$$

**Example 17.2.2.** How many roulettes with 12 wedges, painted 2 blue, 2 green and 8 red, are there when we allow rotations?

Let $S$ be the set of painted roulettes. Let us enumerate the sectors of a roulette by the numbers $1, \dots, 12$. The set $S$ is a set of $\binom{12}{2}\binom{10}{2} = 2970$ elements (choose which 2 are blue, and then choose out of the 10 that are left which 2 are green).

Let $G$ be the group $\mathbb{Z}/12\mathbb{Z}$. It acts on $S$ by rotations. The element 1 rotates a painted roulette by angle $2\pi/12$ clockwise. The element $n$ rotates a painted roulette by angle $2n\pi/12$ clockwise. We are interested in $N$ – the number of orbits for this action. We use **CFF**.

The identity element always fixes the whole set. Thus $I(0) = 2970$. We claim that if $1 \leq i \leq 11$ and $i \neq 6$ then $i$ doesn't fix any element of $S$. Indeed, suppose that $i$ fixes a painted roulette. Say in that roulette the $r$-th sector is blue. Then so must be the $i + r$ sector (because the $r$-th sector goes under the action of $i$ to the $r + i$-th sector). Therefore so must be the $r + 2i$ sector. But there are only 2 blue sectors! The only possibility is that the $r + 2i$ sector is the same as the $r$ sector, namely, $i = 6$.

If $i$ is equal to 6 and we enumerate the sectors of a roulette by the numbers $1, \dots, 12$ we may write $i$ as the permutation

$$(1\ 7)(2\ 8)(3\ 9)(4\ 10)(5\ 11)(6\ 12).$$

In any colouring fixed by $i = 6$ the colors of the pairs $(1\ 7), (2\ 8), (3\ 9), (4\ 10), (5\ 11)$ and $(6\ 12)$ must be the same. We may choose one pair for blue, one pair for green. The rest would be red. Thus there are $30 = 6 \cdot 5$ possible choices. We summarize:

| element $g$ | $I(g)$ |
|---|---|
| 0 | 2970 |
| $i \neq 6$ | 0 |
| $i = 6$ | 30 |

Applying **CFF** we get that there are

$$N = \frac{1}{12}(2970 + 30) = 250$$

different coloured roulettes.

**Example 17.2.3.** In this example $S$ is the set of necklaces made of four rubies and four sapphires laid on the table. We ask how many necklaces there are when we allow rotations and flipping-over.

We may think of $S$ as the colourings of a regular octagon, such that four vertices are green and four are red. The group $G = D_8$ acts on $S$ and we are interested in the number of orbits for the group $G$.

The results are the following

| element $g$ | $I(g)$ |
|---|---|
| $e$ | 70 |
| $x, x^3, x^5, x^7$ | 0 |
| $x^2, x^6$ | 2 |
| $x^4$ | 6 |
| $yx^i$ for $i = 0, \ldots, 7$ | 6 |

We explain how the entries in the table are obtained:

- The identity always fixes the whole set $S$. The number of elements in $S$ is $\binom{8}{4} = 70$ (choosing which 4 would be green).
- The element $x$ cannot fix any colouring, because any colouring fixed by $x$ must have all sections of the same colour (because $x = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$). If $x^r$ fixes a colouring $s_0$ so does any power of $x^r$, in particular $(x^r)^r = x^{(r^2)}$, because the stabilizer is a subgroup. Apply that for $r = 3, 5, 7$ to see that if $x^r$ fixes a colouring so does $x$ , which is impossible. (For instance, $x^{(3^2)} = x^9 = x$, because $x^8 = e$.)
- $x^2$ written as a permutation is $(1\ 3\ 5\ 7)(2\ 4\ 6\ 8)$. We see that if 1 is green, say, so are $3, 5, 7$ and the rest must be red. That is, all the freedom we have is to choose whether the cycle $(1\ 3\ 5\ 7)$ is green or red. This gives us two colourings fixed by $x^2$. The same rational applies to $x^6 = (8\ 6\ 4\ \ 2)(7\ 5\ 3\ 1)$.
- Consider now $x^4$. It may written in permutation notation as $(1\ 5)(2\ 6)(3\ 7)(4\ 8)$. In any colouring fixed by $x^4$ each of the cycles $(1\ 5)(2\ 6)(3\ 7)$ and $(4\ 8)$ must be single colored. There are thus $\binom{4}{2} = 6$ possibilities (Choosing which 2 out of the four cycles would be green).
- It remains to deal with the elements $yx^i$. We recall that these are all reflections. There are two kinds of reflections. One may be written using permutation notation as

  $$(i_1\ i_2)(i_3\ i_4)(i_5\ i_6).$$

  That is, these are reflections with two fixed vertices. For example $y = (2\ 8)(3\ 7)(4\ 6)$ is of this form). The other kind is of the form

  $$(i_1\ i_2)(i_3\ i_4)(i_5\ i_6)(i_7\ i_8).$$

  These are reflections that do not fix any vertex. For example $yx = (1\ 8)(2\ 7)(3\ 6)(4\ 5)$ is of this sort. Whatever is the case, one uses similar reasoning to deduce that there are 6 colourings preserved by a reflection.

One needs only apply **CFF** to get that there are

$$N = \frac{1}{16}(70 + 2 \cdot 2 + 6 + 8 \cdot 6) = 8$$

distinct necklaces.

It is possible to develop general formulas for the number of roulettes of $n$ wedges coloured according to some specifications. The starting point in developing such formula is the following principle that we used in the calculation above. Every element of the dihedral group $D_n$ has a composition into disjoint cycles according to the following cases:

- If $n = 2r + 1$ is odd, any reflection has a unique fixed vertex and so can be written as a product of disjoint transpositions
$$(i_1\ i_2) \cdots (i_{2r-1}\ i_{2r}).$$
- If $n = 2r$ is even, there are $n/2 = r$ reflections that don't have any fixed vertex and they can be written as a product of disjoint transpositions
$$(i_1\ i_2) \cdots (i_{2r-1}\ i_{2r}).$$
There are also $n/2 = r$ reflections that have precisely two fixed vertices and they can be written as a product of disjoint transpositions
$$(i_1\ i_2) \cdots (i_{2r-3}\ i_{2r-2}).$$
- The element $x^a$, $1 \leq a \leq n-1$, has order $d := n/\gcd(a, n)$. It is a product of $n/d = \gcd(a, n)$ disjoint cycles, each of length $d$:
$$(i_1\ \cdots\ i_d)(i_{d+1}\ \cdots\ i_{2d}) \cdots (i_{n-d+1}\ \cdots\ i_n).$$
- Every element of $D_n$ falls into one of the cases above. The analysis also applies to $\mathbb{Z}/n\mathbb{Z}$ thought of as the cyclic group $\langle x \rangle \subset D_n$.
- In any colouring that is fixed by an element $z \in D_n$ each cycle in the decomposition of $z$ into disjoint cycles is assigned a single colour.

**Example 17.2.4.** For example, suppose that we want to know the number of necklaces with $n$ wedges where 3 are painted red and the rest are blue. *Let us suppose for simplicity that $n$ is odd*. Such a colouring is fixed by a reflection only if its fixed vertex is assigned the colour red and then we can choose which of the $(n-1)/2$ pairs of vertices are red. Thus, each reflection fixes $(n-1)/2$ colourings.

If a colouring is fixed by $x^a$, $1 \leq a \leq n-1$ then each cycle in $x$ has length 3. Such $x$ exists if $3|n$ only and then there are precisely two such elements $x$ (recall our discussion in §4 of cyclic groups!). Every such element $x$ will have precisely one of its $n/3$ cycles coloured red and we may choose which. Namely, such $x$ fixes $n/3$ distinct colourings.

To summarize, if $3 \nmid n$, the number of such necklaces is $\frac{1}{2n}(\binom{n}{3} + n\frac{n-1}{2}) = \frac{n^2-1}{12}$. You may perform a check that such a number is always an integer! On the other hand, if $3 \mid n$ then the number of such necklaces is $\frac{1}{2n}(\binom{n}{3} + n\frac{n-1}{2} + 2\frac{n}{3}) = \frac{n^2+3}{12}$.

### 17.3. **Rubik's cube.** [9]

In the case of the Rubik cube there is a group $G$ acting on the cube. The group $G$ is generated by 6 basic moves $a, b, c, d, e, f$ (each is a rotation of a certain "third of the cube") and could be

[9] Also known as the Hungarian cube.

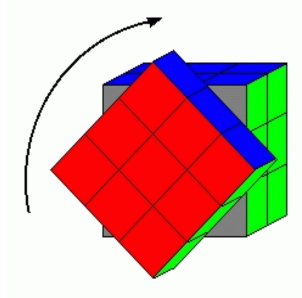


FIGURE 7. The Rubik Cube.

thought of as a subgroup of the symmetric group on $54 = 9 \times 6$ letters. It is called the cube group. The structure of this group is known. It is isomorphic to

$$(\mathbb{Z}/3\mathbb{Z}^7 \times \mathbb{Z}/2\mathbb{Z}^{11}) \rtimes ((A_8 \times A_{12}) \rtimes \mathbb{Z}/2\mathbb{Z})$$

(the notation will make sense once we have defined semi-direct products). The order of the cube group is

$$2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11 = 43,252,003,274,489,856,000,$$

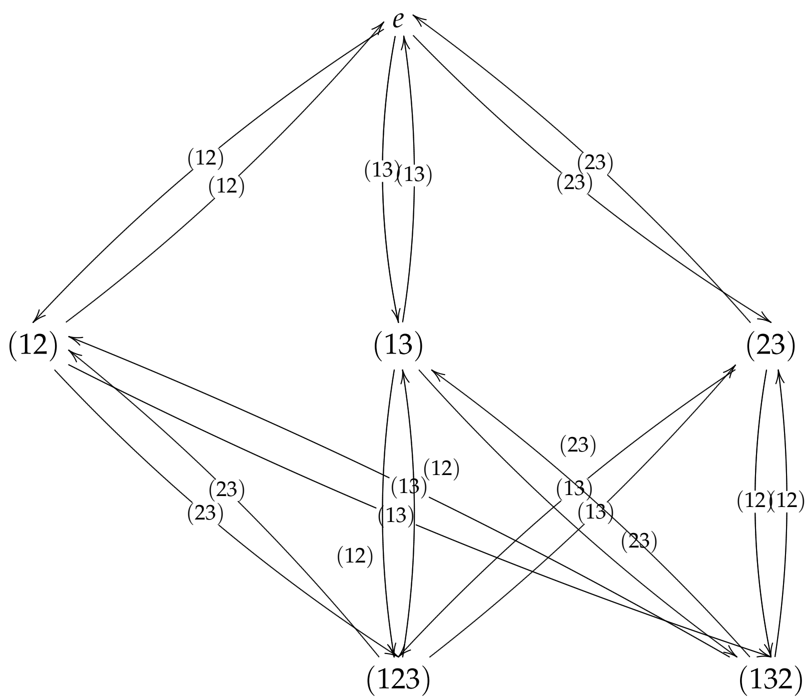
while the order of $S_{54}$ is

$$230843697339241380472092742683027581083278564571807941132288000000000000.$$

One is usually interested in solving the cube. Namely, reverting it to its original position. Since the current position was gotten by applying an element $\tau$ of $G$, in group theoretic terms we attempt to find an algorithm of writing every $G$ in terms of the generators $a, b, c, d, e, f$ since then also $\tau^{-1}$ will have such an expression, which is nothing else than a series of moves that returns the cube to its original position. It is natural do deal with the set of generators $a^{\pm 1}, b^{\pm 1}, \dots, f^{\pm 1}$ (why do 3 times $a$ when you can do $a^{-1}$??). A common question is what is the maximal number of basic operations that may be required to return a cube to its original position. Otherwise said, what is the diameter of the Cayley graph? But more than that, is there a simple algorithm of finding for every element of $G$ an expression in terms of the generators? (The speed at which some people are able so solve the cube certainly suggests that the answer is yes! The current world record (June 2020) is 3.47 seconds, achieved by Yusheng Du from China in 2018.)

**The Cayley graph.**
Suppose that $\{g_\alpha : \alpha \in I\}$ are generators for $G$. We define an oriented graph taking as vertices the elements of $G$ and taking for every $g \in G$ an oriented edge from $g$ to $gg_\alpha$. If we forget the orientation, the property of $\{g_\alpha : \alpha \in I\}$ being a set of generators is equivalent to the graph being connected.
Suppose that the set of generators consists of $n$ elements. Then, by definition, from every vertex we have $n$ vertices emanating and also $n$ arriving. We see therefore that all Cayley graphs are regular graphs. This, in turn, gives a systematic way of constructing regular graphs.
Suppose we take as a group the symmetric group (see below) $S_n$ and the transpositions as generators. One can think as a permutation as being performed in practice by successively swapping the places of two elements. Thus, in the Cayley graph, the distance between a permutation and the identity (the distance is defined as the minimal length of a path between the two vertices) is the minimal way to write a permutation as a product of transpositions, and could be thought of as a certain measure of the complexity of a permutation.

The figure below gives the Cayley graph of $S_3$ with respect to the generating set of transpositions. It is a 3-regular oriented graph and a 6 regular graph.




Now, since the Cayley graph of the cube group $G$ has 12 edges emanating from each vertex (and is a connected graph, by definition of the cube group) it follows that to reach all positions one is forced to allow at least $\log_{12}|G| \sim 18.2$, thus at least 19, moves.[10] The actual number is surprisingly close to this simple estimate. It was found that the cube can always be solved by at most 20 moves and, as there are positions that require 20 moves to be solved, this is optimal.

[10] There is a subtle point we are glossing over here as we must distinguish between the symmetries of the cube provided by $G$ and the effect they have on the colouring of its pieced. Thus, we must ask if there are operations that move the cube but leave the overall colouring fixed – we move the pieces but in the end it "looks the same". That is, is the stabilizer of every position of the cube trivial? It seems that the answer is yes; note that it is enough to prove that for the original position (as stabilizers of elements in the same orbit are conjugate subgroups). Here, it seems that the key point is to consider the corner pieces and then the edge pieces.

# Part 4. The Symmetric Group

## 18. Conjugacy classes

Let $\sigma \in S_n$. We write $\sigma$ as a product of disjoint cycles:

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_r.$$

Since disjoint cycles commute, the order does not matter and we may assume that the length of the cycles is non-increasing. Namely, if we let $|(i_1 i_2 \dots i_t)| = t$ (we shall call it the length of the cycle; it is equal to its order as an element of $S_n$), then

$$|\sigma_1| \geq |\sigma_2| \geq \cdots \geq |\sigma_r|.$$

We may also allow cycles of length 1 (they simple stand for the identity permutation) and then we find that

$$n = |\sigma_1| + |\sigma_2| + \cdots + |\sigma_r|.$$

We therefore get a **partition** $p(\sigma)$ of the number $n$, that is, a set of non-increasing positive integers $a_1 \geq a_2 \geq \cdots \geq a_r \geq 1$ such that $n = a_1 + a_2 + \cdots + a_r$. Note that every partition is obtained from a suitable $\sigma$.

**Lemma 18.0.1.** *Two permutations, $\sigma$ and $\rho$, are conjugate (namely there is a $\tau$ such that $\tau\sigma\tau^{-1} = \rho$) if and only if $p(\sigma) = p(\rho)$.*

*Proof.* Recall the formula we used before, if $\sigma(i) = j$ then $(\tau\sigma\tau^{-1})(\tau(i)) = \tau(j)$. This implies that for every cycle $(i_1\ i_2 \dots i_t)$ we have

$$\tau(i_1\ i_2 \dots i_t)\tau^{-1} = (\tau(i_1)\ \tau(i_2) \dots \tau(i_t)).$$

In particular, since $\tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1})(\tau\sigma_2\tau^{-1}) \cdots (\tau\sigma_r\tau^{-1})$, a product of disjoint cycles, we get that $p(\sigma) = p(\tau\sigma\tau^{-1})$.

Conversely, suppose that $p(\sigma) = p(\rho)$. Say

$$\begin{aligned}\sigma &= \sigma_1\sigma_2 \dots \sigma_r \\ &= (i_1^1 \dots i_{t(1)}^1)(i_1^2 \dots i_{t(2)}^2) \dots (i_1^r \dots i_{t(r)}^r),\end{aligned}$$

and

$$\begin{aligned}\rho &= \rho_1\rho_2 \dots \rho_r \\ &= (j_1^1 \dots j_{t(1)}^1)(j_1^2 \dots j_{t(2)}^2) \dots (j_1^r \dots j_{t(r)}^r).\end{aligned}$$

Define $\tau$ by

$$\tau(i_b^a) = j_b^a.$$

Then $\tau\sigma\tau^{-1} = \rho$. □

**Corollary 18.0.2.** *Let $p(n)$ be the number of partitions of $n$.*[11] *There are $p(n)$ conjugacy classes in $S_n$.*

Next, we discuss conjugacy classes in $A_n$. Note that if $\sigma \in A_n$ then since $A_n \lhd S_n$ also $\tau\sigma\tau^{-1} \in A_n$. That is, all the $S_n$-conjugacy classes of elements of $A_n$ are in $A_n$. However, we would like to consider the $A_n$-conjugacy classes of elements of $A_n$.

[11] Since $2 = 2 = 1+1,\ 3 = 3 = 2+1 = 1+1+1,\ 4 = 4 = 2+2 = 3+1 = 2+1+1 = 1+1+1+1,\ 5 = 5 = 3+2 = 4+1 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1 \dots$ we get $p(1) = 1, p(2) = 2, p(3) = 3, p(4) = 5, p(5) = 7, p(6) = 11, \dots$. The function $p(n)$ is asymptotic to $\frac{e^{\pi\sqrt{2n/3}}}{4n\sqrt{3}}$.

**Lemma 18.0.3.** *The $S_n$-conjugacy class of an element $\sigma \in A_n$ is a disjoint union of $[S_n : A_n\mathrm{Cent}_{S_n}(\sigma)]$ $A_n$-conjugacy classes. In particular, it is a single $A_n$-conjugacy class if there is an odd permutation commuting with $\sigma$ and it decomposes into two $A_n$-conjugacy class if there is no odd permutation commuting with $\sigma$. In the latter case, the $S_n$-conjugacy class of $\sigma$ is the disjoint union of the $A_n$-conjugacy class of $\sigma$ and the $A_n$-conjugacy class of $\tau\sigma\tau^{-1}$, where $\tau$ can be chosen to be any odd permutation, and these two conjugacy classes have the same size.*

*Proof.* Let $A$ be the $S_n$-conjugacy class of $\sigma$. Write $A = \coprod_{\alpha \in J} A_\alpha$, a disjoint union of $A_n$-conjugacy classes. We first note that $S_n$ acts on the set $B = \{A_\alpha : \alpha \in J\}$. Indeed, if $A_\alpha$ is the $A_n$-conjugacy class of $\sigma_\alpha$, and $\rho \in S_n$ then define $\rho A_\alpha \rho^{-1}$ to be the $A_n$-conjugacy class of $\rho\sigma_\alpha\rho^{-1}$. This is well defined: if $\sigma'_\alpha$ is another representative for the $A_n$-conjugacy class of $\sigma_\alpha$ then $\sigma'_\alpha = \tau\sigma_\alpha\tau^{-1}$ for some $\tau \in A_n$. It follows that $\rho\sigma'_\alpha\rho^{-1} = \rho\tau\sigma_\alpha\tau^{-1}\rho^{-1} = (\rho\tau\rho^{-1})(\rho\sigma_\alpha\rho^{-1})(\rho\tau\rho^{-1})^{-1}$ is in the $A_n$-conjugacy class of $\rho\sigma_\alpha\rho^{-1}$ (because $\rho\tau\rho^{-1} \in A_n$). The action of $S_n$ is clearly transitive on $B$.

Consider the $A_n$-conjugacy class of $\sigma$ and denote it by $A_0$. The stabilizer of $A_0$ in $S_n$ is just $A_n\mathrm{Cent}_{S_n}(\sigma)$. Indeed, $\rho A_0 \rho^{-1} = A_0$ if and only if $\rho\sigma\rho^{-1}$ is in the same $A_n$-conjugacy class as $\sigma$. Namely, if and only if $\rho\sigma\rho^{-1} = \tau\sigma\tau^{-1}$ for some $\tau \in A_n$, equivalently, $(\tau^{-1}\rho)\sigma = \sigma(\tau^{-1}\rho)$, that is $(\tau^{-1}\rho) \in \mathrm{Cent}_{S_n}(\sigma)$ which is to say that $\rho \in A_n\mathrm{Cent}_{S_n}(\sigma)$.

We conclude that the size of $B$ is the length of the orbit of $A_0$ under the action of $S_n$ and hence is of size $[S_n : A_n\mathrm{Cent}_{S_n}(\sigma)]$. Since $[S_n : A_n] = 2$, we get that $[S_n : A_n\mathrm{Cent}_{S_n}(\sigma)] = 1$ or $2$, with the latter happening if and only if $A_n \supseteq \mathrm{Cent}_{S_n}(\sigma)$. That is, if and only if $\sigma$ does not commute with any odd permutation. Moreover, the orbit consists of the $A_n$-conjugacy classes of the elements $g\sigma g^{-1}$, $g$ running over a complete set of representatives for the cosets of $A_n\mathrm{Cent}_{S_n}(\sigma)$ in $S_n$.

Finally, if there are two $A_n$ orbits, say $\mathrm{Conj}_{A_n}(\sigma)$ and $\mathrm{Conj}_{A_n}(g\sigma g^{-1})$, then the function from $\mathrm{Conj}_{A_n}(\sigma)$ to $\mathrm{Conj}_{A_n}(g\sigma g^{-1})$ taking $h\sigma h^{-1}$ to $gh\sigma h^{-1}g^{-1}$ is a well-defined (check!) bijection as its inverse is given by conjugating by $g^{-1}$. □

In the case we need this lemma, that is in the case of $A_5$, one can decide the situation "by inspection". However, it is interesting to understand in general when does the centralizer of a permuation contain an odd permutation.

**Lemma 18.0.4.** *Let $\sigma$ be a permutation and write $\sigma$ as a product of disjoint cycles of non-increasing length:*

$$\sigma = c_1c_2\cdots c_a = (i_1^1, i_2^1, \dots, i_{r_1}^1)(i_1^2, \dots, i_{r_2}^2)\cdots(i_1^a, \dots, i_{r_a}^a).$$

*Thus, $r_1 \geq r_2 \geq \cdots \geq r_a$ where we have also listed cycles of length 1, if any. The centralizer of $\sigma$ contains an odd permutation unless each cycle has odd length and all the lengths are different, that is, unless each $r_i$ is odd and $r_1 > r_2 > \cdots > r_a$. In that case, the centralizer of $\sigma$ consists of even permutations only.*

*Proof.* Suppose first that there is a cycle $c_j$ of even length, which is thus an odd permutation. Since disjoint cycles commute $c_jc_ic_j^{-1} = c_i$ and so

$$c_j\sigma c_j^{-1} = (c_jc_1c_j^{-1})(c_jc_2c_j^{-1})\cdots(c_jc_ac_j^{-1}) = c_1\cdots c_a = \sigma.$$

Thus, the centralizer of $\sigma$ contains the odd permutation $c_j$.

Suppose now that there are two cycles of the same length. To ease notation, let's assume these are $c_1$ and $c_2$, but the same argument works in general. We may assume that they are both of odd length, otherwise we have already shown that the centralizer contains an odd permutation. Then, let $\tau = (i_1^1 i_1^2)(i_2^1 i_2^2)\cdots(i_{r_1}^1 i_{r_1}^2)$. Then $\tau$ is an odd permutation and we find $\tau\sigma\tau^{-1} = \sigma$.

The case left at this point is when $\sigma$ is a product of disjoint cycles, all of odd lengths and strictly decreasing order: $r_1 > r_2 > \cdots > r_a$. In this case, if $\tau\sigma\tau^{-1} = \sigma$ – that is, if

$$(\tau(i_1^1), \tau(i_2^1), \ldots, \tau((i_{r_1}^1))(\tau(i_1^2), \ldots, \tau((i_{r_2}^2)) \cdots (\tau(i_1^a), \ldots, \tau(i_{r_a}^a))$$
$$= (i_1^1, i_2^1, \ldots, i_{r_1}^1)(i_1^2, \ldots, i_{r_2}^2) \cdots (i_1^a, \ldots, i_{r_a}^a),$$

then, by comparing sizes of cycles, we see that $\tau c_i \tau^{-1} = c_i$. But that means that $\tau = c_1^{b_1} c_2^{b_2} \cdots c_a^{b_a}$ for some integers $b_i$ and so $\tau$ is even. □

## 19. THE SIMPLICITY OF $A_n$

In this section we prove that $A_n$ is a simple group for $n \neq 4$. The cases where $n < 4$ are trivial; for $n = 4$ we have seen it fails (the Klein 4-group is normal). We shall focus on the case $n \geq 5$ and prove the theorem inductively. We therefore first consider the case $n = 5$.

We make the following general observation:

**Lemma 19.0.1.** *Let $N \lhd G$ then $N$ is a disjoint union of $G$-conjugacy classes.*

*Proof.* Distinct conjugacy classes, being orbits for a group action, are always disjoint. If $N$ is normal and $n \in N$ then its conjugacy class $\{gng^{-1} : g \in G\}$ is contained in $N$. □

Let us list the conjugacy classes of $S_5$ and their sizes.

Conjugacy classes in $S_5$

| cycle type | representative | size of conjugacy class | order | even? |
|---|---|---|---|---|
| 5 | (12345) | 24 | 5 | ✓ |
| 1+4 | (1234) | 30 | 4 | × |
| 1+1+3 | (123) | 20 | 3 | ✓ |
| 1+ 2+ 2 | (12)(34) | 15 | 2 | ✓ |
| 1 + 1 + 1 + 2 | (12) | 10 | 2 | × |
| 1 + 1+ 1+ 1+ 1 | 1 | 1 | 1 | ✓ |
| 2+ 3 | (12)(345) | 20 | 6 | × |

Let $\tau$ be a permutation commuting with (12345). Then

$$(12345) = \tau(12345)\tau^{-1} = (\tau(1)\ \tau(2)\ \tau(3)\ \tau(4)\ \tau(5))$$

and so $\tau$ is the permutation $i \mapsto i + n$ for $n = \tau(1) - 1$. In particular, $\tau = (12345)^{n-1}$ and so is an even permutation. We conclude that the $S_5$-conjugacy class of (12345) breaks into two $A_5$-conjugacy classes, with representatives (12345), (21345).

One checks that (123) commutes with the odd permutation (45). Therefore, the $S_5$-conjugacy class of (123) is also an $A_5$-conjugacy class. Similarly, the permutation $(12)(34)$ commutes with the odd permutation $(12)$. Therefore, the $S_5$-conjugacy class of $(12)(34)$ is also an $A_5$-conjugacy class. We get the following table for conjugacy classes in $A_5$.

Conjugacy classes in $A_5$

| cycle type | representative | size of conjugacy class |
|---|---|---|
| 5 | (12345) | 12 |
| 5 | (21345) | 12 |
| 1+1+3 | (123) | 20 |
| 1+ 2+ 2 | (12)(34) | 15 |
| 1 + 1+ 1+ 1+ 1 | 1 | 1 |

If $N \lhd A_5$ then $|N|$ divides 60 and is the sum of 1 and some of the numbers in $(12, 12, 20, 15)$. One checks that this is impossible unless $N = A_5$. We deduce

**Lemma 19.0.2.** *The group $A_5$ is simple.*

The family of cyclic groups of prime order are an infinite family of simple group, but this is a rather elementary fact. We are now in a position to exhibit an infinite family of simple groups that is much more interesting.

**Theorem 19.0.3.** *The group $A_n$ is simple for $n \geq 5$.*

*Proof.* The proof is by induction on $n$. We may assume that $n \geq 6$. Let $N$ be a normal subgroup of $A_n$ and assume $N \neq \{1\}$.

First step: There is a permutation $\rho \in N, \rho \neq 1$ and $1 \leq i \leq n$ such that $\rho(i) = i$.

Indeed, let $\sigma \in N$ be a non-trivial permutation and write it as a product of disjoint non-trivial cycles, $\sigma = \sigma_1\sigma_2 \dots \sigma_s$, say in decreasing length. Suppose that $\sigma_1$ is $(i_1 i_2 \dots i_r)$, where $r \geq 3$. We write $\sigma_2 = (i_{r+1} \cdots)$ and so on.

Then, conjugating by the transposition $\tau = (i_1 i_2)(i_5 i_6)$, we get that $\tau\sigma\tau^{-1}\sigma \in N$, $\tau\sigma\tau^{-1}\sigma(i_1) = i_1$ and if $r > 3$ $\tau\sigma\tau^{-1}\sigma(i_2) = i_4 \neq i_2$.

If $r = 3$ then $\sigma = (i_1 i_2 i_3)(i_4 \dots) \dots$ and we choose instead $\tau = (i_1 i_2)(i_3 i_4)$. Then $\tau\sigma\tau^{-1}\sigma(i_1) = i_1$ and $\tau\sigma\tau^{-1}\sigma(i_2) = \tau\sigma(i_4) \in \{i_3, i_5\}$, depending on whether $\sigma_2 = (i_4)$ or is a cycle of length greater than 1. Thus, $\tau\sigma\tau^{-1}\sigma$ is a permutation of the kind we were seeking.

It still remains to consider the case where each $\sigma_i$ is a transposition. Then, if $\sigma = (i_1 i_2)(i_3 i_4)$ then $\sigma$ moves only 4 elements out of $N$, and thus fixes some element and we are done. Otherwise, $\sigma = (i_1 i_2)(i_3 i_4)(i_5 i_6) \dots$. Let $\tau = (i_1 i_2)(i_3 i_5)$ then

$$[\tau\sigma\tau^{-1}]\sigma = [(i_2 i_1)(i_5 i_4)(i_3 i_6) \dots](i_1 i_2)(i_3 i_4)(i_5 i_6) \cdots = (i_3 i_5)(i_4 i_6) \dots$$

and so is a permutation of the sort we were seeking.

Second step: $N = A_n$.

Consider the subgroups $G_i = \{\sigma \in A_n : \sigma(i) = i\}$. We note that each $G_i$ is isomorphic to $A_{n-1}$ and hence, by the induction hypothesis, is simple. By the preceding step, for some $i$ we have that $N \cap G_i$ is a non-trivial normal subgroup of $G_i$, hence equal to $G_i$.

Next, note that $(12)(34)G_1(12)(34) = G_2$ and, similarly, all the groups $G_i$ are conjugate in $A_n$ to each other. It follows that $N \supseteq < G_1, G_2, \dots, G_n >$. Now, every element in $S_n$ is a product of (usually not disjoint) transpositions and so every element $\sigma$ in $A_n$ is a product of an even number of transpositions, $\sigma = \lambda_1\mu_1 \dots \lambda_r\mu_r$ ($\lambda_i, \mu_i$ transpositions). Since $n > 4$ every product $\lambda_i\mu_i$ belongs to some $G_j$ and we conclude that $< G_1, G_2, \dots, G_n >= A_n$, therefore also $N = A_n$. □

# **Part** 5. *p*-groups, Cauchy's and Sylow's Theorems

## 20. THE CLASS EQUATION

Let $G$ be a finite group. $G$ acts on itself by conjugation: $g * h = ghg^{-1}$. The orbits are called in this case **conjugacy classes**.The **class equation** follows from the partitioning of $G$ into orbits obtained this way. Since $G$ is partitioned into disjoint conjugacy classes, its cardinality is the sum of the cardinalities of its conjugacy classes. We shall denote a conjugacy class of an element $x$ by $\mathrm{Conj}(x)$. Thus,

$$\mathrm{Conj}(x) = \{gxg^{-1} : g \in G\}.$$

Note that the stabilizer of $x \in G$ is $\mathrm{Cent}_G(x) := \{g \in G : gxg^{-1} = x\}$ and so its orbit has length $[G : \mathrm{Cent}_G(x)]$. That is,

$$|\mathrm{Conj}(x)| = [G : \mathrm{Cent}_G(x)].$$

Note that the elements with orbit of length 1 are precisely the elements in the center $Z(G)$ of $G$. We get the class equation

$$|G| = |Z(G)| + \sum_{\text{reps.} x \notin Z(G)} \frac{|G|}{|\mathrm{Cent}_G(x)|}. \tag{3}$$

**Theorem 20.0.1.** *Let $N \geq 1$ be a positive integer. Up to isomorphism there are finitely many finite groups with $N$ conjugacy classes.*

*Proof.* We will need the following easy lemma:

**Lemma 20.0.2.** *Fix an integer $M$. There are finitely many groups, up to isomorphism, of order $M$.*

*Proof.* We may assume that such a group is always specified by providing a group law on some fixed set with $M$ elements. Say, $X = \{x_1, \dots, x_M\}$. A group law on this set is specified by a function

$$m : X \times X \to X.$$

But there are finitely many such functions $m$. □

We can of course strengthen the Lemma as follows

**Corollary 20.0.3.** *Fix an integer $M$. There are finitely many groups, up to isomorphism, of order at most $M$.*

It would therefore suffice to prove that the size of a finite group with $N$ conjugacy classes is bounded in terms of $N$ alone. We require the following:

**Lemma 20.0.4.** *Let $q$ be a positive rational number and $N$ a fixed integer. There are finitely many tuples of positive integers $(n_1, \dots, n_N)$ such that*

$$q = \frac{1}{n_1} + \cdots + \frac{1}{n_N}.$$

*Proof.* We argue by induction on $N$. The case $N = 1$ is clear. Assume for $N - 1$. To prove finiteness we may assume that $n_1 \geq n_2 \geq \cdots \geq n_N$ (as every tuple can be rearranged to satisfy this condition and at most $N!$ tuples will give a given tuple $(n_1, \dots, n_N)$ that satisfies the inequalities). Now,

$$q = \frac{1}{n_1} + \cdots + \frac{1}{n_N} \leq \frac{N}{n_N}$$

and consequently

$$n_N \leq \frac{N}{q}.$$

Thus, there are finitely many possibilities for the integer $n_N$. For each such possibility consider

$$q' := q - \frac{1}{n_N} = \frac{1}{n_1} + \cdots + \frac{1}{n_{N-1}}.$$

By induction, there are finitely many tuples $(n_1, \ldots, n_{N-1})$ that satisfy this equality. □

We now come back to the proof of the theorem. We saw that it is enough to prove that if $G$ has $N$ conjugacy classes then the order of $G$ is bounded.

Use the class equation to write

$$1 = \underbrace{\frac{1}{|G|} + \cdots + \frac{1}{|G|}}_{|Z(G)|-\text{times}} + \sum_{\text{reps.} x \notin Z(G)} \frac{1}{|\mathrm{Cent}_G(x)|}.$$

There are $N$ summands in this equation. By the Lemma, there are finitely many ways to write 1 as the sum of such $N$ summands and so the maximal denominator appearing in all these equations is bounded by some constant $M$. But in each such expression the maximal denominator is the order of the group. Thus, the order of each group with $N$ conjugacy classes is bounded by $M$. □

**Example 20.0.5.** Let us consider some simple cases of the theorem.

(1) $N = 1$. Then we have $1 = \frac{1}{1}$ and there is one group with one conjugacy class which is $\{1\}$.
(2) $N = 2$. The only possibility is $1 = \frac{1}{2} + \frac{1}{2}$. The order of the group is thus 2 and there is one group of order 2 up to isomorphism: $\mathbb{Z}/2\mathbb{Z}$.
(3) $N = 3$. Here we find three possibilities: $1 = \frac{1}{3} + \frac{1}{3} + \frac{1}{3} = \frac{1}{6} + \frac{1}{3} + \frac{1}{2} = \frac{1}{4} + \frac{1}{4} + \frac{1}{2}$. The first possibility should be associated to a group of order 3 and there is one such group up to isomorphism (3 is prime): $\mathbb{Z}/3\mathbb{Z}$. It indeed has 3 conjugacy classes.

   The next possibility should be associated with a group of order 6. The group $S_3$ has order 6 and 3 conjugacy classes of orders $1, 2$ and 3 and gives the class equation $1 = \frac{1}{6} + \frac{1}{3} + \frac{1}{2}$.

   The third possibility should be associated to a group of order 4. But all groups of order 4 are abelian (using the Table on page 10) and thus have 4 conjugacy classes. So the expression $1 = \frac{1}{4} + \frac{1}{4} + \frac{1}{2}$ doesn't actually come from a group.

## 21. $p$-GROUPS

Let $p$ be a prime. A finite group $G$ is called a ***p*-group** if its order is a positive power of $p$. Thus, we talk about a 2-group, a 3-group, etc.

**Lemma 21.0.1.** *Let $G$ be a finite $p$-group. Then the center of $G$ is not trivial.*

*Proof.* We use the Class Equation (3). Note that if $x \notin Z(G)$ then $\mathrm{Cent}_G(x) \neq G$ and so the integer $\frac{|G|}{|\mathrm{Cent}_G(x)|}$ is divisible by $p$. Thus, the left hand side of

$$|G| - \sum_{\text{reps.} x \notin Z(G)} \frac{|G|}{|\mathrm{Cent}_G(x)|} = |Z(G)|$$

is divisible by $p$, hence so is the right hand side. In particular $|Z(G)| \geq p$. □

**Theorem 21.0.2.** *Let $G$ be a finite $p$-group, $|G| = p^n$.*

(1) *For every normal subgroup $H \lhd G$, $H \neq G$, there is a subgroup $K \lhd G$ such that $H < K < G$ and $[K : H] = p$.*

(2) *There is a chain of subgroups $H_0 = \{1\} < H_1 < \cdots < H_n = G$, such that each $H_i \lhd G$ and $|H_i| = p^i$.*

*Proof.* (1) The group $G/H$ is a $p$-group and hence its center is a non-trivial group. Take an element $e \neq x \in Z(G/H)$; its order is $p^r$ for some $r$. Then $y = x^{p^{r-1}}$ has exact order $p$. Let $K' =< y >$. It is a normal subgroup of $G/H$ of order $p$ ($y$ commutes with any other element). Let $K = \pi_H^{-1}(K')$. By the Third Isomorphism Theorem, $K$ is a normal subgroup of $G$, $K/H \cong K'$ so $[K : H] = p$.

(2) The proof just given shows that every $p$-group has a normal subgroup of $p$ elements. Now apply repeatedly the first part.

□

A variant of the theorem above is the following, slightly harder, proposition.

**Proposition 21.0.3.** *Let $G$ be a $p$-group and let $H$ be a proper subgroup of $G$, then there is a subgroup $H^+ \supset H$ such that $[H^+ : H] = p$ and, if $H$ is not the identity subgroup, there is a subgroup $H^- \subset H$ such that $[H : H^-] = p$.*

*Proof.* We argue by induction on the order of $G$. If $|G| = p$, the Proposition is clear. Assume the result for groups of order $p^r$ and let $G$ have order $p^{r+1}$ with $r \geq 1$. From the Theorem applied to $H = \{1\}$, we know that $G$ has a normal subgroup with $p$ elements, say $J$. If $J$ is not contained in $H$ let $H^+ = JH$. As $J$ is normal, $H^+$ is a subgroup and $|H^+| = |J| \cdot |H|/|J \cap H| = p \cdot |H|$.

If $J \subseteq H$, consider $G/J$ that has order $p^r$ and the proper subgroup $H/J$. By induction, there is a subgroup $K$ of $G/J$ in which $H/J$ is contained with index $p$. Let $H^+$ be the pre-image of $K$ under the natural homomorphism $G \to G/J$. Then $H^+ \supset H$ and $[H^+ : H] = \frac{|H^+|}{|H|} = \frac{|H^+|/|J|}{|H|/|J|} = \frac{|K|}{|H/J|} = [K : (H/J)] = p$. This finishes the first part of the Proposition.

As to the second part, this follows easily from the Theorem: $H$ is itself a $p$-group and so it has a series of subgroups as in part (2) of the theorem, in particular a subgroup of index $p$. □

## 21.1. **Examples of $p$-groups.**

21.1.1. *Groups of order $p$.* We proved in the assignments that every such group is cyclic, thus isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

21.1.2. *Groups of order $p^2$.* We first prove a general result.

**Lemma 21.1.1.** *Let $G$ be a group and $H \subset Z(G)$ a subgroup. Suppose that $G/H$ is cyclic. Then $G$ is abelian.*

*Proof.* First note that $H$ is normal, because it consists of elements in the centre. Let $g \in G$ be an element such that $\langle \bar{g} \rangle = G/H$, where $\bar{g}$ denotes the image of $g$ in $G/H$. Then every element of $G$ is of the form $g^i h$ for some integer $i \in \mathbb{Z}$ and $h \in H$.

Given $x, y \in G$ write them in this form as $x = g^i h, y = g^j h'$. Then, as $h$ and $h'$ commute with any element we find that $xy = g^i h g^j h' = g^j g^i h h' = g^j h' g^i h = yx$. □

Let $G$ be a group of $p^2$ elements, then $Z(G) \neq \{1\}$ and so there is an element $g \in Z(G)$ of order $p$. Let $H = \langle g \rangle$, a subgroup of order $p$. Then $G/H$ has $p$-elements and hence is cyclic. The Lemma applies and we conclude $G$ is abelian. We pass to additive notation.

We now distinguish two cases.

(1) There is an element of order $p^2$ in $G$. Then $G$ is cyclic and so isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$.
(2) Every element of $G$, different from $\{0\}$ is of order $p$. That is, $pg = 0$ for all $g \in G$. Recall first that for every $n \in \mathbb{Z}$ we have the element $ng$ ($g^n$ in multiplicative notation) and the following holds

$$(n+m)g = ng + mg, \quad n(gh) = ng + nh.$$

In our case, also

$$(n+p)g = ng + pg = ng.$$

Therefore, we an make $G$ into a vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, where we define

$$\bar{n}g := ng,$$

where $n$ is any representative of the congruence class $\bar{n}$.

As such, $G$ is isomorphic to $\mathbb{F}_p^2$ as a vector space, in particular as a group. That is, $G$ is the group $(\mathbb{Z}/p\mathbb{Z})^2$ and, in fact, up to isomorphism, these are the only groups of order $p^3$.

That completes the classification of groups of order $p^2$.

21.1.3. *Groups of order $p^3$.* First, there are the abelian groups $\mathbb{Z}/p^3\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and $(\mathbb{Z}/p\mathbb{Z})^3$.

We have seen in Lemma 21.1.1 that if $G$ is not abelian then $G/Z(G)$ cannot be cyclic. It follows that $Z(G) \cong \mathbb{Z}/p\mathbb{Z}$ and $G/Z(G) \cong (\mathbb{Z}/p\mathbb{Z})^2$. One example of such a group is provided by the matrices

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix},$$

where $a, b, c \in \mathbb{F}_p$. Note that if $p \geq 3$ then every element in this group is of order $p$ (use $(I + N)^p = I + N^p$), yet the group is non-abelian. (This group, using a terminology to be introduced later, is a semi-direct product $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$.) More generally the upper unipotent matrices in $\mathrm{GL}_n(\mathbb{F}_p)$ are a group of order $p^{n(n-1)/2}$ in which every element has order $p$ if $p \geq n$. Notice that these groups are non-abelian.

Getting back to the issue of non-abelian groups of order $p^3$, one can prove that there is precisely one additional non-abelian group of order $p^3$. It is generated by two elements $x, y$ satisfying: $x^p = y^{p^2} = 1, xyx^{-1} = y^{1+p}$. (This group is a semi-direct product $(\mathbb{Z}/p^2\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}$.)

21.2. **The Frattini subgroup.** Let $G$ be a group. Define the **Frattini subgroup** $\Phi(G)$ of $G$ to be the intersection of all maximal subgroups of $G$, where by a **maximal subgroup** we mean a subgroup of $G$, not equal to $G$ and not strictly contained in any proper subgroup of $G$. If $G$ has no such subgroup (for example, if $G = \{1\}$, or if $G = \mathbb{Q}$ with addition) then we define $\Phi(G) = G$.

**Proposition 21.2.1.** *Let $G$ be a finite $p$-group. The Frattini subgroup of $G$ is a normal subgroup of $G$ and has the following properties:*

*(1) $G/\Phi(G)$ is a non-trivial abelian group and every non-zero element in it has order $p$. It is the largest quotient of $G$ with this property.*
*(2) $\Phi(G) = G^pG'$, where $G'$ is the commutator subgroup of $G$ and $G^p$ is the subgroup of $G$ generated by the set $\{g^p : g \in G\}$.*

*Proof.* Any automorphism $f\colon G \to G$ takes maximal subgroups to maximal subgroups, in particular, conjugation does. Therefore, $\Phi(G)$ is a normal subgroup.

Since any maximal subgroup $H$ has index $p$ (by our previous results), it follows from Exercise 37 that $H$ is normal because $p$ is the minimal prime dividing the order of $G$. Thus, $G/H$ is a group with $p$ elements and thus abelian. Therefore, $H \supseteq G'$. It follows that $\Phi(G) \supset G'$ and therefore $G/\Phi(G)$ is abelian. Further, let $g \in G$ then $gH$ has order 1 or $p$ in $G/H$ and, in particular $g^pH = (gH)^p = H$. That is, $H \supset G^p$ and so $\Phi(G) \supseteq G^pG'$ and every non-trivial element of $G/\Phi(G)$ has order $p$.

Let $N$ be a normal subgroup of $G$ and suppose $G/N$ is abelian and killed by $p$. The same argument as above shows that $N \supseteq G^pG'$. Therefore, once we show $\Phi(G) = G^pG'$ we will get the first part of the Theorem too.

It remains to show that $\Phi(G) \subseteq G^pG'$. First, note that since $G'$ is normal in $G$, indeed $G^pG'$ is a subgroup of $G$ and in fact a normal subgroup of $G$ as $G^p$ is a normal subgroup too (since $gx^pg^{-1} = (gxg^{-1})^p$, the set of generators of $G^p$, hence $G^p$ itself, is stable under conjugation). Let us also note that $G/G^pG'$ is an abelian group in which every element has order $p$. Therefore, similar to what we have done for groups of order $p^2$, we may view $G/G^pG'$ as a vector space over $\mathbb{F}_p$.

If $G/G^pG'$ is cyclic it has a unique maximal subgroup $\{0\}$ and its preimage $G^pG'$ is a maximal subgroup of $G$, in particular containing $\Phi(G)$. Suppose then that $G/G^pG'$ is not cyclic. Suppose there is an element $g \in \Phi(G) \setminus G^pG'$. Pass to $G/G^pG'$ and to the image $\bar{g}$ of $g$ in it. Then $\bar{g} \neq 0$ and $G/G^pG'$ is isomorphic to $\mathbb{F}_p^r$ for some $r > 1$, where $\mathbb{F}_p$ is the field of $p$ elements $\mathbb{Z}/p\mathbb{Z}$. In this perspective $\bar{g}$ is viewed as a non-zero vector. In that case, we can find a hyperplane $W$ of codimension 1, such that $\bar{g} \notin W$. The pre-image of $W$ in $G$ is a maximal subgroup that doesn't contain $g$ and that's a contradiction. ☐

## 22. Cauchy's Theorem

One application of group actions is to provide a simple proof of an important theorem in the theory of finite groups – Cauchy's theorem. We remark that Cauchy's theorem will not be used in the proof of Sylow's theorem below, and, in fact, is an easy consequence of Sylow's theorem. The reason we prove it here is simply to illustrate an ingenious use of group actions.

**Theorem 22.0.1.** *(Cauchy) Let $G$ be a finite group of order $n$ and let $p$ be a prime dividing $n$. Then $G$ has an element of order $p$.*

*Proof.* Let $S$ be the set consisting of $p$-tuples $(g_1, \dots, g_p)$ of elements of $G$, considered up to cyclic permutations. Thus, if $T$ is the set of $p$-tuples $(g_1, \dots, g_p)$ of elements of $G$, $S$ is the set of orbits for the action of $\mathbb{Z}/p\mathbb{Z}$ on $T$ by cyclic shifts . One may therefore apply **CFF** and get

$$|S| = \frac{n^p - n}{p} + n.$$

Note that $n \nmid |S|$ .

Now define an action of $G$ on $S$. Given $g \in G$ and $(g_1, \dots, g_p) \in S$ we define

$$g(g_1, \dots, g_p) = (gg_1, \dots, gg_p).$$

This is a *well-defined* action .

Since the order of $G$ is $n$, since $n \nmid |S|$, and since $S$ is a disjoint union of orbits of $G$, there must be an orbit $\mathrm{Orb}(s)$ whose size is not $n$. However, the size of an orbit is $|G|/|\mathrm{Stab}(s)|$, and we conclude that there must an element $(g_1, \dots, g_p)$ in $S$ with a non-trivial stabilizer. This means that for some $g \in G$, such that $g \neq e$, we have

$$(gg_1, \dots, gg_p) \text{ is equal to } (g_1, \dots, g_p) \text{ up to a cyclic shift.}$$

This means that for some $i$ we have

$$(gg_1, \dots, gg_p) = (g_{i+1}, g_{i+2}, g_{i+3}, \dots, g_p, g_1, g_2, \dots, g_i).$$

Therefore, $gg_1 = g_{i+1}$, $g^2 g_1 = gg_{i+1} = g_{2i+1}, \dots, g^p g_1 = \cdots = g_{pi+1} = g_1$ (we always read the indices mod $p$). That is, there exists $g \neq e$ with

$$g^p = e.$$

□

## 23. Sylow's Theorem

Sylow's theorem is one of the main results proven in this course. It states that a finite group $G$ always has $p$-subgroups as large as is possible given Lagrange's theorem. It is easy to see that $G$ is generated by these groups. At the same time, we have gained some understanding into the structure of $p$-groups above. Thus, at some vague conceptual level, the combination of the two –Sylow's theorem and the theory of $p$-groups – gives us a better understanding of all finite groups.

### 23.1. Proof of Sylow's theorem.

Let $G$ be a finite group and let $p$ be a prime dividing its order. Write $|G| = p^r m$, where $(p, m) = 1$. By a $p$-subgroup of $G$ we mean a subgroup whose order is a positive power of $p$. By a **maximal $p$-subgroup** of $G$ we mean a $p$-subgroup of $G$ not contained in a strictly larger $p$-subgroup.

**Theorem 23.1.1.** *Let $G$ be a finite group and let $p$ be a prime dividing its order. Write $|G| = p^r m$, where $(p, m) = 1$.*

*(1) Every maximal $p$-subgroup of $G$ has order $p^r$ (such a subgroup is called a* **Sylow $p$-subgroup***) and such a subgroup exists.*
*(2) All Sylow $p$-subgroups are conjugate to one another.*
*(3) The number $n_p$ of Sylow $p$-subgroups satisfies:*
  *(a) $n_p | m$;*
  *(b) $n_p \equiv 1 \pmod{p}$.*

*Remark* 23.1.2. To say that $P$ is conjugate to $Q$ means that there is a $g \in G$ such that $gPg^{-1} = Q$. Recall that the map $x \mapsto gxg^{-1}$ is an automorphism of $G$. This implies that $P$ and $Q$ are isomorphic as groups.

Another consequence is that saying that there is a unique $p$-Sylow subgroup is the same as saying that a $p$-Sylow is normal. This is often used this way: given a finite group $G$ the first question in ascertaining whether it is simple or not is to ask whether a $p$-Sylow subgroup is unique for some $p$ dividing the order of $G$. Often one engages in combinatorics of counting $p$-Sylow subgroups, trying to conclude there can be only one for a given $p$, and hence getting a normal subgroup.

We first prove a lemma that is a special case of Cauchy's Theorem 22.0.1, but much easier. Hence, we supply a self-contained proof that doesn't use Cauchy's theorem.

**Lemma 23.1.3.** *Let $A$ be a finite abelian group, let $p$ be a prime dividing the order of $A$. Then $A$ has an element of order $p$.*

*Proof.* We prove the result by induction on $|A|$. The base case $|A| = p$ is clear, of course. In the general case, let $N$ be a maximal subgroup of $A$, distinct from $A$. If $p$ divides the order of $N$ we are done by induction. Otherwise, let $x \notin N$ and let $B = \langle x \rangle$. By maximality the subgroup $BN$ is equal to $A$. On the other hand $|BN| = |B| \cdot |N| / |B \cap N|$. Thus, $p$ divides the order of $B$. That is, the order of $x$ is $pa$ for some $a$ and so the order of $x^a$ is precisely $p$. □

**Proposition 23.1.4.** *There is a $p$-subgroup of $G$ of order $p^r$.*

*Proof.* We prove the result by induction on the order of $G$, where the case $|G| = p$ is clear. Assume first that $p$ divides the order of $Z(G)$. Let $x$ be an element of $Z(G)$ of order $p$ and let $N = \langle x \rangle$, a normal subgroup. The order of $G/N$ is $p^{r-1}m$ and by induction it has a $p$-subgroup $H'$ of order $p^{r-1}$. (If $r - 1 = 0$ this still works by taking $H' = \{1\}$.) Let $H$ be the preimage of $H'$ in $G$. It is a subgroup of $G$ such that $H/N \cong H'$ and thus $H$ has order $|H'| \cdot |N| = p^r$.

Consider now the case where $p$ does not divide the order of $Z(G)$. Consider the class equation

$$|G| = |Z(G)| + \sum_{\text{reps.} x \notin Z(G)} \frac{|G|}{|\text{Cent}_G(x)|}.$$

As $p$ divides $|G|$ and not $|Z(G)|$, we see that for some $x \notin Z(G)$ we have that $p$ does not divide $\frac{|G|}{|\text{Cent}_G(x)|}$. Thus, $p^r$ divides $\text{Cent}_G(x)$. The subgroup $\text{Cent}_G(x)$ is a *proper* subgroup of $G$ because $x \notin Z(G)$. Thus, by induction, $\text{Cent}_G(x)$, and hence $G$, has a $p$-subgroup of order $p^r$. □

This result already has interesting consequences.

**Corollary 23.1.5.** *Let $p_1^{a_1} \cdots p_t^{a_t}$ be the prime factorization of $|G|$. Let $P_i$ be a subgroup of $G$ of order $p_i^{a_i}$, then*

$$G = \langle P_1, \dots, P_t \rangle.$$

*Proof.* Indeed, the right hand side is a subgroup of $G$ containing each $P_i$. Hence, its order is divisible by $p_1^{a_1} \cdots p_t^{a_t}$. It must therefore be equal to $G$. □

**Corollary 23.1.6.** *(Cauchy's theorem) Let $G$ be a finite group and $p$ a prime dividing the order of $G$, then $G$ has an element of order $p$.*

*Proof.* If we write $|G| = p^r m$ with $(m, p) = 1$ then we know that $G$ has a subgroup $P$ of order $p^r$. Let $x \in P$ be an element different than the identity. Then, by Lagrange, $\text{ord}(x) = p^b$ for some positive integer $b \leq r$. The element $x^{p^{b-1}}$ then has order $p$. □

The next ingredient we will need to prove Sylow's theorem is a technical lemma about normalizers. It will make more sense when we see it in action in the proof of the theorem.

**Lemma 23.1.7.** *Let $P$ be a maximal $p$-subgroup and $Q$ any $p$-subgroup then*

$$Q \cap P = Q \cap N_G(P).$$

*Proof.* Let $H = Q \cap N_G(P)$. Since $P \triangleleft N_G(P)$ we have that $HP$ is a subgroup of $N_G(P)$. Its order is $|H| \cdot |P|/|H \cap P|$ and so is a power of $p$. Since $P$ is a maximal $p$-subgroup we must have $HP = P$ and thus $H \subset P$. This means that $Q \cap N_G(P) = Q \cap N_G(P) \cap P = Q \cap P$. □

*Proof.* (of Sylow's Theorem) Let $P$ be a Sylow subgroup of $G$. Such exists by Proposition 23.1.4. Let

$$S = \{P_1, \dots, P_a\}$$

be the set of conjugates of $P = P_1$. That is, the subgroups $gPg^{-1}$ one gets by letting $g$ vary over $G$. Note that for a fixed $g$ the map $P \to gPg^{-1}$, $x \mapsto gxg^{-1}$ is a group isomorphism. Thus, every $P_i$ is a Sylow $p$-subgroup. Our task is to show that every maximal $p$-subgroup is an element of $S$ and find properties of $a$.

Let $Q$ be any $p$-subgroup of $G$. The subgroup $Q$ acts by conjugation on $S$. The size of $Orb(P_i)$ is $|Q|/|\text{Stab}_Q(P_i)|$. Now $\text{Stab}_Q(P_i) = Q \cap N_G(P_i) = Q \cap P_i$ by Lemma 23.1.7. Thus, the orbit consists of one element if $Q \subset P_i$ and is a proper power of $p$ otherwise.

Take first $Q$ to be $P_1$. Then, the orbit of $P_1$ has size 1. Since $P_1$ is a maximal $p$-subgroup it is not contained in any other $p$-subgroup, thus the size of every other orbit is a power of $p$. It follows, using that $S$ is a disjoint union of orbits, that $a = 1 + tp$ for some $t$. Note also that $a = |G|/|N_G(P)|$ and thus divides $|G|$.

We now show that all maximal $p$-subgroups are conjugate. Suppose, to the contrary, that $Q$ is a maximal $p$-subgroup which is not conjugate to $P$. Thus, for all $i$, $Q \neq P_i$ and so $Q \cap P_i$ is a proper subgroup of $Q$. It follows then that $S$ is a union of disjoint orbit all having size a proper power of $p$. Thus, $p|a$. This is a contradiction. □

23.2. **Examples and applications.**

23.2.1. *p-groups.* Every finite $p$-group is of course the only $p$-Sylow subgroup (trivial case).

23.2.2. $\mathbb{Z}/6\mathbb{Z}$. In every abelian group the $p$-Sylow subgroups are normal and unique. The 2-Sylow subgroup is $< 3 >$ and the 3-Sylow subgroup is $< 2 >$.

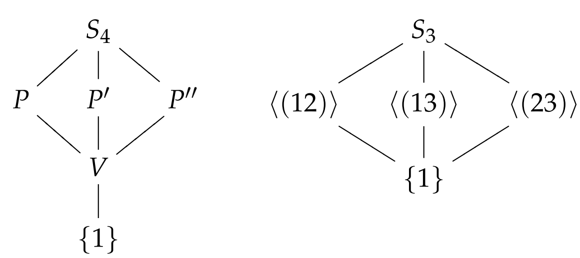
23.2.3. $S_3$. Consider the symmetric group $S_3$. Its 2-Sylow subgroups are given by $\{1, (12)\}$, $\{1, (13)\}, \{1, (23)\}$. There are thus three of them and note that indeed $3|m = 3!/2 = 3$ in this case, and $3 \equiv 1 \pmod 2$. The group $S_3$ has a unique 3-Sylow subgroup $\{1, (123), (132)\}$. This is expected since $n_3|2 = 3!/3$ and $n_3 \equiv 1 \pmod 3$ implies $n_3 = 1$.

23.2.4. $S_4$. We want to find the 2-Sylow subgroups. Their number is given by $n_2|3 = 24/8$ and is congruent to 1 modulo 2. It is thus either 1 or 3. Using the expression of a permutation as a product of disjoint cycles, we see that every element of $S_4$ has order $1, 2, 3$ or 4. The number of elements of order 3 is 8 (the 3-cycles) and so there are 16 elements of order $1, 2$ or 4. Thus, we cannot have a unique subgroup of order 8 (it will need to contain any element of order $1, 2$ or 4). We conclude that $n_2 = 3$. One such subgroup is $D_8 \subset S_4$; the rest are conjugates of it.

Further, $n_3|24/3$ and $n_3 \equiv 1 \pmod 3$. If $n_3 = 1$ then that unique 3-Sylow would need to contain all 8 element of order 3 but is itself of order 3. Thus, $n_3 = 4$.

*Remark* 23.2.1. A group of order 24 is never simple, though it does not mean that one of the Sylow subgroups is normal, as the example of $S_4$ shows. However, consider the representation of $S_4$ on the cosets of $P$, where $P$ is its 2-Sylow subgroup. As we have seen in Example 16.0.1, this coset representation is surjective onto $S_3$ and its kernel is the Kline group $V$.

The group $V$ is is contained in $P$ and is normal. Thus, it is also contained in all the conjugates of $P$; namely, in all the 2-Sylow subgroups. We therefore have the following picture




Further, as $S_4/V \cong S_3$, the subgroups $P, P', P''$ are in bijection with the 2-Sylow subgroups of $S_3$ of which there are 3.

23.2.5. *Groups of order pq.* Let $p < q$ be primes. Let $G$ be a group of order $pq$. Then $n_q | p$, $n_q \equiv 1 \pmod{q}$. Since $p < q$ we have $n_q = 1$ and the $q$-Sylow subgroup is normal (in particular, $G$ is never simple). Also, $n_p | q$, $n_p \equiv 1 \pmod{p}$. Thus, either $n_p = 1$, or $n_p = q$ and the last possibility can happen only for $q \equiv 1 \pmod{p}$.

We conclude that if $p \nmid (q-1)$ then both the $p$-Sylow $P$ subgroup and the $q$-Sylow subgroup $Q$ are normal. Note that the order of $P \cap Q$ divides both $p$ and $q$ and so is equal to 1. Let $x \in P, y \in Q$ then $[x,y] = (xyx^{-1})y^{-1} = x(yx^{-1}y^{-1}) \in P \cap Q = \{1\}$. Thus, $PQ$, which is equal to $G$, is abelian. And it is not hard to prove it is cyclic.

We shall later see that whenever $p | (q-1)$ there is a non-abelian group of order $pq$ (in fact, unique up to isomorphism). The case of $S_3$ falls under this.

23.2.6. *Groups of order $p^2q$.* Let $G$ be a group of order $p^2q$, where $p$ and $q$ are distinct primes. We prove that $G$ is not simple:

If $q < p$ then $n_p \equiv 1 \pmod{p}$ and $n_p | q < p$, which implies that $n_p = 1$ and the $p$-Sylow subgroup is normal.

Suppose that $p < q$, then $n_q \equiv 1 \pmod{q}$ and $n_q | p^2$, which implies that $n_q = 1$ or $n_q = p^2$. If $n_q = 1$ then the $q$-Sylow subgroup is normal and we are done.

Assume that $n_q = p^2$. Each pair of the $q$-Sylow subgroups, and there are $p^2$ of them, intersects only at the identity (since $q$ is prime). Hence, together with the identity element, they account for $1 + p^2(q-1)$ elements of the group. Suppose that there were 2 $p$-Sylow subgroups. They intersect at most at a subgroup of order $p$ (and they intersect any of the $q$-Sylow subgroups at the identity alone). Thus, they contribute at least $2p^2 - p$ new elements. All together we got at least $1 + p^2(q-1) + 2p^2 - p = p^2q + p^2 - p + 1 > p^2q$ elements. That's a contradiction, and so if $n_q \neq 1$ we must have $n_p = 1$; the $p$-Sylow subgroup is normal.

*Remark* 23.2.2. A theorem of Burnside states that a group of order $p^a q^b$ with $a + b > 1$ is not simple. We leave it as an exercise that groups of order $pqr$ ($p < q < r$ primes) are not simple. Note that $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$ and $A_5$ is simple. A theorem of Feit and Thompson – among the hardest theorems in mathematics – says that a finite simple group is either of prime order, or of even order. We can also state it as saying that non-commutative finite simple group has even order.

23.2.7. $\mathrm{GL}_n(\mathbb{F})$. Let $\mathbb{F}$ be a finite field with $q$ elements. The order of $\mathrm{GL}_n(\mathbb{F})$ is $(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) = q^{(n-1)n/2}(q^n - 1)(q^{n-1} - 1) \cdots (q - 1)$. Thus, a $p$-Sylow has order $q^{(n-1)n/2}$. One such subgroup consists of the upper triangular matrices with 1 on the diagonal (the unipotent group):

$$\begin{pmatrix} 1 & * & \dots & * \\ 0 & 1 & \cdots & * \\ & & \ddots & \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

See the exercises for further treatment of this example.

Let us look at the particular case of $G = \mathrm{GL}_2(\mathbb{F}_3)$, a group with $(3^2-1)(3^2-3) = 48$ elements. As $48 = 2^4 3$, we are looking for 2-Sylow subgroups and for 3-Sylow subgroups, one of which we already know. The stabilizer of the unipotent subgroup under conjugation can be checked to be the upper triangular matrices. And so, the number of 3-Sylow subgroups is $48/12 = 4$. How does a 2-Sylow subgroup $Q$ of $G$ looks like?

To give a subgroup $Q$ of index 3 is to give a transitive action of $G$ on 3 elements, $Q$ being the stabilizer of one of the elements in this action. Can we find a set of 3 elements on which $G$ acts? I don't have a good idea for doing this, but we can find $Q$ in a different way.

Consider the dihedral group of 8 elements. As this is the group of symmetries of a square in the plane, we can realize it as matrices in $\mathrm{GL}_2(\mathbb{R})$; as such, it is generated by the matrices $y = \left(\begin{smallmatrix} -1 & \\ & 1 \end{smallmatrix}\right)$ and $x = \left(\begin{smallmatrix} & 1 \\ -1 & \end{smallmatrix}\right)$. We can view these matrices as having entries in $\mathbb{F}_3$ and that way $D_4$ is realized as a subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ consisting of the matrices $\left\{\left(\begin{smallmatrix} \pm 1 & \\ & \pm 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} & \pm 1 \\ \pm 1 & \end{smallmatrix}\right)\right\}$. Now consider the matrix $t = \left(\begin{smallmatrix} -1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. It is invertible and $t^2 = \left(\begin{smallmatrix} -1 & \\ & -1 \end{smallmatrix}\right)$. So $t$ has order 4, $t^2 \in D_4$. It is therefore a good guess that $Q = \langle t, D_4 \rangle$. To check $\langle t, D_4 \rangle$ is a subgroup we need to check that $t$ normalizes $D_4$. We find that $tyt^{-1} = xy$ and $txt^{-1} = (txyt^{-1})(tyt^{-1}) = (t^2yt^{-2})(xy) = yxy = x^{-1}$ and that's enough to show that $t$ normalizes $D_4$. Now $|\langle t, D_4 \rangle| = |\langle t \rangle| \cdot |D_4| / |\langle t \rangle \cap D_4| = 4 \cdot 8/2 = 16$ and so we may take $Q$ to be $\langle t, D_4 \rangle$.

The number of 2-Sylow subgroups is either 1 or 3. In fact, there are 3, but that requires some additional work (calculate the conjugate of $Q$ by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$).

23.2.8. *More examples.*

**Example 23.2.3.** We look now at groups of order 12. We would need to use a surprising amount of theory to gain insight into their structure and, in fact, we will only be able to complete our discussion later in §28.5, making use of the theory of semi-direct products.

One can wonder why is the determination of groups of order 12 so complicated. Perhaps the following will help: a group of order is determined by its multiplication table and for a group of order 12 this table has 144 cells. A priori in each cell there could be any element of the group and so we have $12^{144}$ possibilities. We can of course improve on that, but not by much: for example, the column and row of multiplying by the identity are determined, so we really have 121 cells. Further, each row, or column contains every element of $G$ and exactly once. That is, the multiplication table is a Latin Square, with one predetermined row and one predetermined column – a so-called reduced Latin square. According to Wikipedia (June 2020) the number of reduced Latin squares of size 12 is about $1.62 \times 10^{44}$. On the other hand, there are precisely 5 groups of order 12 up to isomorphism, and the size of their automorphism groups is rather small too, so we may conclude that the number of Latin squares arising as multiplication tables is tiny in comparison to $1.6210^{44}$ (in the hundreds, perhaps). This suggest that there is a lot of structure for groups of order 12 which dramatically cuts down the number of possibilities for multiplication tables.

Suppose then that $G$ is a group of order 12. If $G$ is abelian, it is a consequence of Theorem 26.2.1 that either $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, which is also isomorphic to $\mathbb{Z}/12\mathbb{Z}$, or $G \cong (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z}$, which is also isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ (use CRT to show the isomorphisms). The $p$-Sylow subgroups are unique because $G$ is abelian. In the first case they are $\mathbb{Z}/4\mathbb{Z} \times \{0\}$ and $\{0\} \times \mathbb{Z}/3\mathbb{Z}$ and in the second case they are $(\mathbb{Z}/2\mathbb{Z})^2 \times \{0\}$ and $\{0\} \times \mathbb{Z}/3\mathbb{Z}$.

Assume now that $G$ is not abelian. Let $P$ be some 2-Sylow of $G$ and $Q$ some 3-Sylow of $G$. We claim that we cannot have that both $P$ and $Q$ are normal. If they are, let $x \in P, y \in Q$ then $xyx^{-1}y^{-1} \in P \cap Q$ (read it first as $(xyx^{-1})y^{-1}$ to see it is in $Q$, and then as $x(yx^{-1}y^{-1})$ to see it is in $P$). But $P \cap Q = \{1\}$. Thus, elements of $P$ commute with elements of $Q$. However, both $P$ and $Q$ are commutative so we deduce that the subgroup $PQ$ is commutative. But this subgroup has 12 elements, so $G$ itself is commutative and that is a contradiction. Thus, either $P$ or $Q$ are not normal.

On the other hand, if $Q$ is not normal, then $n_3 > 1$. As $n_3 | 4, n_3 \equiv 1 \pmod 3$, it follows that $n_3 = 4$. So there are 4 3-Sylow subgroups, say $Q = Q_1, \dots, Q_4$. Note that any pair of which intersects at $\{1\}$ only. Thus, $\cup Q_i$ contains 9 elements. On the other hand, as $P$ doesn't have an element of order 3, $P \cap \cup Q_i = \{1\}$. As $G - \cup Q_i$ has 3 elements and $P$ has 4 elements, we must have

$$P = \{1\} \cup (G - \cup Q_i).$$

Thus, $P$ is uniquely determined and so is normal.

The situation therefore is as follows: either $P$ is normal, or $Q$ is normal, but not both.

Suppose that $P$ is normal. There is another piece of information here that is completely general so we state it as a lemma. We denote by $\mathrm{Aut}(G)$ the **automorphism group** of a group $G$. This is the group whose elements are bijective homomorphisms $f\colon G \to G$, where the group law is composition. Cf. Exercise 29.

**Lemma 23.2.4.** *Let $G$ be a group and $P$ a normal subgroup of $G$. There is a homomorphism:*

$$\tau\colon G \to \mathrm{Aut}(P), \quad g \mapsto \tau_g,$$

*where*

$$\tau_g(x) = gxg^{-1}.$$

*If $P$ is abelian, $\tau$ induces a homomorphism*

$$\tau\colon G/P \to \mathrm{Aut}(P).$$

*Proof.* We will be brief here, as part of it is Exercise 29. In general, we have a homomorphism

$$\tau\colon G \to \mathrm{Aut}(G),$$

provided by the same formula. If $P$ is normal, $\tau_g(P) = P$ and so the $\tau$ of the lemma is really $\tau_g|_P$ (the restriction of $\tau_g$ to $P$). If $P$ is abelian and $g \in P$ then conjugating by $g$ elements of $P$ is trivial: $gxg^{-1} = x, \forall g, x \in P$. That is $\tau_g|_P$ is the identity. Hence, by the First Isomorphism Theorem, we may factor $\tau$ through $G/P$ and get a homomorphism $\tau\colon G/P \to \mathrm{Aut}(P)$. □

To apply it to our study of groups of order 12 we need another fact, left as an exercise.

*Exercise* 23.2.5. Let $d, n$ be positive integers.

$$\mathrm{Aut}((\mathbb{Z}/n\mathbb{Z})^d) \cong \mathrm{GL}_d(\mathbb{Z}/n\mathbb{Z}).$$

Let return now to the situation where $G$ is a non-abelian group of order 12 and assume that $P$, the 2-Sylow subgroup, is normal. If $P = \mathbb{Z}/4\mathbb{Z}$ then $\mathrm{Aut}(P) = \mathrm{GL}_1(\mathbb{Z}/4\mathbb{Z}) = (\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\}$ is a group of 2 elements. (Recall that $\mathrm{GL}_d(R)$ are matrices whose determinant is a unit of $R$. In particular, for $d = 1$, $\mathrm{GL}_1(R) = R^\times$.)

However, by the lemma, we have a homomorphism

$$G/P \to (\mathbb{Z}/4\mathbb{Z})^\times.$$

As $G/P$ is a group of order 3, this homomorphism is trivial. That means that $P$ is contained in the centre of $G$ and in particular $Q$ and $P$ commute. We saw this is not possible. Thus, if $P$ is normal, we must have $P \cong (\mathbb{Z}/2\mathbb{Z})^2$.

So, to summarize, for non-abelian groups of order 12, we have one of the following situations:

(1) $P$ is normal and $Q$ is not, and $P \cong (\mathbb{Z}/2\mathbb{Z})^2$. (The group $A_4$ has this property where $P = V$ is the Klein group and $Q = \langle (123) \rangle$.)
(2) $Q$ is normal and $P$ is not, and $P \cong (\mathbb{Z}/2\mathbb{Z})^2$. (The group $D_6$ has this property where $P = \langle y, x^3 \rangle$ and $Q = \langle x^2 \rangle$.)
(3) $Q$ is normal and $P$ is not, and $P \cong \mathbb{Z}/4\mathbb{Z}$. (There is a group with this property. We denote $T$; we will later construct it using the theory of semi-direct product.)

**Example 23.2.6.** Let $G$ be a group of order $231 = 3 \cdot 7 \cdot 11$. As $n_{11} | 21$ and $n_{11} \equiv 1 \pmod{11}$ we must have that $n_{11} = 1$. Let $R$ be the unique 11-Sylow subgroup. $R$ is normal. As $R$ has a prime order $R \cong \mathbb{Z}/11\mathbb{Z}$, is abelian, and $\mathrm{Aut}(R) \cong (\mathbb{Z}/11\mathbb{Z})^\times$ is a group of 10 elements. The homomorphism

$$G/R \to \mathrm{Aut}(R),$$

must therefore be trivial (the l.h.s. is a group of order 21). Thus, $G$ has a non-trivial centre; in fact, $R \subseteq Z(G)$. We leave it as an exercise to show that if $G$ is non-abelian then $R = Z(G)$.

## 23.3. **Being a product of Sylow subgroups.**

**Proposition 23.3.1.** *Let $G$ be a finite group of order $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where the $p_i$ are distinct primes and the $a_i > 0$. Choose for every prime $p_i$ a Sylow subgroup $P_i$. Then*

$$G \cong P_1 \times P_2 \times \cdots \times P_r \iff P_i \lhd G, \forall i.$$

Before the proof we need to collect a few more facts. The proofs are easy; in fact, in one way or another we have seen them in the previous examples, and we leave them as exercises.

**Lemma 23.3.2.** *Let $G$ be a finite group, $p \neq q$ primes dividing the order of $G$ and $P, Q$ corresponding Sylow subgroups then $P \cap Q = \{1\}$.*

**Lemma 23.3.3.** *Let $G$ be a group with normal subgroups $A, B$. If $A \cap B = \{1\}$ then the elements of $A$ commute with those of $B$, namely, for all $a \in A, b \in B$,*

$$ab = ba.$$

We now prove the Proposition 23.3.1. Suppose that each $P_i$ is normal. Define a function

$$f : P_1 \times \cdots P_r \to G, \quad f(x_1, \dots, x_r) = x_1 x_2 \cdots x_r.$$

Using the lemmas above, we see that $P_i$ and $P_j$ commutes for all $i \neq j$. A direct verification now gives that $f$ is a homomorphism. The homomorphism $f$ is surjective because the image contains $f(\{1\} \times \cdots \times P_i \times \cdots \{1\}) = P_i$ and $\langle P_1, \dots, P_r \rangle$ is a group whose order is divisible by $p_i^{a_i}$ for all $i$, hence equal to $G$. As the source has the same number of elements, $f$ is bijective.

Conversely, if $G \cong P_1 \times P_2 \times \cdots \times P_r$, then, in the left hand side, each group $\{1\} \times \cdots \times P_i \times \cdots \times \{1\}$ is a normal $p_i$-Sylow subgroup. Thus, also, in the right hand side, each $p_i$-Sylow is normal.

**Definition 23.3.4.** A finite group is called **nilpotent** if it is a product of its $p$-Sylow subgroups.

We remark that usually one defines nilpotent completely differently, but it is a theorem that the other definition is equivalent to the one given here.

# Part 6. Composition series, the Jordan-Hölder theorem and solvable groups

## 24. Composition series

24.1. **Two philosophies.** In the study of finite groups one can sketch two broad philosophies:

The first one, that we may call the *"Sylow philosophy"* (though such was not made by Sylow, I believe), is given a finite group to study its $p$-subgroups and then study how they fit together. Sylow's theorems guarantee that the size of $p$-subgroup is as big as one can hope for, guaranteeing the first step can be taken. The theory of $p$-groups, the second step, is a beautiful and powerful theory, which is quite successful. I know little about a theory that tells us how $p$-groups fit together.[12]

The second philosophy, that one may call the *"Jordan-Hölder philosophy"*, suggests given a group $G$ to find a non-trivial normal subgroup $N$ in $G$ and study the possibilities for $G$ given $N$ and $G/N$. The first step then is to hope for the classification of all finite simple groups. Quite astonishingly, this is possible and was completed towards the end of the last ($20^{th}$) century.

The second step is figuring out how to create groups $G$ from two given subgroups $N$ and $H$ such that $N$ will be a normal subgroup of $G$ and $G/N$ will be isomorphic to $H$. There is a lot known here. We will shortly study one machinery for that: the semi-direct product $N \rtimes H$.

## 25. The Jordan-Hölder theorem and solvable groups

25.1. **Composition series and composition factors.** Let $G$ be a group. A **normal series** for $G$ is a series of subgroups

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}.$$

Unless stated otherwise, we will assume that normal series are **strictly descending**. A **composition series** for $G$ is a series of subgroups

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\},$$

such that $G_{i-1}/G_i$ is a nontrivial simple group for all $i = 1, \dots, n$. The **composition factors** are the quotients $\{G_{i-1}/G_i : i = 1, 2, \dots, n\}$. The quotients are considered up to isomorphism, where the order of the quotients doesn't matter, but we do take the quotients with multiplicity. For example, the group $D_4$ has a composition series

$$D_4 \rhd \langle x \rangle \rhd \langle x^2 \rangle \rhd \{1\}.$$

The composition factors are $\{\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}\}$. More generally, from our results on $p$-groups, we know that any finite $p$-group has a composition series with quotients $\mathbb{Z}/p\mathbb{Z}$.

A group $G$ is called **solvable** if it has a normal series in which all the composition factors are abelian groups.

**Lemma 25.1.1.** *Let $G$ be a finite group. Any strictly descending normal series*

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\},$$

*for $G$ can be refined to a composition series. Moreover, if the quotients $G_{i-1}/G_i$ are abelian, then the quotients for the composition series are groups isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime $p$.*

*Proof.* Note that since the series is strictly descending the quotients $G_{i-1}/G_i$ are non-trivial and their order divides the order of the group. In fact, $|G| = \prod_{i=1}^{n} |G_{i-1}/G_i|$. Thus any strictly descending normal series has bounded length. As a result, it is enough to show that a strictly

[12] The class of nilpotent groups turns out to be the same as the class of groups that are a direct product of their $p$-Sylow subgroups.

descending normal series that is not a composition series can be refined to a series of longer length.

Let

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$$

be a strictly descending normal series that is not a composition series. Choose $i$ such that $G_{i-1}/G_i$ is not simple. Let $H'$ be a non-trivial normal subgroup of $G_{i-1}/G_i$ and let $H$ be the subgroup of $G_{i-1}$ that corresponds to it. We then have

$$G = G_0 \rhd G_1 \rhd \cdots G_{i-1} \rhd H \rhd G_i \rhd \cdots \rhd G_n = \{1\}.$$

Note that, indeed, by the correspondence theorem, since in $G_{i-1}/G_i$ we have $(G_{i-1}/G_i) \rhd H' \rhd \{1\}$, indeed $G_{i-1} \rhd H \rhd G_i$ and

$$G_{i-1}/H \cong (G_{i-1}/G_i)/H', \qquad H/G_i \cong H'.$$

Thus, we have a *longer* strictly descending normal series. If the original quotients were abelian then the new series also has abelian quotients, because $(G_{i-1}/G_i)/H'$ is a quotient of the abelian group $G_{i-1}/G_i$ (hence abelian) and $H'$ is a subgroup of an abelian group (hence abelian).

Thus, as explained, by repeating this refinement process finitely many times, we obtain a composition series. If the original series had abelian quotients, so does the composition series. The only thing remaining to show that is that a simple finite abelian group must have prime order.

Let $A$ be a simple finite abelian group. Choose $x \in A$ such that $x \neq 1$. Since $\langle x \rangle$ is a non-trivial subgroup of $A$, automatically normal, we have $\langle x \rangle = A$. Let $p$ be a prime dividing the order of $x$. Then also $\langle x^p \rangle$ is a normal subgroup and is a proper subgroup of $\langle x \rangle$. Thus, we must have $\langle x^p \rangle = \{1\}$. It follows that $A$ has order $p$. □

**Corollary 25.1.2.** *Let G be a finite group. G is solvable if and only if it has a composition series whose composition factors are cyclic groups of prime order.*

25.2. **Jordan-Hölder Theorem.** The Jordan-Holder theorem clarifies greatly the yoga behind the concept of composition series.

**Theorem 25.2.1.** *Let G be a finite group. Any two composition series for G have the same composition factors (considered with multiplicity).*

Note that a consequence of the theorem is that any two composition series have the same length, since the length determines the number of composition factors.

The proof of the theorem is quite technical, unfortunately. It rests on the following lemma.[13]

**Lemma 25.2.2.** *(Zassenhaus) Let $A \lhd A^*$, $B \lhd B^*$ be subgroups of a group G. Then*

$$A(A^* \cap B) \lhd A(A^* \cap B^*), \qquad B(B^* \cap A) \lhd B(B^* \cap A^*),$$

*and*

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \frac{B(B^* \cap A^*)}{B(B^* \cap A)}.$$

Before the proof, recall the following facts: (i) Let $S \lhd G$, $T < G$ be subgroups of a group $G$. Then $ST$ is a subgroup of $G$ (and $ST = TS$). (ii) If also $T \lhd G$ then $ST \lhd G$.

*Proof.* Let $D$ be the following set:

$$D = (A^* \cap B)(A \cap B^*).$$

We show that $D$ is a normal subgroup of $A^* \cap B^*$, $D = (A \cap B^*)(A^* \cap B)$ and

$$\frac{B(B^* \cap A^*)}{B(B^* \cap A)} \cong \frac{A^* \cap B^*}{D}.$$

[13]Our proof follows Rotman's in *An introduction to the theory of groups*.

The lemma then follows from the symmetric role played by $A$ and $B$.

It is easy to check directly from the definitions that $(A^* \cap B) \lhd A^* \cap B^*$ and, similarly, $(A \cap B^*) \lhd A^* \cap B^*$. It follows that $D \lhd A^* \cap B^*$ and that $D = (A \cap B^*)(A^* \cap B)$. The subtle point of the proof is to construct a homomorphism

$$f\colon B(B^* \cap A^*) \to \frac{A^* \cap B^*}{D}.$$

Let $x \in B(B^* \cap A^*)$, say $x = bc$ for $b \in B, c \in (B^* \cap A^*)$. Let

$$f(x) = cD$$

(which is an element of $\frac{A^* \cap B^*}{D}$.)

First, $f$ is well defined. If $x = b_1 c_1$ then $c_1 c^{-1} = b_1^{-1} b \in (B^* \cap A^*) \cap B \subset D$. As $D \lhd (B^* \cap A^*)$ and $c_1 \in (B^* \cap A^*)$ also $c^{-1} c_1 \in D$, and so $cD = c_1 D$. Next, $f$ is a homomorphism. Suppose that $x = bc, y = b_1 c_1$ and so $xy = bcb_1 c_1$. Note that $cb_1 c^{-1} \in B$ (as $B$ is normal in $B^*$ and $c \in B^*$) and so $xy = bb' cc_1$ for some $b' \in B$. It now follows that $f(xy) = f(x) f(y)$.

It is clear from the definition that $f$ is a surjective homomorphism. When is $x = bc \in \mathrm{Ker}(f)$? This happens if and only if $c \in D$, that is $x \in B(A^* \cap B)(A \cap B^*) = B(A \cap B^*)$. This shows that $B(A \cap B^*) \lhd B(A^* \cap B^*)$ and the desired isomorphism. □

**Theorem 25.2.3.** *Let $G$ be a group. Any two finite composition series for $G$ are equivalent; namely, have the same composition factors.*

*Proof.* More generally, we prove that any two normal series for $G$ have refinements that are equivalent; namely, have the same composition factors (with the same multiplicities). This holds also for infinite groups that may not have composition series, and so is useful in other situations. In the case of composition series, since they cannot be refined in a non-trivial way because the quotients are simple groups, we get that any two composition series for $G$ (if they exist at all) are equivalent.

Thus, consider two normal series of $G$,

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\},$$

and

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_m = \{1\}.$$

First, use the second series to refine the first. Define:

$$G_{ij} = G_{i+1}(G_i \cap H_j).$$

For fixed $i$, this is a descending series of sets, beginning at $G_{i0} = G_{i+1} G_i = G_i$ and ending at $G_{im} = G_{i+1}$. Taking in the Zassenhaus lemma $A = G_{i+1}, A^* = G_i, B = H_{j+1}, B^* = H_j$ gives us that $G_{i,j+1} = A(A^* \cap B) \lhd G_{ij} = A(A^* \cap B^*)$ (and, in particular, that these are all subgroups).

Similarly, use the first series to refine the second by defining

$$H_{ij} = H_{j+1}(H_j \cap G_i).$$

As above, the series $H_j = H_{0j} \supset H_{1j} \supset \cdots \supset H_{nj} = H_{j+1}$ is a series of subgroups, each normal in the former. Finally, applying the Zassenhaus lemma again, we find that

$$\frac{G_{ij}}{G_{i,j+1}} = \frac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \frac{B(B^* \cap A^*)}{B(B^* \cap A)} = \frac{H_{ij}}{H_{i+1,j}}.$$

This gives a precise matching of the factors. □

Note that every finite group $G$ has a composition series. While the composition series itself is not unique, the composition factors are. So, in a sense, the Jordan-Hölder theorem is a unique factorization theorem for groups. From this point of view, the simplest groups are the so-called solvable groups; these are the groups with the simplest factors - cyclic groups of prime order. We therefore now focus our attention on solvable groups for a while.

25.3. **Solvable groups.** Recall that a group $G$ is called solvable if there is a finite normal series for $G$,

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\},$$

with abelian quotients.

**Example 25.3.1.** Every abelian group is solvable.

**Example 25.3.2.** It follows from our results on $p$-groups that every $p$-group is solvable.

**Example 25.3.3.** Any group of order $pq$, where $p < q$ are primes, is solvable as the $q$-Sylow is always normal and the quotient is a group of order $p$, hence cyclic.

**Example 25.3.4.** Groups of order $p^2q$ are solvable. Indeed, as we have seen, either the $p$-Sylow or the $q$-Sylow is normal. Whatever is the case, not that automatically groups of order $p^2$ and of order $q$ are abelian.

We leave it as an exercise that a group of order $pqr$, where $p, q, r$ are distinct primes, is solvable.

**Example 25.3.5.** A product of solvable groups is solvable.

Of course, not every group is solvable. Any non-abelian simple group (such as $A_n$ for $n \geq 5$, and $\mathrm{PSL}_n(\mathbb{F}_q)$ for $n \geq 2$ and $(n, q) \neq (2, 2)$ or $(2, 3)$) is non-solvable.

The class of solvable groups is closed under basic operations. More precisely we have the following results.

**Proposition 25.3.6.** *Let $G$ be a solvable group and $K < G$ a subgroup. Then $K$ is solvable.*

*Proof.* Let

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\},$$

be a normal series with abelian quotients. Consider the normal series

$$K = K \cap G_0 \rhd K \cap G_1 \rhd \cdots \rhd K \cap G_n = \{1\}.$$

It need not be strictly descending but that is not a problem. It is enough to show that $K \cap G_{i-1}/K \cap G_i$ is abelian. Consider the homomorphism which is the composition

$$K \cap G_{i-1} \to G_{i-1} \to G_{i-1}/G_i.$$

The image is an abelian group and the kernel is $K \cap G_i$. Thus, by the First Isomorphism Theorem, $K \cap G_{i-1}/K \cap G_i$ is isomorphic to a subgroup of the abelian group $G_{i-1}/G_i$, hence abelian. $\square$

Before continuing, it will convenient to introduce some terminology. A sequence of groups and homomorphisms

$$\cdots \longrightarrow G_a \xrightarrow{f_a} G_{a+1} \xrightarrow{f_{a+1}} G_{a+2} \xrightarrow{f_{a+2}} \cdots$$

is called **exact**, if for every $a$, $\mathrm{Im}(f_a) = \mathrm{Ker}(f_{a+1})$. If the sequence terminates at $G_a$ there is no condition on $\mathrm{Im}(f_a)$, and if it begins with $G_a$ there is no condition on $\mathrm{Ker}(f_a)$. A **short exact sequence** (or **ses**, for short) is an exact sequence of the sort

$$1 \longrightarrow G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3 \longrightarrow 1\ ,$$

where 1 stands for the group of 1 element. Note that the maps $1 \to G_1$ and $G_3 \to 1$ are uniquely determined, hence we do not specify them. Thus, this sequence is short exact if $f$ is injective, $g$ is surjective and $\mathrm{Im}(f) = \mathrm{Ker}(g)$.

**Proposition 25.3.7.** *Let*

$$1 \to K \xrightarrow{f} G \xrightarrow{g} H \to 1$$

*be a short exact sequence of groups. Then $G$ is solvable if and only if both $K$ and $H$ are solvable.*

*Proof.* Assume that $G$ is solvable. We already proved that $f(K) < G$ is solvable. As $f : K \to f(K)$ is an isomorphism, $K$ is solvable too. Let

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\},$$

be a normal series with abelian quotients. Let

$$H_i = g(G_i).$$

The series of subgroups $H = H_0 > H_1 > \cdots > H_n = \{1\}$ is a series of normal subgroups. Indeed, for every $i$, $g : G_{i-1} \to H_{i-1}$ is a surjective homomorphism and so, as $G_i$ is normal in $G_{i-1}$, $H_i$ is normal in $H_{i-1}$. We therefore have a normal series

$$H = H_0 \rhd H_1 \rhd \cdots \rhd H_n = \{1\}.$$

We prove that its quotients are abelian. Consider the surjective homomorphism obtained as the composition

$$G_{i-1} \to H_{i-1} \to H_{i-1}/H_i.$$

The kernel contains $G_i$. Thus, by the first isomorphism theorem we get a surjective homomorphism

$$G_{i-1}/G_i \to H_{i-1}/H_i.$$

Therefore, $H_{i-1}/H_i$ is a quotient of an abelian group and so is abelian too.

Now suppose that $K$ and $H$ are solvable. Thus, we have normal series

$$H = H_0 \rhd H_1 \rhd \cdots \rhd H_n = \{1\},$$

and

$$K = K_0 \rhd K_1 \rhd \cdots \rhd K_m = \{1\},$$

with abelian quotients. Let

$$J_i = \begin{cases} g^{-1}(H_i), & 0 \le i \le n \\ f(K_{i-n}), & n \le i \le m+n. \end{cases}.$$

(Note that $f(K_0) = f(K) = \mathrm{Ker}(g) = g^{-1}(H_n)$ and so $J_n$ is well defined.) Then $J_i$ is a normal series with abelian quotients:

$$J_{i-1}/J_i \cong \begin{cases} H_{i-1}/H_i, & 0 \le i \le n \\ K_{i-n-1}/K_{i-n}, & n < i \le m+n. \end{cases}.$$

□

**Example 25.3.8.** *Every group $G$ of order $p^a q^b$, where $p, q$ is are distinct primes and $p^a! < p^a q^b$ has a non-trivial normal subgroup.* Indeed, let $Q$ be the $q$-Sylow subgroup and let $G$ act on its cosets by the coset representation. Since the index of $Q$ is $p^a$ we get a homomorphism:

$$f : G \to S_{p^a}.$$

As $|G| > p^a!$ the kernel of $f$ is not trivial. On the other hand $\mathrm{Ker}(f) < Q$. Thus, $\mathrm{Ker}(f)$ is a non-trivial normal subgroup of $G$.

**Theorem 25.3.9.** *Every group of order less than* 60 *is solvable.*

*Proof.* First note that the following integers are prime:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59.$$

The following are prime powers:

$$4, 8, 9, 16, 25, 27, 32, 49.$$

The following are a product of two distinct primes:

$$6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 46, 51, 55, 57, 58.$$

The following are of the form $p^2q$, where $p$ and $q$ are distinct primes:

$$12, 18, 20, 28, 44, 45, 50, 52.$$

And, the following are for the form $pqr$ for distinct primes $p, q, r$:

$$30, 42.$$

We already know that groups of the order listed are solvable. The orders left to consider are

$$24, 36, 40, 48, 54, 56$$

Of those, $24 = 3 \cdot 2^3, 36 = 2^2 \cdot 3^2, 48 = 3 \cdot 2^4$ and $54 = 2 \cdot 3^3$ are of the form $p^a q^b$, where $p, q$ is are distinct primes and $p^a! < p^a q^b$, so they have a non-trivial normal subgroup $K$. By induction on the order of the group, both $K$ and $G/K$ are solvable. Hence, by Proposition 25.3.7, $G$ is solvable. It remains to consider groups of order $40 = 2^3 \cdot 5$ and $56 = 2^3 \cdot 7$.

Let $G$ be a group of order 40. Let $P$ be the 5-Sylow subgroup. As $n_5|8$ and $n_5 \equiv 1 \pmod 5$ we must have $n_5 = 1$ and so $P$ is normal. By induction, the groups $P$ and $G/P$ are solvable and therefore so is $G$.

Let $G$ be a group of order 56. Suppose that the 7-Sylow of $G$ is not normal. Then there are eight 7-Sylow subgroups. These already account for a set $S$ consisting of $1 + (7 - 1) \times 8 = 49$ distinct elements of $G$. If $P$ is a 2-Sylow subgroup then $P \cap S = \{e\}$ and it follows that $P = G \setminus S \cup \{e\}$. Since this holds for any 2-Sylow subgroup, we conclude that $P$ is the unique 2-Sylow subgroup and hence is normal. As above, using induction we find that $G$ is solvable. □

The motivation for the study of solvable groups comes from Galois theory. Let $f(x) = x^n + a_{n_1}x^{n-1} + \cdots + a_0$ be an irreducible polynomial with rational coefficients. In Galois theory one associates to $f$ a finite group $G_f \subseteq S_n$, called the Galois group of $f$. It is a transitive subgroup of $S_n$ whose exact structure depends on the polynomial. It may be $S_n$ and it may be $\langle(1\ 2\ \cdots\ n)\rangle$, or many other subgroups of $S_n$. One of Évariste Galois's main achievements was to prove that one can solve $f$ in radicals – meaning, express the solutions of $f$ using operations such as taking roots (of any order), adding and multiplying – if and only if $G_f$ is a solvable group. This explains the origin of the terminology "solvable".

It follows that there are formulas in radicals to solve equations of degree $\leq 4$; every group that can possibly arise as $G_f$ has order less than 60, hence is solvable. On the other hand, one can produce easily an equation $f$ of degree 5 such that $G_f = S_5$, which is not a solvable group. Indeed, if $S_5$ is solvable, so is $A_5$. But $A_5$ is a non-abelian simple group hence not solvable.

*Remark* 25.3.10. Here are two theorems concerning solvable groups. The first is hard, but can be done in a graduate course in algebra. The second is among the most difficult proofs in algebra ever written. (Please do not use these theorems in the assignments.)

*Theorem* 25.3.11 (Burnside). *Let $p, q$ be primes. A finite group of order $p^a q^b$ is solvable.*

*Theorem* 25.3.12 (Feit-Thompson). *Every finite group of odd order is solvable.*

# Part 7. Finitely Generated Abelian Groups, Semi-direct Products and Groups of Low Order

## 26. The structure theorem for finitely generated abelian groups

26.1. **Generators.** A group $G$ is called **finitely generated** if there are elements $g_1, g_2, \dots, g_n$ in $G$ such that $G = \langle g_1, \dots, g_n \rangle$. We saw two interpretations of this: (i) $G$ is the minimal subgroup of $G$ that contains all the elements $g_1, \dots, g_n$ (namely, no proper subgroup of $G$ will contain all these elements). (ii) Every element of $G$ can be written in the form $x_1 x_2 \cdots x_N$, where each $x_i$ is either $g_j$ or $g_j^{-1}$ for some $j$.

It is sometimes easier to use the first, seemingly more abstract, definition. For example, consider the elements $\{(1234), (13), (123), (12345)\}$ of $S_5$. $S_5$ is generated by them. Indeed, the first two elements generate a copy of $D_4$ and so it follows that every subgroup containing these elements will have order divisible by $8, 3$ and $5$ and so will have order divisible by 120, thus equal to $S_5$. On the other hand, it is a rather unpleasant exercise to explicitly write every one of the 120 permutations in $S_5$ as a product of these generators.

Let $G$ be an abelian group and use additive notation. Then $G$ is finitely generated if and only if there exist elements $g_1, g_2, \dots, g_n$ of $G$ such that

$$G = \left\{ \sum_{i=1}^{n} a_i g_i : a_i \in \mathbb{Z} \right\}.$$

**Lemma 26.1.1.** *An abelian group $G$ is finitely generated if and only if for some positive integer $n$ there is a surjective homomorphism*

$$\mathbb{Z}^n \to G.$$

*Proof.* Suppose that $G$ is finitely generated by elements $\{g_1, g_2, \dots, g_n\}$. Define a homomorphism

$$\mathbb{Z}^n \to G, \qquad (a_1, \dots, a_n) \mapsto \sum_{i=1}^{n} a_i g_i.$$

This is a surjective homomorphism.

Conversely, given a surjective homomorphism $f\colon \mathbb{Z}^n \to G$, let

$$g_i = f(e_i) = f(0, \dots, 1, \dots, 0) \quad (1 \text{ in the } i\text{-th place}).$$

Every element of $G$ is of the form $f(a_1, \dots, a_n)$ for some $a_i \in \mathbb{Z}$. But, $f(a_1, \dots, a_n) = \sum_{i=1}^{n} a_i f(e_i) = \sum_{i=1}^{n} a_i g_i$ and so $G$ is generated by $\{g_1, g_2, \dots, g_n\}$. ☐

26.2. **The structure theorem.** The **structure theorem for finitely generated abelian groups** will be proven in the next semester as a corollary of the structure theorem for modules over a principal ideal domain. That same theorem will also yield the Jordan canonical form of a matrix, which we have already studied in the course in Linear Algebra. It is really the "correct way" to prove both these theorems, hence we defer the proof to that time.

**Theorem 26.2.1.** *Let $G$ be a finitely generated abelian group. Then there exists a unique data consisting of a non-negative integer $r$, and integers $1 < n_1 | n_2 | \dots | n_t$ $(t \geq 0)$ such that*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z}.$$

*Remark* 26.2.2. The integer $r$ is called the **rank** of $G$. The subgroup in $G$ that corresponds to $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z}$ under such an isomorphism is canonical (independent of the isomorphism). It is the subgroup of $G$ consisting of all elements of finite order; it is called the **torsion subgroup** of $G$ and sometime denoted $G_{\text{tor}}$. On the other hand, the subgroup corresponding to $\mathbb{Z}^r$ is not canonical and depends very much on the isomorphism.

A group is called **free abelian group** if it is isomorphic to $\mathbb{Z}^r$ for some $r$ (the case $t = 0$ in the theorem above). In this case, elements $x_1, \dots, x_r$ of $G$ that correspond to a basis of $\mathbb{Z}^r$ are called a basis of $G$; every element of $G$ has the form $a_1x_1 + \dots + a_rx_r$ for unique integers $a_1, \dots, a_r$.

The Chinese Remainder Theorem gives that if $n = p_1^{a_1} \cdots p_s^{a_s}$, $p_i$ distinct primes, then

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_s^{a_s}\mathbb{Z}.$$

Thus, one could also write an isomorphism $G \cong \mathbb{Z}^r \times \prod_i \mathbb{Z}/p_i^{b_i}\mathbb{Z}$ for suitable primes and exponents. More precisely, we have the following variant of the structure theorem:

**Theorem 26.2.3.** *Let $G$ be a finitely generated abelian group. There exists a unique data consisting of a non-negative integer $r$, unique primes $p_1, \dots, p_s$ ($s \geq 0$), and for each prime $p_a$ unique integers $0 < b_{a,1} \leq \dots \leq b_{a,n_a}$, such that*

$$G \cong \mathbb{Z}^r \times \prod_{a=1}^{s} \mathbb{Z}/p_a^{b_{a,1}} \times \dots \times \mathbb{Z}/p_a^{b_{a,n_a}}.$$

We shall also prove the following corollary in greater generality next semester.

**Corollary 26.2.4.** *Let $G, H$ be two free abelian groups of rank $r$. Let $f\colon G \to H$ be a homomorphism such that $G/f(H)$ is a finite group. There are bases, $x_1, \dots, x_r$ of $G$ and $y_1, \dots, y_r$ of $H$, and integers $1 \leq n_1 | \dots | n_r$ such that $f(y_i) = n_i x_i$.*

**Example 26.2.5.** Let $G$ be a finite abelian $p$-group, $|G| = p^n$. Then $G \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_s^{a_s}\mathbb{Z}$ for unique $a_i$ satisfying $1 \leq a_1 \leq \dots \leq a_s$ and $a_1 + \dots + a_s = n$. It follows that the number of isomorphism classes of finite abelian groups of order $p^n$ is $p(n)$ (the partition function of $n$).

## 27. Semi-direct products

Semi-direct products are a powerful method to create new groups, or to describe very precisely the structure of certain groups. They appear often in applications.

Given two groups $B, N$ we have formed their *direct product* $G = N \times B$. Identifying $B, N$ with their images $\{1\} \times B, N \times \{1\}$ in $G$, we find that: (i) $G = NB$, (ii) $N \lhd G, B \lhd G$, (iii) $N \cap B = \{1\}$. Conversely, one can easily prove that if $G$ is a group with subgroups $B, N$ such that: (i) $G = NB$, (ii) $N \lhd G, B \lhd G$, (iii) $N \cap B = \{1\}$, then $G \cong N \times B$. The definition of a semi-direct product relaxes the conditions a little.

**Definition 27.0.1.** Let $G$ be a group and let $B, N$ be subgroups of $G$ such that: (i) $G = NB$; (ii) $N \cap B = \{1\}$; (iii) $N \lhd G$. Then we say that $G$ is a **semi-direct product** of $N$ and $B$.

Let $N$ be any group. Let $\mathrm{Aut}(N)$ be the set of automorphisms of the group $N$. It is a group in its own right under composition of functions.

Let $B$ be another group and $\phi\colon B \to \mathrm{Aut}(N), b \mapsto \phi_b$ be a homomorphism (so $\phi_{b_1b_2} = \phi_{b_1} \circ \phi_{b_2}$). Define a group, called the **semi-direct product of $N$ and $B$ relative to $\phi$**

$$G = N \rtimes_\phi B$$

as follows: as a set $G = N \times B$, but the group law is defined as

$$(n_1, b_1)(n_2, b_2) = (n_1 \cdot \phi_{b_1}(n_2), b_1b_2).$$

We check associativity:

$$\begin{aligned}[(n_1,b_1)(n_2,b_2)](n_3,b_3) &= (n_1\cdot\phi_{b_1}(n_2), b_1b_2)(n_3,b_3)\\ &= (n_1\cdot\phi_{b_1}(n_2)\cdot\phi_{b_1b_2}(n_3), b_1b_2b_3)\\ &= (n_1\cdot\phi_{b_1}(n_2\cdot\phi_{b_2}(n_3)), b_1b_2b_3)\\ &= (n_1,b_1)(n_2\cdot\phi_{b_2}(n_3), b_2b_3)\\ &= (n_1,b_1)[(n_2,b_2)(n_3,b_3)].\end{aligned}$$

The identity is clearly $(1_N, 1_B)$. The inverse of $(n_2, b_2)$ is $(\phi_{b_2^{-1}}(n_2^{-1}), b_2^{-1})$. Thus $G$ is a group.

The two bijections

$$N \to G, \quad n \mapsto (n,1); \qquad B \to G, \quad b \mapsto (1,b),$$

are group isomomorphisms. We identify $N$ and $B$ with their images in $G$. We claim that $G$ is indeed a semi-direct product of $N$ and $B$: Clearly the first two properties of the definition hold. It remains to check that $N$ is normal and it's enough to verify that $B \subset N_G(N)$. According to the calculation above:

$$(1,b)(n,1)(1,b^{-1}) = (\phi_b(n), 1).$$

The last formula is interesting: the construction of the semi-direct product $G = N \rtimes_\phi B$ transforms the abstract action of $B$ on $N$ provided by $\phi\colon B \to \mathrm{Aut}(N)$, into conjugation inside the group $G$.

We now claim that every semi-direct product is obtained this way: Let $G$ be a semi-direct product of $N$ and $B$. Let $\phi_b\colon N \to N$ be the map $n \mapsto bnb^{-1}$. That is, $\phi_b(n) = bnb^{-1}$. This is an automorphism of $N$ and the map

$$\phi\colon B \to \mathrm{Aut}(N)$$

is a group homomorphism. We claim that $N \rtimes_\phi B \cong G$. Indeed, define a map

$$(n,b) \mapsto nb.$$

It follows from the definition that the map is surjective. It is a group homomorphism, because $(n_1\cdot\phi_{b_1}(n_2), b_1b_2) \mapsto n_1\phi_{b_1}(n_2)b_1b_2 = n_1b_1n_2b_1^{-1}b_1b_2 = (n_1b_1)(n_2b_2)$. It is also injective since $nb = 1$ implies that $n = b^{-1} \in N \cap B$, hence $n = 1$.

The construction of direct product also follows into this paradigm. To be precise:

**Proposition 27.0.2.** *A semi-direct product $N \rtimes_\phi B$ is the direct product $N \times B$ if and only if the homomorphism $\phi\colon B \to \mathrm{Aut}(N)$ is the trivial homomorphism.*

*Proof.* Indeed, we get the direct product if and only if for all pairs $(n_1, b_1), (n_2, b_2)$ we have $(n_1\phi_{b_1}(n_2), b_1b_2) = (n_1n_2, b_1b_2)$. That is, iff for all $b_1, n_2$ we have $\phi_{b_1}(n_2) = n_2$, which implies $\phi_{b_1} = id$ for all $b_1$. That is, $\phi$ is the trivial homomorphism. □

**Example 27.0.3.** The Dihedral group $D_{2n}$ is a semi-direct product. Take $N = \langle x \rangle \cong \mathbb{Z}/n\mathbb{Z}$ and $B = \langle y \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Then $D_{2n} \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$ with $\phi_1 = -1$.

27.1. **Application to groups of order $pq$.** We have seen in § 23.2.5 that if $p < q$ and $p \nmid (q-1)$ then every group of order $pq$ is abelian. Assume therefore that $p|(q-1)$.

**Proposition 27.1.1.** *If $p|(q-1)$ there is a unique non-abelian group of order $pq$, up to isomorphism.*

*Proof.* Let $G$ be a non-abelian group of order $pq$. We have seen that in every such group $G$ the $q$-Sylow subgroup $Q$ is normal. Let $P$ be any $p$-Sylow subgroup. Then $P \cap Q = \{1\}$ and $G = QP$. Thus, $G$ is a semi-direct product of $Q$ and $P$.

It is thus enough to show then that there *is* a non-abelian semi-direct product and that any two such products are isomorphic. We may consider the case $Q = \mathbb{Z}/q\mathbb{Z}, P = \mathbb{Z}/p\mathbb{Z}$.

**Lemma 27.1.2.** $\mathrm{Aut}(Q) = (\mathbb{Z}/q\mathbb{Z})^\times$.

*Proof.* Since $Q$ is cyclic any group homomorphism $f\colon Q \to H$ is determined by its value on a generator of $Q$, say the generator 1. Conversely, if $h \in H$ is of order dividing $q$ then there is such a group homomorphism with $f(1) = h$.

Now, take $H = Q$. The image of $f$ is the cyclic subgroup $\langle h \rangle$ and thus $f$ is surjective (equivalently, isomorphic) iff $h$ is a generator. Thus, any element $h \in (\mathbb{Z}/q\mathbb{Z})^\times$ determines an automorphism $f_h$ of $Q$ by $a \mapsto f_h(a) := ha$, and every automorphism must have this shape. Note that $f_h(f_g)(a) = f_h(ga) = hga = f_{hg}(a)$ and so the association $h \leftrightarrow f_h$ is a group isomorphism $(\mathbb{Z}/q\mathbb{Z})^\times \cong \mathrm{Aut}(Q)$. □

Since $(\mathbb{Z}/q\mathbb{Z})^\times$ is a cyclic group of order $q-1$ (Corollary 4.2.3), and since by assumption $p|(q-1)$, there is an element $h$ of exact order $p$ in $(\mathbb{Z}/q\mathbb{Z})^\times$. We denote, as above, the matching element in $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ by $f_h$.

Let $\phi$ be the homomorphism determined by $\phi_1 = f_h$ and let $G = Q \rtimes_\phi P$. We claim that $G$ is not abelian.

$$(n,0)(0,b) = (n,b), \quad (0,b)(n,0) = (\phi_b(n), b).$$

The two are always equal only if $\phi_b(n) = n$ for all $b$ and $n$, i.e., $\phi_b = Id$ for all $b$, but choosing $b = 1$ we get $\phi_1 = f_h$, which is not the identity map. Contradiction.

We now show that $G$ is unique up to isomorphism. If $H$ is another such semi-direct product then $H = \mathbb{Z}/q\mathbb{Z} \rtimes_\psi \mathbb{Z}/p\mathbb{Z}$, where $\psi_1$ is an element of order $p$ (if it is the identity $H$ is abelian) and thus $\psi_1 = \phi_1^r = \phi_r$ for some $r$ prime to $p$.

Define a map

$$\mathbb{Z}/q\mathbb{Z} \rtimes_\psi \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z}, \quad (n,b) \mapsto (n, rb).$$

This function is easily checked to be injective, hence bijective. We check it is a group homomorphism:

In $G$ we have $(n_1, rb_1)(n_2, rb_2) = (n_1 + \phi_{rb_1}(n_2), r(b_1+b_2)) = (n_1 + \psi_{b_1}(n_2), r(b_1+b_2))$. This is the image of the element $t := (n_1 + \psi_{b_1}(n_2), b_1 + b_2)$ of $H$; but $t$ is the product $(n_1, b_1)(n_2, b_2)$ in $H$. The finishes the proof of the Proposition. □

**Example 27.1.3.** Is there a non-abelian group of order $165 = 3 \cdot 5 \cdot 11$ containing $\mathbb{Z}/55\mathbb{Z}$?

In such a group $G$, the subgroup $\mathbb{Z}/55\mathbb{Z}$ would be normal (because, say, its index is the minimal prime dividing the order of $G$ – see Exercise 37). Since there is always a 3-Sylow, we conclude that $G$ is a semi-direct product $\mathbb{Z}/55\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$. This is determined by a homomorphism $\mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/55\mathbb{Z}) \cong (\mathbb{Z}/55\mathbb{Z})^\times$. The right hand side has order $\varphi(55) = 4 \cdot 10$. Thus, the homomorphism is trivial and $G$ is a direct product. It follows that $G$ must be commutative.

27.2. **Cases where two semi-direct products are isomorphic.** It is useful to generalize the arguments showing that all non-trivial semi-direct products $\mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z}$ are isomorphic.

Let $\phi\colon B \to \mathrm{Aut}(N)$, $b \mapsto \phi_b$, be a homomorphism and consider the group

$$G = N \rtimes_\phi B.$$

Consider two automorphisms of groups

$$f\colon N \to N, \quad g\colon B \to B.$$

Let $S$ be $G$, considered merely as a set, and consider the bijective self map $h$ defined by

$$h : S \to S, \quad (n, b) \overset{h}{\mapsto} (f(n), g(b)).$$

We may define a new group law on $S$ by "transport of structure"; that is, let

$$\begin{aligned}(n_1, b_1) * (n_2, b_2) &= h\left[h^{-1}(n_1, b_1) \cdot h^{-1}(n_2, b_2)\right] \\ &= h\left[(f^{-1}(n_1), g^{-1}(b_1)) \cdot (f^{-1}(n_2), g^{-1}(b_2))\right] \\ &= h\left[(f^{-1}(n_1) \cdot \phi_{g^{-1}(b_1)}(f^{-1}(n_2)), g^{-1}(b_1) \cdot g^{-1}(b_2))\right] \\ &= (n_1 \cdot (f \circ \phi_{g^{-1}(b_1)} \circ f^{-1})(n_2), b_1 b_2)\end{aligned}$$

Clearly, $S$ with the new group law is isomorphic as a group to $G$; the isomorphism is provided by $h\colon G \to S$. Let

$$\psi : B \to \mathrm{Aut}(N), \qquad \psi_b := f \circ \phi_{g^{-1}(b)} \circ f^{-1}.$$

Then $\psi$ is a group homomorphism, and we have the isomorphism

$$G = N \rtimes_\phi B \cong N \rtimes_\psi B,$$

where the isomorphism is

$$(n, b) \mapsto (f(n), g(b)).$$

It is sometimes convenient to replace $g$ by $g^{-1}$ and conclude the following

**Summary:** *Let*

$$\psi : B \to \mathrm{Aut}(N), \qquad \psi_b := f \circ \phi_{g(b)} \circ f^{-1}.$$

*Then $\psi$ is a group homomorphism, and we have the isomorphism*

$$G = N \rtimes_\phi B \cong N \rtimes_\psi B, \quad (n, b) \mapsto (f(n), g^{-1}(b)).$$

To illustrate, in the case of groups of order $pq$ we took $f = id$ and let $g$ vary over all possible automorphisms of $\mathbb{Z}/p\mathbb{Z}$ so see that as $g$ varies the maps $\psi$ that we get are *all* the non-zero homomorphisms $\mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z}/q\mathbb{Z})^\times$ thereby proving the uniqueness of non-abelian groups of order $pq$.

## 28. Groups of low, or simple, order

28.1. **Groups of prime order.** Let $p$ be a prime and $G$ a group of order $p$. We have seen that all such groups are cyclic. By Example 7.1.2, the unique cyclic group of order $p$ up to isomorphism is $\mathbb{Z}/p\mathbb{Z}$.

28.2. **Groups of order $p^2$.** Every such group is abelian. By the structure theorem it is either isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ or to $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$.

28.3. **Groups of order $pq$, $p<q$ primes.** This case was discussed in § 27.1 above. We summarize the results: there is a unique abelian group of order $pq$ and it is cyclic. If $p\nmid(q-1)$ then every group of order $pq$ is abelian. If $p|(q-1)$ there is a unique non-abelian group up to isomorphism; it can be taken as any non trivial semi-direct product $\mathbb{Z}/q\mathbb{Z}\rtimes\mathbb{Z}/p\mathbb{Z}$.

28.3.1. *Groups of order* $1,2,3,4,5,6,7,9,10,11,13,14,15$. The results about groups of prime order and of order $pq$, $p\le q$ allow us to determine the following possibilities:

| order | abelian groups | non-abelian groups |
|---|---|---|
| 1 | $\{1\}$ | |
| 2 | $\mathbb{Z}/2\mathbb{Z}$ | |
| 3 | $\mathbb{Z}/3\mathbb{Z}$ | |
| 4 | $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ | |
| 5 | $\mathbb{Z}/5\mathbb{Z}$ | |
| 6 | $\mathbb{Z}/6\mathbb{Z}$ | $S_3$ |
| 7 | $\mathbb{Z}/7\mathbb{Z}$ | |
| 9 | $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$ | |
| 10 | $\mathbb{Z}/10\mathbb{Z}$ | $D_5$ |
| 11 | $\mathbb{Z}/11\mathbb{Z}$ | |
| 13 | $\mathbb{Z}/13\mathbb{Z}$ | |
| 14 | $\mathbb{Z}/14\mathbb{Z}$ | $D_7$ |
| 15 | $\mathbb{Z}/15\mathbb{Z}$ | |

28.4. **Groups of order 8.** We know already the structure of abelian groups of order 8: $(\mathbb{Z}/2\mathbb{Z})^3$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$. We also know two non-isomorphic non-abelian groups of order 8: the dihedral group $D_4$ and the quaternion group $Q$ (in $Q$ there are six elements of order 4, while in $D_4$ there are two).

We prove that every non-abelian group $G$ of order 8 is isomorphic to either $D_4$ or $Q$. Suppose that $G$ has a non-normal subgroup of order 2. Then the kernel of the coset representation $G\to S_4$ is trivial. Thus, $G$ is a 2-Sylow subgroup of $S_4$, but so is $D_4$. Since all 2-Sylow subgroups are conjugate, hence isomorphic, we conclude that $G\cong D_4$.

Thus, assume that $G$ doesn't have a non-normal subgroup of order 2. Consider the center $Z(G)$ of $G$. We claim that the center has order 2. Indeed, otherwise $G/Z(G)$ is of order 2 hence cyclic. But $G/Z(G)$ can never be a non-trivial cyclic group (see Lemma 21.1.1).

We now claim that $Z(G) = \{1, z\}$ is the unique subgroup of $G$ of order 2. Indeed, if $\{1, h\} = H < G$ is a subgroup of order 2 it must be normal by hypothesis. Then, for every $g \in G$, $ghg^{-1} = h$, i.e. $h \in Z(G)$ and so $H = Z(G)$.

It follows that every element $x$ in $G$ apart from 1 or $z$ has order 4, and so every such $x$ satisfies $x^2 = z$. Rename $z$ to $-1$ and the rest of the elements (which are of order 4, so come in pairs) may then denoted by $i, i^{-1}, j, j^{-1}, k, k^{-1}$. Since $i^2 = j^2 = k^2 = -1$ we can write $i^{-1} = -i$, etc.

Note that the subgroup $\langle i, j \rangle$ must be equal to $G$ and so $i$ and $j$ do not commute. Thus, $ij \neq 1, -1, i, -i, j, -j$ (for example, $ij = -i$ implies that $j = (-i)ij = (-i)^2 = -1$ and so commutes with $i$). Without loss of generality $ij = k$ and then $ji = -k$ (because the only other possibility is $ji = k$ which gives $ij = ji$). We therefore get the relations (the new ones are easy consequences):

$$G = \{\pm 1, \pm i, \pm j, \pm k\}, \quad i^2 = j^2 = k^2 = -1,\ ij = -ji = k.$$

This determines completely the multiplication table of $G$ which is identical to that of $Q$. Thus, $G \cong Q$.

28.5. **Groups of order** 12**.** We continue our discussion from Example 23.2.3. We know that the abelian groups are $\mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. We are also familiar with the groups $A_4$ and $D_6$. One checks that in $A_4$ there are no elements of order 6 so these two groups are not isomorphic.

Note that in $A_4$ a 3-Sylow is not normal, but the 2-Sylow subgroup is normal (it is the Klein group $V = \{1, (12)(34), (13)(24), (14)(23)\}$). Note that in $D_6$ the 3-Sylow is normal. It is given by $\{1, x^2, x^4\}$. To see it is normal one can note that the rest of the elements of $D_6$ are the 6 reflections and the rotations $x, x^3, x^5$, none of which is an element of order 3. As conjugation preserves order, the conclusion follows.

As we have already seen, in a non-abelian group of order $12 = 2^2 3$, either the 3-Sylow is normal or the 2-Sylow is normal, but not both.

We conclude that a non-abelian group of order 12 is the semi-direct product of a group of order 4 and a group of order 3. For example, one checks that

$$A_4 = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z},$$

and

$$D_6 = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \ltimes \mathbb{Z}/3\mathbb{Z}.$$

We have already explained that every semi-direct product $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ is actually a direct product and so is commutative. Let us then consider a semi-direct product $\mathbb{Z}/4\mathbb{Z} \ltimes \mathbb{Z}/3\mathbb{Z}$ Here $1 \in \mathbb{Z}/4\mathbb{Z}$ acts on $\mathbb{Z}/3\mathbb{Z}$ as multiplication by $-1$. This gives a non-abelian group with a cyclic group of order 4 that is therefore not isomorphic to the previous groups. Call it $T$:

$$T = \mathbb{Z}/4\mathbb{Z} \ltimes \mathbb{Z}/3\mathbb{Z}.$$

The proof that these are all the non-abelian groups of order 12 is easy given the results of §27.2. We already know that every such group is a non-trivial semi-direct product $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \ltimes \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z} \ltimes \mathbb{Z}/3\mathbb{Z}$.

A non-trivial homomorphism $\mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = \mathrm{GL}_2(\mathbb{F}_2) \cong S_3$ corresponds to an element of order 3 in $S_3$. All those elements are conjugate and by § 27.2 all these semi-direct products are isomorphic.

A non-trivial homomorphism $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ is determined by its kernel which is a subgroup of order 2 = line in the 2-dimensional vector space $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ over $\mathbb{Z}/2\mathbb{Z}$. The automorphism group of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ acts transitively on lines and by § 27.2 all these semi-direct products are isomorphic.

A non-trivial homomorphism $\mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ is uniquely determined.

## 29. Free groups, generators and relations

Let $X$ be a set. It will be called the **alphabet**. A **word** $\omega$ in the **alphabet** $X$ is a finite string $\omega = \omega_1\omega_2\dots\omega_n$, where each $\omega_i$ is equal to either $x \in X$ or $x^{-1}$ for $x \in X$. Here $x^{-1}$ is a formal symbol. So, for example, if $X = \{x\}$ then words in $X$ are $x, xxx^{-1}x, \emptyset$, etc. If $X = \{x, y\}$ we have as examples $x, y, x^{-1}yyxy, x^{-1}y^{-1}y$, and so on. We say that two words $\omega, \sigma$ are **equivalent words** if one can get from one word to the other performing the following basic operations:

*Replace $\omega_1 \dots \omega_i xx^{-1}\omega_{i+1}\dots\omega_n$ and $\omega_1\dots\omega_i x^{-1}x\omega_{i+1}\dots\omega_n$ by $\omega_1\dots\omega_i\omega_{i+1}\dots\omega_n$, and the opposite of those operations (i.e., inserting $xx^{-1}$ or $x^{-1}x$ at some point in the word).*

We denote this equivalence relation by $\omega \sim \sigma$. For example, for $X = \{x, y\}$ we have

$$x \sim xyy^{-1} \sim xyxx^{-1}y^{-1} \sim xyy^{-1}yxx^{-1}y^{-1}.$$

A word is called **reduced** if it does not contain a string of the form $xx^{-1}$ or $x^{-1}x$ for some $x \in X$.

We now construct a group $\mathscr{F}(X)$ called the **free group on** $X$ as follows. The elements of the group $\mathscr{F}(X)$ are equivalence classes

$$[\omega] = \{\sigma | \sigma \sim \omega\}$$

of words in the alphabet $X$. Multiplication is defined using representatives:

$$[\sigma][\tau] = [\sigma\tau]$$

(the two words are simply written one after the other). It is easy to see that this is well-defined on equivalence classes: the operations performed on $\sigma$ to arrive at an equivalent word $\sigma'$ can be performed on the initial part of $\sigma\tau$ to arrive at $\sigma'\tau$, etc. The identity element is the empty word; we also denote it 1, for convenience. The inverse of $[\omega]$ where $\omega = \omega_1\dots\omega_n$ is the equivalence class of $\omega_n^{-1}\dots\omega_1^{-1}$ (where we define $(x^{-1})^{-1} = x$ for $x \in X$). Finally, the associative law is clear. We have constructed a group. Clearly this group depends up to isomorphism only on the cardinality of the set $X$. Name, if we have a bijection of sets $X \cong Y$ then it induces an isomorphism $\mathscr{F}(X) \cong \mathscr{F}(Y)$; for that reason we may denote $\mathscr{F}(X)$ simply by $\mathscr{F}(d)$, where $d$ is the cardinality of $X$.

29.1. **Properties of free groups.** The group $\mathscr{F}(d)$ has the following properties:

(1) Given a group $G$, and $d$ elements $s_1, \dots s_d$ in $G$, there is a unique group homomorphism $f\colon \mathscr{F}(d) \to G$ such that $f(x_i) = s_i$. Indeed, one first defines for a word $y_1\dots y_t$, $y_i = x_{n(i)}^{e_i}, e_i \in \{\pm 1\}$, $f(y_1\cdots y_t) = s_{n(1)}^{e_1}\cdots s_{n(t)}^{e_t}$. One checks that equivalent words have the same image and so one gets a well defined function $\mathscr{F}(d) \to G$. It is easily verified to be a homomorphism.

(2) If $G$ is a group generated by $d$ elements there is a surjective group homomorphism $\mathscr{F}(d) \to G$. This follows immediately from the previous point. If $s_1, \dots, s_d$ are generators take the homomorphism taking $x_i$ to $s_i$.

(3) If $w_1, \dots w_r$ are words in $\mathscr{F}(d)$, let $N$ be the minimal normal subgroup containing all the $w_i$ (such exists!). The group $\mathscr{F}(d)/N$ is also denoted

$$\langle x_1, \dots, x_d | w_1, \dots, w_r\rangle$$

and is said to be given by the generators $x_1, \dots x_d$ and relations $w_1, \dots, w_r$. For example, one can prove the isomorphisms $\mathbb{Z} \cong \mathscr{F}(1)$, $\mathbb{Z}/n\mathbb{Z} \cong \langle x_1 | x_1^n\rangle$, $\mathbb{Z}^2 \cong \langle x_1, x_2 | x_1x_2x_1^{-1}x_2^{-1}\rangle$, $S_3 \cong \langle x_1, x_2 | x_1^2, x_2^3, (x_1x_2)^2\rangle$, $D_{2n} \cong \langle x, y | x^n, y^2, xyxy\rangle$. This is discussed in more detail below.

(4) If $d = 1$ then $\mathscr{F}(d) \cong \mathbb{Z}$, but if $d > 1$ then $\mathscr{F}(d)$ is a non-commutative infinite group. In fact, for every $k$, $S_k$ is a homomorphic image of $\mathscr{F}(d)$ if $d \geq 2$. And since $S_k$ is not abelian for $k \geq 3$, so must be the groups $\mathscr{F}(d)$ for $d \geq 2$

### 29.2. **Reduced words.**

**Theorem 29.2.1.** *Any word is equivalent to a unique reduced word.*

*Proof.* It is clear that every word is equivalent to some reduced word. We need to show that two reduced words that are equivalent are in fact equal. Let $\omega$ and $\tau$ be equivalent reduced words. Then, there is a sequence

$$\omega = \sigma_0 \sim \sigma_1 \sim \cdots \sim \sigma_n = \tau,$$

where at each step we either insert, or delete, one couple of the form $xx^{-1}$ or $x^{-1}x$, $x \in X$. Let us look at the lengths of the words. The length function, evaluated along the chain, receives a relative minimum at $\omega$ and $\tau$. Suppose it receives another relative minimum first at $\sigma_r$ (so the length of $\sigma_{r-1}$ is bigger than that of $\sigma_r$ and the length of $\sigma_r$ is smaller than that of $\sigma_{r+1}$. We can take $\sigma_r$ and reduce it by erasing repeatedly pairs of the form $xx^{-1}$, or $x^{-1}x$, until we cannot do that any more. We get a chain of equivalences $\sigma_r = \alpha_0 \sim \alpha_1 \sim \cdots \sim \alpha_s$, where $\alpha_s$ is a reduced word. We now modify our original chain to the following chain

$$\omega = \sigma_0 \sim \sigma_1 \sim \cdots \sim \sigma_r = \alpha_0 \sim \cdots \sim \alpha_{s-1} \sim \alpha_s \sim \alpha_{s-1} \sim \cdots \sim \alpha_0 = \sigma_r \sim \sigma_{r+1} \ldots \sigma_n = \tau.$$

A moment reflection shows that by this device, we can reduce the original claim to the following.

*Let $\sigma$ and $\tau$ be two reduced words that are equivalent as follows:*

$$\omega = \sigma_0 \sim \sigma_1 \sim \cdots \sim \sigma_n = \tau$$

*where the length increases at every step from $\sigma_0$ to $\sigma_a$ and decreases from $\sigma_a$ to $\sigma_n = \tau$. Then $\sigma = \tau$.*

We view $\sigma$ and $\tau$ as two reduced words obtained by cancellation only from the word $\sigma_a$. We argue by induction on the length of $\sigma_a$.

If $\sigma_a$ is reduced, there's nothing to prove because then necessarily $0 = a = n$ and we are considering a tautology. Else, there is a pair of the form $dd^{-1}$ or $d^{-1}d$ in $\sigma_a$. We allow ourselves here $(d^{-1})^{-1} = d$ and then we may say that there is a pair $dd^{-1}$ where $d$ or $d^{-1}$ are in $X$. Let us highlight that pair using a yellow marker and keep track of it. If in the two cancellations processes (one leading to $\sigma$, the other to $\tau$) the first step is to delete the highlighted pair, then using induction for the word $\sigma_a$ with the highlighted pair deleted, we may conclude that $\sigma = \tau$. If in the cancellation process leading to $\sigma$ at some point the highlighted pair is deleted, then we may change the order of the cancellations so that the highlighted pair is deleted first. Similarly concerning the reduction to $\tau$. And so, in those cases we return to the previous case. Thus, we may assume that in either the reduction to $\sigma$, or the reduction to $\tau$, the highlighted pair is not deleted. Say, in the reduction to $\sigma$. How then can $\sigma$ be reduced? The only possibility is that at some point in the reduction process (not necessarily the first point at which it occurs) we arrive at a word of the form $\cdots d^{-1}\boxed{dd^{-1}}\cdots$ or $\cdots\boxed{dd^{-1}}d\cdots$ and then it is reduced to $\cdots \not{d}^{-1}\boxed{\not{d}d^{-1}}\cdots$ or $\cdots\boxed{d\not{d}^{-1}}\not{d}\cdots$. But note that the end result is the same as if we strike out the highlighted pair. So we reduce to the previous case. ☐

Note that as a consequence, if $\omega \in [\omega]$ is a word whose length is the minimum of the lengths of all words in $[\omega]$ then $\omega$ is the unique reduced word in the equivalence class $[\omega]$.

29.3. **Generators and relations.** Let $X$ be a set. Denote by $\mathscr{F}(X)$ the free group on $X$, as above. Let $R = \{r_\alpha\}$ a collection of words in the alphabet $X$. We define the group $G$ generated by $X$, subject to the **relations** $R$ as follows. Let $N$ be the minimal *normal* subgroup of $\mathscr{F}(X)$ containing $[r]$ for all $r \in R$. Define $G$ as $\mathscr{F}(X)/N$. Note that in $G$ any word $r \in R$ becomes trivial. Note also that $G$ is a universal object for this property. Namely, given a function $f\colon X \to H$, $H$ a group, such that $f(r) = 1_H$ for all $r \in R$ (where if $r = \omega_1 \dots \omega_n$, $\omega_i = x^{\pm 1}$ for $x \in X$, then $f(r) := f(\omega_1) \cdots f(\omega_n)$ (with $f(x^{-1}) := f(x)^{-1}$)), there is a unique homomorphism $F\colon G \to H$ such that $F([r] \pmod N) = f([r])$. We denote $G$ also by

$$\langle X | R \rangle.$$

A **presentation** of a group $H$ is an isomorphism

$$H \cong \langle X | R \rangle$$

for some $X$ and $R$. A group can have many presentations. There is always the tautological presentation. Take $X = \{\underline{g}\colon g \in G\}$ - we write $\underline{g}$ so that we can distinguish between $g$ as an element of the group $G$ and $\underline{g}$ an element of $X$, and take

$$R = \{r = \underline{\omega_1} \dots \underline{\omega_n} : \text{in the group } G \text{ we have that the product } \omega_1 \cdots \omega_n = 1_G\}.$$

But usually there are more interesting, and certainly more economical presentations.

(1) Let $\mathscr{F}(X)'$ be the commutator subgroup of $\mathscr{F}(X)$ then $\langle X : \mathscr{F}(X)' \rangle$ is a presentation of the free abelian group on $X$. But, for example, for $X = \{x, y\}$, we have the more economical presentation

$$\langle \{x, y\} : xyx^{-1}y^{-1} \rangle.$$

Lets prove it. First, from the universal property, since in $\mathbb{Z}^2$ all commutators are trivial, there is a unique homomorpism

$$\langle \{x, y\} : xyx^{-1}y^{-1} \rangle \;\to\; \mathbb{Z}^2, \qquad x \mapsto (1, 0), y \mapsto (0, 1).$$

Clearly this is a surjective homomorphism. Define now a homomorphism

$$\mathbb{Z}^2 \to \langle \{x, y\} : xyx^{-1}y^{-1} \rangle, \qquad f(m, n) = x^m y^n.$$

We need to show that $f$ is a homomorphism. Namely, that in the group $\langle \{x, y\} : xyx^{-1}y^{-1} \rangle$ we have

$$x^a y^b x^c y^d = x^{a+c} y^{b+d}.$$

It's enough to show that $xy = yx$ because then we may pass the powers of $x$ through those of $y$ one at the time. But we have the equality $yx = (xyx^{-1}y^{-1})(yx) = xy$. It is easy to check that $f$ is an inverse to the previous homomorphism.

(2) $S_n$ is generated by the permutations $(12)$ and $(12 \cdots n)$ and so it follows that it has a presentation of the kind $\langle \{x, y\} : R \rangle$ for some set of relations $R$; for example, $R$ could be the kernel of the surjective homomorphism $\mathscr{F}(\{x, y\}) \to S_n$ that takes $x$ to $(12)$ and $y$ to $(12 \cdots n)$. As such, $R$ is an infinite set. But, can we replace $R$ be a finite list of relations? The answer is yes. It follows from the following two theorems, that we will not prove in this course. One reason for that being that the best proofs use the theory of covering spaces and fundamental groups that we do not assume as prerequisites to this course.

**Theorem 29.3.1.** *(Nielsen-Schreier) A subgroup of a free group is free.*

**Theorem 29.3.2.** *Let $F$ be a free group of rank $r$ and let $H$ be a subgroup of $F$ of finite index $h$. The $H$ is free of rank $h(r-1)+1$.*

It follows that we can determine all the relations in $S_n$ as a consequence of certain $n! + 1$ relations. However, this is far from optimal. For example, $S_3$ has the presentation

$$\langle \{x, y\} : x^2, y^3, xyxy \rangle$$

The explanation for this particular saving is that we take the minimal *normal* subgroup generated by the relations and not the minimal subgroup generated by the relations. In this example, the minimal normal subgroup generated by these relations has rank $7 = 3! + 1$, while the minimal subgroup generated by these relations has rank at most 3. We leave it as an exercise to prove that this is indeed a presentation for $S_3$ and to find a similar presentation for $S_4$.

(3) After experimenting a little with examples, one easily concludes that it is in general difficult to decide whether a finitely presented group is isomorphic to a given one. In fact, a theorem (which is essentially "the word problem" for groups) says that there is no algorithm that given as an input a finite presentation $\langle X|R\rangle$, $X$ and $R$ finite, will decide in finite time whether this is a presentation of the finite group or not.

29.4. **Some famous problems in group theory.** Fix positive integers $d, n$. The **Burnside problem** asks if a group generated by $d$ elements in which every element $x$ satisfies $x^n = 1$ is finite. Every such group is a quotient of the following group $B(d, n)$: it is the free group $\mathscr{F}(d)$ generated by $x_1, \dots, x_d$ moded out by the minimal normal subgroup containing the expressions $f^n$ where $f$ is an element of $\mathscr{F}(d)$. It turns out that in general the answer is negative; $B(d, n)$ is infinite for $d \geq 2, n \geq 4381$, $n$ odd. There are some instances where it is finite: $d \geq 2, n = 2, 3, 4, 6$.

One can then ask, is there a finite group $B_0(d, n)$ such that every finite group $G$, generated by $d$ elements and in which $f^n = 1$ for every element $f \in G$, is a quotient of $B_0(d, n)$? E. Zelmanov, building on the work of many others, proved that the answer is yes. He received the 1994 Fields medal for this.

The **word problem** asks whether there is an algorithm (guaranteed to stop in finite time) that determines whether a finitely presented group, that is a group gives by generators and relations as $\langle x_1, \dots, x_d | w_1, \dots, w_r\rangle$ for some integers $d, r$, is the trivial group or not. It is known that the answer to this question (and almost any variation on it!) is *no*. This has applications to topology. It is known that every finitely presented group is the fundamental group of a manifold[14] of dimension 4. It then follows that there is no good classification of 4-manifolds. If one can decide if a manifold $X$ is isomorphic to the 4-dimensional sphere or not, one can decide the question of whether the fundamental group of $X$ is isomorphic to that of the sphere, *which is the trivial group*, and so solve the word problem.

[14]A manifold of dimension 4 is a space that locally looks like $\mathbb{R}^4$. The fundamental group is a topological construction that associate a group to any topological space. The group has as its elements equivalent classes of closed loops in the space, starting and ending at some arbitrarily chosen point, where if we can deform, within the space, one loop to another we consider them as the same element of the fundamental group.

# **Part** 8. **Complex representations of finite groups**

## 30. THE SETTING AND THE MAIN THEOREMS

30.1. **Basic definitions and conventions.** In this part of the notes, a *vector space* $V$ would always denote a finite dimensional vector space over the complex numbers. If $V, W$, are vector spaces then

$$\mathrm{Hom}(V, W),$$

denotes the $\mathbb{C}$-linear maps $T\colon V \to W$; $\mathrm{Hom}(V, W)$ is a $\mathbb{C}$-vector space whose dimension is $\dim(V) \cdot \dim(W)$. A particular case is

$$\mathrm{End}(V) := \mathrm{Hom}(V, V),$$

which is not just a $\mathbb{C}$-vector space of dimension $\dim(V)^2$, but in fact a ring under addition of linear maps and where multiplication is given by composition of maps. By

$$\mathrm{Aut}(V)$$

we mean the invertible elements of $\mathrm{End}(V)$, namely, all the invertible linear transformations $T\colon V \to V$. Throughout, $G$ denotes a finite group.

The main definition of this part of the course is the following:

**Definition 30.1.1.** A finite dimensional **linear representation** of $G$ is a homomorphism

$$\rho\colon G \to \mathrm{Aut}(V),$$

for some finite dimensional vector space $V$.

We will usually just say "representation" and not "finite-dimensional linear representation", which is a bit of a mouthful. Note: a representation of $G$ is really two pieces of data: (i) $\rho$ and (ii) $V$. And so, we will often say that $(\rho, V)$ is a representation of $G$. Also note that when we are given a representation, the group $G$ acts on the set $V$ in the sense of groups actions on sets, albeit in a very particular way – through linear invertible transformations.

**Definition 30.1.2.** A **morphism of representations** $T\colon (\rho_1, V_1) \to (\rho_2, V_2)$ is a linear map

$$T\colon V_1 \to V_2,$$

such that

$$\rho_2(g) \circ T = T \circ \rho_1(g), \qquad \forall g \in G.$$

In diagram:

$$\begin{array}{ccc} V_1 & \xrightarrow{\rho_1(g)} & V_1 \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle T} \\ V_2 & \xrightarrow{\rho_2(g)} & V_2 \end{array}, \qquad \forall g \in G.$$

An **isomorphism of representations** is such a bijective morphism $T$.

There is therefore an *important distinction*. Even if $V_1, V_2$ are representations of $G$ we use $\mathrm{Hom}(V_1, V_2)$ to denote the linear maps from $V_1$ to $V_2$. We shall use

$$\mathrm{Hom}_G(V_1, V_2)$$

to denote the morphisms of representations $(\rho_1, V_1) \to (\rho_2, V_2)$. It is a subspace of $\mathrm{Hom}(V_1, V_2)$ (and more on that below). A more accurate notation for $\mathrm{Hom}_G(V_1, V_2)$ is $\mathrm{Hom}_G((\rho_1, V_1), (\rho_2, V_2))$ but we shall avoid if we can, because it is harder to read.

Let $(\rho, V)$ be a representation of $G$. A **sub-representation** is a subspace $W \subseteq V$ such that for all $g \in G$ we have

$$\rho(g)(W) \subseteq W.$$

In fact, we then have necessarily $\rho(g)(W) = W$ because $\rho(g)$ is invertible and so $\rho(g)(W)$ and $W$ have the same dimension. In that case $(\rho|_W, W)$ is a representation and the inclusion map $(\rho|_W, W) \to (\rho, V)$ is a morphism of representations. Note that $V$ and $\{0\}$ are always sub-representations and we shall refer to them as trivial sub-representations.

The following definition is one of the key concepts.

**Definition 30.1.3.** A representation $(\rho, V)$ is called **irreducible** if $V \neq \{0\}$ and its only sub-representations are the trivial ones.

Before giving some examples, we give some general constructions of representations that will be used repeatedly.

30.2. **Constructing new representations from old.** Let $G$ be a group and $(\rho, V), (\tau, W)$ be two representations of $G$. Then

$$(\rho \oplus \tau, V \oplus W)$$

is a representation of $G$ where

$$(\rho \oplus \tau)(g) = (\rho(g), \tau(g)).$$

This representation is called the **direct sum representation**. If we wish, we can also use the notation $\rho(g) \oplus \tau(g)$, which we have used before for the direct sum of two linear maps. We will often be rather loose with our notation and write either $V \oplus W$, or $\rho \oplus \tau$, for the direct sum. Similarly, we shall write the direct sum of $(\rho, V)$ with itself $a$-times as either $(\rho, V)^a$, $V^a$ or $\rho^a$.

Another construction is

$$\mathrm{Hom}(V, W).$$

Let us the denote the representation simply by

$$\sigma : G \to \mathrm{Aut}(\mathrm{Hom}(V, W)),$$

where for every $g \in G$, $T : V \to W$,

$$\sigma(g)(T) := \tau(g) \circ T \circ \rho(g^{-1}).$$

There is actually quite a bit to verify here. We only indicate what should be verified and leave the verification as an exercise.

- As $\mathrm{Hom}(V, W)$ is a complex vector space, we need to verify that for every $g \in G$, $\sigma(g)$ is an endomorphism of that space. Namely, that indeed $\tau(g) \circ T \circ \rho(g^{-1})$ is a linear map from $V$ to $W$, and that
$$T \mapsto \tau(g) \circ T \circ \rho(g^{-1}),$$
is linear in $T$. This just establishes that $\sigma(g)$ is a linear map of the vector space $\mathrm{Hom}(V, W)$.
- Next, one needs to verify that $\sigma(gh) = \sigma(g) \circ \sigma(h)$. This shows that we have a multiplicative map $G \to \mathrm{End}(\mathrm{Hom}(V, W))$. But note that since every element in $G$ is invertible and $\sigma(1)$ is the identity map, automatically $\sigma(g)$ is invertible, because $\sigma(g) \circ \sigma(g^{-1}) = \sigma(1) = Id$, etc. Thus, it follows that we get a homomorphism
$$\sigma : G \to \mathrm{Aut}(\mathrm{Hom}(V, W)).$$

Let $(\sigma, U)$ be a representation of $G$ and let

$$U^G := \{u \in U : \sigma(g)(u) = u, \forall g \in G\}.$$

This is the space of invariant vectors. Note that $U^G$ is a sub-representation of $U$ on which $G$ acts trivially. The homomorphism

$$G \to \mathrm{Aut}(U^G),$$

induced from $\sigma$ is simply $g \mapsto Id, \forall g \in G$.

Applying this to to $U = \mathrm{Hom}(V, W)$ and $\sigma$ as given above, we make the following observation:

$$\mathrm{Hom}_G(V, W) = \mathrm{Hom}(V, W)^G.$$

*Remark* 30.2.1. We also remark that the construction $\mathrm{Hom}(V, W)$, besides its theoretical useful that we shall see repeatedly below, is a very good way to construct representations. For example, if $W$ is a representation and $V$ is a one dimensional representation then $\mathrm{Hom}(V, W)$ is another representation of the same dimension as $W$. In fact, if $W$ is irreducible, it will be the case that $\mathrm{Hom}(V, W)$ is irreducible too, but that requires a proof; it would be much easier to give once we have the main theorems available. It may be the case that $\mathrm{Hom}(V, W) \cong W$ as representations, but often this is not the case, and so once we have constructed an irreducible representation $W$ we are often able to construct more as $\mathrm{Hom}(V, W)$ for various one dimensional representations $V$.

**Lemma 30.2.2.** *Let $(\rho, V)$ be an irreducible representation then either $V^G = \{0\}$ or $V = V^G$ and is then a one-dimensional space on which G acts trivially.*

*Proof.* As $V^G$ is a sub-representation and $V$ is irreducible, either $V^G = \{0\}$ or $V^G = V$. In the latter case, let $v \in V$ be a non-zero vector. Then $\mathrm{Span}_{\mathbb{C}}(v)$ is a sub-representation and consequently $V = \mathrm{Span}_{\mathbb{C}}(v)$, hence a one-dimensional subspace. □

### 30.3. **Examples of represenations.**

30.3.1. *Passing to coordinates.* Let

$$\rho : G \to \mathrm{GL}_n(\mathbb{C})$$

be a homomorphism of groups. Then $(\rho, \mathbb{C}^n)$ is a representation as we have a canonical identification

$$\mathrm{GL}_n(\mathbb{C}) = \mathrm{Aut}(\mathbb{C}^n),$$

by sending every linear map $T$ to the matrix $[T]_{St}$ representing it in the standard basis.

More generally, let $V$ be an $n$-dimensional vector space and $(\rho, V)$ a representation of $G$. Let $B$ be a basis for $V$. We get then

$$T\colon (\rho, V) \cong (\tau, \mathbb{C}^n),$$

where $T\colon V \to \mathbb{C}^n$ is the map sending $v$ to $[v]_B$ and

$$\tau(g) = [\rho(g)]_B.$$

The identity $T \circ \rho(g) = \tau(g) \circ T$, namely, for all $v \in V$, $T \circ \rho(g)(v) = \tau(g) \circ T(v)$ translates in this case to the identity $[\rho(g)(v)]_B = [\rho(g)]_B[v]_B$, which is precisely the property defining the matrix $[\rho(g)]_B$.

Thus, in some sense, all linear representations can be viewed as group homomorphisms $G \to \mathrm{GL}_n(\mathbb{C})$. However, this perspective is not canonical. If we choose another basis $C$ we get a different represenation

$$\tau'\colon G \to \mathrm{GL}_n(\mathbb{C}), \quad \tau'(g) = [\rho(g)]_C.$$

The two representations are isomorphic

$$(\tau, \mathbb{C}^n) \cong (\tau', \mathbb{C}^n)$$

via the change of basis matrix ${}_CM_B$ that may be viewed as an isomorphism

$$ {}_CM_B : \mathbb{C}^n \to \mathbb{C}^n; $$

Indeed, we have

$$ \tau'(g)\ {}_CM_B = {}_CM_B\ \tau(g). $$

30.3.2. *The standard representation of $S_n$.* We define the **standard representation** $\rho^{st}$ of $S_n$ by associating to $\sigma \in S_n$ the linear transformation given on the standard basis by

$$ e_i \mapsto e_{\sigma(i)}. $$

In matrices

$$ \sigma \mapsto M_\sigma, $$

where $M_\sigma$ is the matrix whose $(\sigma(j), j)$ entry is 1 (for any $j$), and all the other entries are zero. To illustrate, for $n = 3$, we have the following matrices

$$ M_1 = \begin{pmatrix} 1&0&0\\0&1&0\\0&0&1 \end{pmatrix}, M_{(12)} = \begin{pmatrix} 0&1&0\\1&0&0\\0&0&1 \end{pmatrix}, M_{(123)} = \begin{pmatrix} 0&0&1\\1&0&0\\0&1&0 \end{pmatrix}. $$

The standard representation has two sub-representations

$$ U_1 = \mathrm{Span}_{\mathbb{C}}\{(1,1,\dots,1)\}, \qquad U_0 = \{(x_1,\dots,x_n) : x_1 + \cdots + x_n = 0\}. $$

In fact, let $\rho^{st}$ denote the standard representation, $\rho^{st}|_{U_1}$ and $\rho^{st}|_{U_0}$ the sub-representations, then

$$ \rho^{st} \cong \rho^{st}|_{U_1} \oplus \rho^{st}|_{U_0}. $$

We also denote the representation $\rho^{st}|_{U_0}$ by $\rho^{st,0}$.

**Proposition 30.3.1.** *Assume that $n \geq 2$. $U_0$ is an irreducible $n-1$ dimensional representation of $S_n$.*

*Proof.* We assume that $n \geq 2$. The case $n = 2$ is easy as $U_0$ is 1-dimensional.

Let $U' \subseteq U_0$ be a non-zero sub-representation. Let $x = (x_1, \dots, x_n)$ be a non-zero vector in $U'$. If $x$ has precisely two zero elements, by multiplying $x$ by a scalar we may assume that $x = (0, \dots, 0, 1, 0 \dots, 0, -1, 0, \dots, 0)$. Then, by acting by $S_n$ we see that every vector of the form $e_i - e_j$ (where $e_i$ are the standard basis) is also in $U'$. But these vectors span $U_0$ and it follows that $U' = U_0$.

Thus, it remains to prove that $U'$ always contains such a vector. Let $x \in U'$ be a non-zero vector. If $x$ has more than 2 non-zero coordinates, we show that there is vector $y \in U'$ that is not zero and has fewer non-zero coordinates. This suffices to reduce to the case considered above.

Assume therefore that $x$ has at least 3 non-zero coordinates. First, by rescaling we may assume that one of these coordinates is 1. Then, as $\sum x_i = 0$, there exists a non-zero coordinate that is not equal to 1. By applying a permutation to $x$ we may assume that

$$ x = (1, x_2, x_3, \dots, x_n), $$

where $x_2 \neq 1$ and is non-zero and also $x_3 \neq 0$. In this case, also the vector

$$ x' = \frac{1}{x_2}(x_2, 1, x_3, \dots, x_n), $$

belongs to $U_1$. Therefore, also

$$ y = x - x' = (0, x_2 - \frac{1}{x_2}, x_3(1 - \frac{1}{x_2}), \dots, x_n(1 - \frac{1}{x_2})), $$

belongs to $U'$ and this vector has fewer non-zero coordinates, yet is not zero (consider its third coordinate). $\square$

30.3.3. *The regular representation.* This is one of the key examples, in fact. Let $G$ be a group of order $n$. Then $G$ acts by left multiplication on itself giving us an embedding

$$G \hookrightarrow \Sigma_G \cong S_n.$$

(This, in a nutshell, is the proof of Cayley's theorem!) We have constructed above the standard representation $\rho^{st}$ of $S_n$. Thus, by composition, we get a representation that we denote $\rho^{reg}$,

$$\rho^{reg}\colon G \to \mathrm{GL}_n(\mathbb{C}).$$

It is called the **regular representation** of $G$.

There is a slightly more canonical way to describe this representation. Let us consider a vector space with a basis given by vectors indexed by elements of $G$. Thus,

$$\{v_g : g \in G\}$$

is a basis to this vector space and its general element is written as $\sum_{g\in G} a_g \cdot g$, where $a_g \in \mathbb{C}$. Addition and multiplication by scalar are done in the expected way:

$$\sum_{g\in G} a_g \cdot g + \sum_{g\in G} b_g \cdot g = \sum_{g\in G} (a_g + b_g) \cdot g,$$

and

$$\alpha \sum_{g\in G} a_g \cdot g = \sum_{g\in G} \alpha a_g \cdot g.$$

We may use the notation $V = \oplus_{g\in G}\mathbb{C} \cdot v_g$ or $V = \mathbb{C}[G]$. The representation $\rho^{reg}$ takes an element $h \in G$ to the linear map (denoted $\rho^{reg}(h)$) of $V$ that has the following effect on basis vectors:

$$v_g \mapsto v_{hg}, \quad \forall g \in G.$$

Or, in a different notation,

$$\rho^{reg}(h)(\sum_{g\in G} a_g \cdot g) = \sum_{g\in G} a_g \cdot hg.$$

30.3.4. *One dimensional representations.* The one dimensional representations of a group $G$ are, up to isomorphism, homomorphisms

$$G \to \mathbb{C}^\times.$$

Let

$$G^* = \{\rho | \rho\colon G \to \mathbb{C}^\times \text{ homomorphism}\}.$$

Then $G^*$ is an abelian group, called the **character group** of $G$, where the group operation is

$$(\rho \cdot \tau)(g) = \rho(g) \cdot \tau(g).$$

The identity is the trivial homomorphism $\rho_1$ giving us the **trivial representation** $(\rho_1, \mathbb{C})$, namely, $\rho_1 : G \to \mathbb{C}^\times, \rho_1(g) = 1$ for all $g \in G$. Note that if $G$ is a finite group, any such $\rho$ takes elements of $G$ to elements of $\mathbb{C}^\times$ that have finite order. Thus, in this case, also

$$G^* = \{\rho | \rho\colon G \to \mathbb{S}^1 \text{ homomorphism}\},$$

where $\mathbb{S}^1$ is the unit circle

$$\mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\}.$$

The following are not too difficult to check (see also Exercise 86):

- $(H \times G)^* \cong H^* \times G^*$.
- $(\mathbb{Z}/n\mathbb{Z})^* \cong \mathbb{Z}/n\mathbb{Z}$.
- Therefore, combining the two facts provided above, if $G$ is a finite abelian group $G^* \cong G$.
- For a general group $G$, we have $G^* = (G/G')^*$, where $G'$ is the commutator subgroup.
- In particular, for a general group $G$, $G^*$ may be very small compared to $G$. For example, for $n \geq 5$ we have $A_n^* = \{1\}$.

Given elements $\alpha_1, \dots, \alpha_n$ of $G^*$ (any elements, repetitions allowed), we get an $n$-dimensional representation of $G$

$$g \mapsto \begin{pmatrix} \alpha_1(g) & & & \\ & \alpha_2(g) & & \\ & & \ddots & \\ & & & \alpha_n(g) \end{pmatrix}.$$

We leave it as an exercise to show that if $G$ is an abelian group, any $n$-dimensional representation of $G$ is isomorphic to a representation as constructed above for a suitable choice of $\alpha_1, \dots, \alpha_n$. (You would need the theorem about simultaneous diagonalization of commuting diagonalizable matrices).

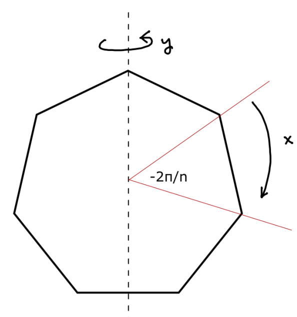
Thus, in a sense, we know all the representations of finite abelian groups. Any irreducible representation is 1-dimensional, given by an element of $\alpha \in G^*$. Any representation is a sum of 1-dimensional representations.

30.3.5. *A representation of $D_n$ and $A_4$.* Let $n \geq 3$ and consider the dihedral group $D_n$ generated by $x, y$. The symmetries of a regular $n$-gon in the plane, provided by elements of $D_n$, are naturally linear transformations of $\mathbb{R}^2$ and we can associate to $x, y$, the following matrices

$$x \mapsto \begin{pmatrix} \cos(2\pi/n) & \sin(2\pi/n) \\ -\sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}, \quad y \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

We view these as complex matrices thereby obtaining a homomorphism

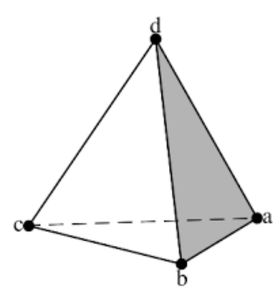
$$\rho^{plane} : D_n \to \mathrm{GL}_2(\mathbb{C}).$$




Another geometric example is the representation of $A_4$ coming from its action on a regular tetrahedron. We view $A_4$ as permuting the letters $a, b, c, d$, thereby acting by symmetries on the tetrahedron. This action comes from a linear representation

$$A_4 \to \mathrm{GL}_3(\mathbb{R}) \subseteq \mathrm{GL}_3(\mathbb{C}).$$

Although this representation certainly looks irreducible, and it is, one has to be careful. Also the action of $\mathbb{Z}/4\mathbb{Z}$ on $\mathbb{R}^2$, where $a \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^a$ looks irreducible (and indeed, it cannot be decomposed as a *real* representation). But, viewed as a representation




$$\mathbb{Z}/4\mathbb{Z} \to \mathrm{GL}_2(\mathbb{C}),$$

it is reducible. Every representation of dimension greater than 1 of an abelian group is reducible!

30.4. **The character of a representation.** We now arrive a key concept: a character. In fact, the whole theory of representations of finite groups relies on it.

Let $(\rho, V)$ be a representation of $G$. Define the **character** of $\rho$, $\chi_\rho$, by

$$\chi_\rho : G \to \mathbb{C}, \quad \chi_\rho(g) = \mathrm{Tr}(\rho(g)).$$

Here Tr denotes the trace of a square matrix, $\mathrm{Tr}(m_{ij}) = \sum m_{ii}$.

**Lemma 30.4.1.** *The function $\chi_\rho$ is well defined and depends on $\rho$ only up to isomorphism. Furthermore, $\chi_\rho$ is a* **class function** *on $G$. That is, for all $g, h \in G$, we have*

$$\chi_\rho(g) = \chi_\rho(hgh^{-1}).$$

*In addition,*

$$\chi_{\rho\oplus\tau} = \chi_\rho + \chi_\tau, \qquad \chi_\rho(1) = \dim(\rho), \qquad \chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}.$$

*(By $\dim(\rho)$ we mean the dimension of $V$ where $\rho : G \to \mathrm{Aut}(V)$.)*

*Proof.* By "well-defined" we mean the following: we have defined the trace of a linear transformation $T$ as the trace of a matrix representing it in a given basis $B$. That is $\mathrm{Tr}(T) := \mathrm{Tr}([T]_B)$. But, we also proved in linear algebra that the value obtained this way was independent of the choice of basis. We concluded that from the fact, proven there, that for any two square matrices of the same size $M_1, M_2$, one has $\mathrm{Tr}(M_1M_2) = \mathrm{Tr}(M_2M_1)$, from which one deduces that $\mathrm{Tr}(M_2^{-1}M_1M_2) = \mathrm{Tr}(M_1)$. Applying this to $M_1 = [T]_B$ and $M_2 = {}_BM_C$, where $C$ is a another basis we find that

$$\mathrm{Tr}([T]_B) = \mathrm{Tr}(M_2^{-1}[T]_BM_2) = \mathrm{Tr}([T]_C).$$

Therefore $\chi_\rho$ is well-defined.

If $\rho \cong \tau$, then by choosing bases we may assume that

$$\rho : G \to \mathrm{GL}_n(\mathbb{C}), \quad \tau : G \to \mathrm{GL}_n(\mathbb{C}).$$

As invertible linear transformations $\mathbb{C}^n \to \mathbb{C}^n$ are represented by invertible matrices, the information that $\rho \cong \tau$ translates into the statement that there is an invertible matrix $M \in \mathrm{GL}_n(\mathbb{C})$ such that for all $g \in G$

$$M\rho(g)M^{-1} = \tau(g).$$

But then,

$$\chi_\rho(g) = \mathrm{Tr}(\rho(g)) = \mathrm{Tr}(M\rho(g)M^{-1}) = \mathrm{Tr}(\tau(g)) = \chi_\tau(g).$$

Actually, the same computation gives

$$\chi_\rho(hgh^{-1}) = \mathrm{Tr}(\rho(hgh^{-1})) = \mathrm{Tr}(\rho(h)\rho(g)\rho(h)^{-1}) = \mathrm{Tr}(\rho(g)) = \chi_\rho(g).$$

Therefore, $\chi_\rho$ is a class function.

If we have two representations $(\rho, V), (\tau, W)$, by choosing bases we may assume that

$$\rho : G \to \mathrm{GL}_m(\mathbb{C}), \quad \tau : G \to \mathrm{GL}_n(\mathbb{C}),$$

and so

$$\rho \oplus \tau : G \to \mathrm{GL}_{m+n}(\mathbb{C}), \quad (\rho \oplus \tau)(g) = \begin{pmatrix} \rho(g) & 0 \\ 0 & \tau(g) \end{pmatrix}.$$

Therefore,

$$\chi_{\rho\oplus\tau}(g) = \mathrm{Tr}\begin{pmatrix} \rho(g) & 0 \\ 0 & \tau(g) \end{pmatrix} = \mathrm{Tr}(\rho(g)) + \mathrm{Tr}(\tau(g)) = \chi_\rho(g) + \chi_\tau(g).$$

Now, $\chi_\rho(1) = \mathrm{Tr}(I_n)$, where $I_n$ is the $n \times n$ identity matrix and $n = \dim(V)$. Thus, $\chi_\rho(1) = \dim(\rho)$.

For the last property stated in the Lemma, fix the element $g$ and let $k$ be its order in the group $G$. Then, $\rho(g)^k = \rho(g^k) = \rho(1) = id$. That means that $\rho(g)$ solves the polynomial $x^k - 1$, which has distinct roots, and so the minimal polynomial of $g$, which divides $x^k - 1$, also has distinct roots and therefore $\rho(g)$ is diagonalizable. And so, we may find a basis $B$ of $V$ in which

$$[\rho(g)]_B = \mathrm{diag}(\alpha_1, \dots, \alpha_n).$$

In addition, as $\rho(g)^k = I_n$, the $\alpha_i$ are roots of unity of order (dividing) $n$.

Note that the basis $B$ is chosen specifically for $g$. There is no reason for $\rho(h)$ to be diagonal in this basis if $h \neq g$. However, because of the homomorphism property, one exception is that

$$\rho(g^{-1}) = \mathrm{diag}(\alpha_1^{-1}, \dots, \alpha_n^{-1}) = \mathrm{diag}(\bar{\alpha}_1, \dots, \bar{\alpha}_n),$$

where the second equality is a consequence of $\alpha_i$ being roots of unity, hence lying on the unit circle in $\mathbb{C}$. Therefore,

$$\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}.$$

□

*Characters are the heart of the whole story. Everything will be determined by characters.*

Here are some interesting examples:

(1) For the standard representation of the symmetric group $S_n$ we have

$$\chi_{\rho^{st}}(\sigma) = \mathrm{Tr}(\rho^{st}(\sigma)) = \text{ the number of fixed points of } \sigma.$$

(2) For the dihedral group $D_n$ we have

$$\chi_{\rho^{plane}}(y) = 0, \qquad \chi_{\rho^{plane}}(x) = 2\cos(2\pi/n).$$

(3) If $(\rho, V)$ is a trivial representation, namely $\rho(g) = Id$ for all $g \in G$, then $\chi_\rho$ is the constant function

$$\chi_\rho \equiv n,$$

where $n = \dim(V)$.

(4) Consider the 1-dimension sign representation of $S_n$ given by

$$\mathrm{sgn} : S_n \to \{\pm 1\} \subset \mathbb{C}^\times.$$

Then $\chi_{\mathrm{sgn}}(\sigma) = +1$ if $\sigma$ is even, and $\chi_{\mathrm{sgn}}(\sigma) = -1$, if $\sigma$ is odd.

(5) If $\alpha \in G^*$ is a 1-dimensional representation then $\chi_\alpha$ is simply $\alpha$.

30.5. **Decomposition into irreducible representations.** We show that every representation decomposes as a sum of irreducible representations. This places the irreducible representations as the fundamental building blocks of representations. Many of the theorems we will study are concerned with classifying the irreducible representations and with understanding how exactly a representation is built from irreducible representations.

**Lemma 30.5.1.** *Let $(\rho, V)$ be a representation of $G$. There is an inner product $\langle \cdot, \cdot \rangle$ on $V$ that is $G$-invariant. That is, for all $v, w \in V$ and $g \in G$ one has*

$$\langle \rho(g)v, \rho(g)w \rangle = \langle v, w \rangle.$$

*Proof.* Let $(v, w)$ be any inner product on $V$. Define

$$\langle v, w \rangle = \frac{1}{|G|} \sum_{g \in G} (\rho(g)v, \rho(g)w).$$

First, this is a $G$-invariant function. If $h \in G$ then

$$\begin{aligned}\langle \rho(h)v, \rho(h)w \rangle &= \frac{1}{|G|} \sum_{g \in G} (\rho(g)\rho(h)v, \rho(g)\rho(h)w) \\ &= \frac{1}{|G|} \sum_{g \in G} (\rho(gh)v, \rho(gh)w) \\ &= \langle v, w \rangle,\end{aligned}$$

because when $h$ is fixed and $g$ varies over $G$ the products $gh$ are all the elements of $G$, each occurring once.

We also have

$$\begin{aligned}\langle \alpha v, w\rangle &= \frac{1}{|G|}\sum_{g\in G}(\rho(g)(\alpha v), \rho(g)w)\\ &= \frac{1}{|G|}\sum_{g\in G}(\alpha\rho(g)v, \rho(g)w)\\ &= \frac{1}{|G|}\sum_{g\in G}\alpha(\rho(g)v, \rho(g)w)\\ &= \alpha\langle v, w\rangle.\end{aligned}$$

And,

$$\begin{aligned}\langle (v+v'), w\rangle &= \frac{1}{|G|}\sum_{g\in G}(\rho(g)(v+v'), \rho(g)w)\\ &= \frac{1}{|G|}\sum_{g\in G}(\rho(g)v+\rho(g)v', \rho(g)w)\\ &= \frac{1}{|G|}\sum_{g\in G}\left[(\rho(g)v, \rho(g)w) + (\rho(g)v', \rho(g)w)\right]\\ &= \langle v, w\rangle + \langle v', w\rangle.\end{aligned}$$

Furthermore,

$$\begin{aligned}\langle w, v\rangle &= \frac{1}{|G|}\sum_{g\in G}(\rho(g)w, \rho(g)v)\\ &= \frac{1}{|G|}\sum_{g\in G}\overline{(\rho(g)v, \rho(g)w)}\\ &= \overline{\langle v, w\rangle}.\end{aligned}$$

Finally, for $v \neq 0$

$$\langle v, v\rangle = \frac{1}{|G|}\sum_{g\in G}(\rho(g)v, \rho(g)v),$$

and each of the summands on the right hand side are positive. Therefore,

$$\langle v, v\rangle > 0.$$

□

**Theorem 30.5.2.** *Any representation $(\rho, V)$ of G is a direct sum of irreducible representations.*

*Proof.* We prove that by induction on $\dim(V)$. Whenever $\dim(V) = 1$, $V$ is irreducible. Whenever $V$ is irreducible (of any dimension) the statement is clear.

Let $V$ be any representation and suppose that $V$ is reducible. Let $U$ be a non-zero sub-representation and let $\langle\cdot,\cdot\rangle$ be a $G$-invariant inner product. Then,

$$U^\perp = \{v \in V : \langle u, v\rangle = 0, \forall u \in U\}$$

is a sub vector space and

$$V = U \oplus U^\perp.$$

It remains to check that $U^\perp$ is a sub representation as well. Let $g \in G$ and $w \in U^\perp$. Then, for all $u \in U$,

$$\langle u, \rho(g)(w)\rangle = \langle \rho(g)^{-1}(u), w\rangle = 0,$$

because $\rho(g)^{-1}(u) \in U$ as well. This proves that $\rho(g)(w) \in U^{\perp}$. Therefore, for all $g \in G$, $\rho(g)(U^{\perp}) \subseteq U^{\perp}$. That is, $U^{\perp}$ is a sub representation.

Using induction for $U$ and $U^{\perp}$, we can decompose them into a sum of irreducible representations. And so $V$ itself is a sum of irreducible representations. □

## 31. The main theorems

In this chapter we list the main theorems concerning representations of finite groups so as to give a compact overview of what we aim to achieve in the following chapters.

31.1. **Unique decomposition.** To simplify notation we use the following device. Let $(\rho_i, V_i), i = 1, ..., t$ be representations of $G$ and $a_i$ positive integers. Then, by

$$\rho_1^{a_1} \oplus \cdots \oplus \rho_t^{a_t}, \quad \text{or} \quad V_1^{a_1} \oplus \cdots \oplus V_t^{a_t},$$

we mean the representation of $G$,

$$(\rho_1, V_1) \oplus \cdots \oplus (\rho_1, V_1) \oplus \cdots \oplus (\rho_t, V_t) \oplus \cdots \oplus (\rho_t, V_t),$$

where the summand $(\rho_1, V_1)$ appears $a_1$ times, the summand $(\rho_2, V_2)$ appears $a_2$ times and so on.

**Theorem 31.1.1** (Theorem A)**.** *Let $(\rho, V)$ be a representation of $G$. Then, there are non-isomorphic irreducible representations $\rho_1, \dots, \rho_t$ and positive integers $a_i$ such that*

$$\rho \cong \rho_1^{a_1} \oplus \cdots \oplus \rho_t^{a_t}.$$

*Moreover, up to isomorphism, the representations $\rho_i$ are uniquely determined by $\rho$ and the $a_i$ are uniquely determined as well.*

31.2. **Class functions and an inner product structure.** Let $G$ be a group. Recall that a class function on $G$ is a function $f\colon G \to \mathbb{C}$ that is constant on conjugacy classes. That is,

$$f(x) = f(gxg^{-1}), \quad \forall x, g \in G.$$

One calls the number of conjugacy classes of $G$ the **class number** of $G$. Let us denote it by $h = h(G)$. The class functions form a vector space of dimension $h$ that we shall denote $Class(G)$. As we have seen, for every representation $\rho$ its character $\chi_\rho$ is a class function.

We define now a structure of inner product on $Class(G)$ by

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \phi(g) \overline{\psi(g)}.$$

For example, the constant function 1, that is also the character of the trivial one-dimensional representation of $G$, is a class function and its norm $\|1\| = 1$ (which explains the choice of normalization).

### 31.3. **Orthogonality relations.**

**Theorem 31.3.1** (Theorem B)**.** *Let $\rho, \tau$ be irreducible representations of $G$. Then*

$$\langle \chi_\rho, \chi_\tau \rangle = \begin{cases} 1, & \text{if } \rho \cong \tau \\ 0, & \text{if } \rho \ncong \tau \end{cases}.$$

**Theorem 31.3.2** (Theorem C)**.** *The characters of irreducible representations of $G$, taken up to isomorphism, form an orthonormal basis for $Class(G)$. In particular, there are precisely $h = h(G)$ irreducible representations up to isomorphism. Let $\rho_1, \dots, \rho_h$ be representatives for the irreducible representations and $\chi_1, \dots, \chi_h$ their characters. Let $\rho$ be any representation. Then*

$$\rho \cong \rho_1^{a_1} \oplus \cdots \oplus \rho_h^{a_h},$$

*where*

$$a_i = \langle \chi_\rho, \chi_{\rho_i} \rangle.$$

**Corollary 31.3.3.** *A representation $\rho$ is irreducible if and only if $\|\chi_\rho\|^2 = 1$.*

*Proof.* Write $\chi_\rho = \sum a_i \chi_i$ as a sum of characters of irreducible representations. Note that the $a_i$ are non-negative integers. Then, by orthonormality, $\|\chi_\rho\|^2 = \sum a_i^2$ and the statement follows. □

**Corollary 31.3.4.** *The dimension of $V^G$, namely, the multiplicity of the trivial 1-dimensional representation in $(\rho, V)$ is $\langle \chi_1, \chi_\rho \rangle$, where $\chi_1$ is the character of the trivial representation. It is given by*

$$\dim(V^G) = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g). \tag{4}$$

*Proof.* We have $\chi_\rho = \sum a_i \chi_{\rho_i}$ and let us agree that, at the expense of putting $a_1 = 0$ if needed, our notation is such that $\rho_1$ is indeed the trivial representation. Using orthogonality of characters: $a_1 = \langle \chi_1, \chi_\rho \rangle$. On the other hand, $\langle \chi_1, \chi_\rho \rangle$ is precisely the right hand side of Equation (4).

Note that if $V = \oplus V_i^{a_i}$ then $V^G = \oplus ((V_i)^G)^{a_i}$ as taking invariants commutes with direct sum of representations. But, as $V_i$ is irreducible and not trivial, by Lemma 30.2.2, $V_i^G = \{0\}$ for $i > 1$ and so $V^G = V_1^{a_1}$. □

**Corollary 31.3.5.** *The regular representation $\rho^{reg}$ of $G$ decomposes as*

$$\rho^{reg} = \oplus_{i=1}^h \rho_i^{\dim(\rho_i)}.$$

*Proof.* Write $\chi^{reg} = \chi_{\rho^{reg}} = \sum a_i \chi_{\rho_i}$ where $\chi_{\rho_i}$ are the characters of the irreducible representations of $G$ and $a_i \geq 0$. Then

$$a_i = \langle \chi_{\rho_i}, \chi_{\rho^{reg}} \rangle,$$

by orthogonality of characters. On the other hand, :

$$\langle \chi_{\rho_i}, \chi_{\rho^{reg}} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{\rho_i}(g) \overline{\chi_{\rho^{reg}}(g)} = \frac{1}{|G|} \chi_{\rho_i}(1) \chi_{\rho^{reg}}(1) = \chi_{\rho_i}(1) = \dim(\rho_i).$$

□

**Example 31.3.6.** Consider the standard representation $\rho$ of $S_n$ for $n \geq 2$. We saw that it decomposes as a direct sum $U_1 \oplus U_0$, where $U_1$ is the trivial one dimensional representation, and we proved that $U_0$ is an irreducible representation. Here we offer another proof based on character calculus.

Let $\chi$ be the character of $\rho$, $\chi_1$ the character of $\rho_1$ and $\chi_0$ of $U_0$. Then

$$\chi = \chi_0 + \chi_1.$$

**Claim:** $\|\chi\|^2 = 2$.

*Proof.* Let $T = \{1, \dots, n\}$. Let $S_n$ act on $T \times T$ diagonally,

$$\sigma(a, b) = (\sigma(a), \sigma(b)).$$

It is easy to see that there two orbits for this action: the orbit of $(1, 1)$ and the orbit of $(1, 2)$. Thus, by CFF,

$$\frac{1}{|S_n|} \sum_{\sigma \in S_n} I(\sigma) = 2.$$

Note that $I(\sigma)$ is equal to the square of the number of fixed points of $\sigma$ in its action on $T$ because the fixed points of $\sigma$ in its action on $T \times T$ are of the form $(a, b)$ where both $a$ and $b$ are fixed points of $\sigma$ in its action on $T$.

On the other hand, $\chi(\sigma)$ is the number of fixed points of $\sigma$ in $T$. We find

$$\begin{aligned} \|\chi\|^2 &= \frac{1}{|S_n|} \sum_{\sigma \in S_n} \chi(\sigma)\bar{\chi}(\sigma) \\ &= \frac{1}{|S_n|} \sum_{\sigma \in S_n} \chi(\sigma)^2 \\ &= \frac{1}{|S_n|} \sum_{\sigma \in S_n} I(\sigma) \\ &= 2 \end{aligned}$$

□

Now,

$$\|\chi\| = \|\chi_1\|^2 + 2\langle \chi_1, \chi_0 \rangle + \|\chi_0\|^2.$$

As $\chi_1$ is an irreducible representation, $\|\chi_1\|^2 = 1$ (and it is easy to do the calculation by hand, too). $\langle \chi_1, \chi_0 \rangle$ is equal to the multiplicity of $\chi_1$ in $\chi_0$. But, there is no non-zero fixed vector in $U_0$, because if $x = (x_1, \dots, x_n)$ is a fixed vector, all its coordinates are equal, but $\sum_i x_i = 0$ and we get that $x = 0$.

If follows that $\|\chi_0\|^2 = 1$ and so that $U_0$ is an irreducible representation.

## 31.4. **The number and dimension of irreducible representations.**

**Theorem 31.4.1** (Theorem D)**.** *Let $\rho_1, \dots, \rho_h$ be representatives for the irreducible representations and let $\chi_1, \dots, \chi_h$ be their characters. Then $h = h(G)$ is the number of conjugacy classes of $G$ and we have the formula*

$$|G| = \sum_{i=1}^{h} \dim(\rho_i)^2.$$

*Proof.* This is a direct consequence of Theorem 31.3.2 and Corollay 31.3.5. □

As we shall see in several examples, this formula is very useful for finding the irreducible representations of a group $G$, especially when one already knows some of the representations (for example, the 1-dimensional representations are easy to find as their number is $|G/G'|$). Another numerical fact that is very useful, but whose proof lies beyond the techniques available for us in this course, is the following.

**Fact.** *Let $\rho$ be an irreducible representation of a group $G$ then*

$$\dim(\rho) | \sharp\, G.$$

## 32. Representations of groups of small order

After the overview of the main results we are going to prove about representations of groups, we wish to give some examples so as to make the theory more tangible.

32.1. **The case where $G$ is abelian.** If $G$ is an abelian group of order $n$ then $n = h(G)$. As we have precisely $n$ irreducible representations, the formula

$$|G| = \sum_{i=1}^{h} \dim(\rho_i)^2$$

shows that each irreducible representation is one-dimensional.

We remark that we actually knew that already. Using simultaneous diagonalization of commuting diagonalizable operators, one knows that every representation of an abelian group is a direct sum of 1-dimensional representations. On the other hand, the 1-dimensional representations are the elements of the group $G^*$ and, as we have asserted before, $G$ and $G^*$ are isomorphic and so, in particular, $G^*$ has $n$ elements as well.

32.2. **Character tables.** In the following we will give the **character tables** of certain groups of small order. The columns will be named by representatives to the distinct conjugacy classes in the group, and the rows will be named by the various characters. The number $[x]$ appearing near a representative for a conjugacy class indicates how many elements are in that conjugacy class (which is handy when one calculates inner products of characters). Note that if $\rho$ is 1-dimensional, $\rho = \chi_\rho$. As the groups $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z})^2$ are abelian, we have the following character tables.

| | 0 [1] | 1 [1] |
|---|---|---|
| $\chi_1$ | 1 | 1 |
| $\chi_2$ | 1 | -1 |

TABLE 2. Character table of $\mathbb{Z}/2\mathbb{Z}$

| | 0 [1] | 1 [1] | 2 [1] |
|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 |
| $\chi_2$ | 1 | $e^{2\pi i/3}$ | $e^{4\pi i/3}$ |
| $\chi_3$ | 1 | $e^{4\pi i/3}$ | $e^{2\pi i/3}$ |

TABLE 3. Character table of $\mathbb{Z}/3\mathbb{Z}$

*Remark* 32.2.1. Note that the rows of character tables should be orthonormal vectors (but be careful when calculating the inner product - every entry $\chi(x)$ must be weighted by the size of the conjugacy class of $x$ that appears as $[y]$ in the heading of the column). It is also true that the columns of the character table are orthogonal – see §35, Equation (91), below.

Another check that could be performed is based on the following. Recall that

$$\chi_{\rho^{reg}} = \sum_{i=1}^{h} \chi_i(e) \cdot \chi_i.$$

| | 0 [1] | (1, 0) [1] | (0, 1) [1] | (1,1) [1] |
|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | -1 | -1 | 1 |
| $\chi_3$ | 1 | -1 | 1 | -1 |
| $\chi_4$ | 1 | 1 | -1 | -1 |

TABLE 4. Character table of $(\mathbb{Z}/2\mathbb{Z})^2$

(We are using here $e$ to denote the identity element so as to avoid confusion when the group is abelian.) That means that if we multiply each row $\chi_i$ in the character table by $\chi_i(e)$ (which is listed in the second column) and then sum up all the rescaled rows, we should get a row vector of the form $(|G|, 0, \dots, 0)$. Sometimes we can turn it around and find a missing character. This is our next example.

32.2.1. *The character table of* $S_3$. Consider the group $S_3$. We have $S_3^{ab} \cong \mathbb{Z}/2\mathbb{Z}$ and so there are precisely two 1-dimensional representations. These are the trivial representations $\chi_1$ and the sign representation $\chi^{\rm sgn}$. Since we have

$$6 = 1^2 + 1^2 + \text{ sum of squares},$$

where each square is at least $2^2$, we conclude that there is a unique additional irreducible representation of $S_3$ and it is two dimensional. From the remark above, we can even figure out its character:

$$2\chi_3 = \chi^{reg} - \chi_1 - \chi_2.$$

We thus find the character table:

| Representation | 1 [1] | (12) [3] | (123) [2] |
|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 |
| $\chi_2$ | 1 | -1 | 1 |
| $\chi_3$ | 2 | 0 | -1 |

TABLE 5. Character table of $S_3$

Luckily, we have a model for this irreducible representation: $S_3 = D_3$ acts on the equilateral triangle in the plane by linear tranformations; this is the representation $\rho^{plane}$ considered previously.

$$y = (23) \leftrightarrow \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad x = (123) \leftrightarrow \begin{pmatrix} \cos(2\pi/3) & \sin(2\pi/3) \\ -\sin(2\pi/3) & \cos(2\pi/3) \end{pmatrix} = \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{pmatrix}.$$

We easily check that the character of $\rho^{plane}$ is $\chi_3$.

We actually have yet another model for this representation arising from the standard representation of $S_3$: this model consists of the vectors in $\mathbb{C}^3$ whose coordinates sum to 0, where $S_3$ acts by permuting the coordinates. A basis for this 2-dimensional space is given by $u = e_1 - e_2, v = e_2 - e_3$. In this basis we have

$$y = (23) \leftrightarrow \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \quad x = (123) \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Call this representation $\rho^{st,0}$.

These two representations, $\rho^{st,0}$ and $\rho^{plane}$, are isomorphic – we see they have the same character – but that is not immediately visible from the matrices. There "ought to be" an invertible matrix $M$ that conjugation by it takes the first representation to the second.

32.2.2. *The character table of $D_4$.* The last example we give in this section is the case of $G = D_4$. The commutator subgroup is given by $\{1, x^2\}$ and $G/G' \cong (\mathbb{Z}/2\mathbb{Z})^2$. We can thus lift every one dimensional representation $\rho_i$ of $(\mathbb{Z}/2\mathbb{Z})^2$ to $D_4$ and get a one dimensional representation

$$\rho_i' : D_4 \to (\mathbb{Z}/2\mathbb{Z})^2 \to \mathbb{C}^\times.$$

This gives us the four 1-dimensional representations of $D_4$. Once more, by using the formula $|G| = \sum_{i=1}^h \dim(\rho_i)^2$, we find that there is a unique additional irreducible representation and it is 2-dimensional. A natural guess is the representation coming from the action on the plane:

$$y = (23) \leftrightarrow \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad x = (1234) \leftrightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(This is the representation we have denoted $\rho^{plane}$ previously.) From this we find the following values for its character:

| | $1$ | $x$ | $x^2$ | $x^3$ | $y$ | $xy$ | $x^2y$ | $x^3y$ |
|---|---|---|---|---|---|---|---|---|
| $\chi^{plane}$ | 2 | 0 | -2 | 0 | 0 | 0 | 0 | 0 |

We calculate that $\|\chi\| = 1$ and therefore this representation is irreducible (even over the complex numbers!). Thus, the character table is:

| | $1$ [1] | $x$ [2] | $x^2$ [1] | $y$ [2] | $xy$ [2] |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | -1 | 1 | -1 | 1 |
| $\chi_3$ | 1 | -1 | 1 | 1 | -1 |
| $\chi_4$ | 1 | 1 | 1 | -1 | -1 |
| $\chi^{plane}$ | 2 | 0 | -2 | 0 | 0 |

TABLE 6. Character table of $D_4$

To illustrate how useful this information is, let us consider $D_4$ as a subgroup of $S_4$ and let

$$\rho : D_4 \to \mathrm{GL}_4(\mathbb{C}),$$

be the restriction of the standard representation of $S_4$ to $D_4$ (where $x = (1234), y = (24), xy = (12)(34)$). Recall that $\chi_{\rho^{std}}(\sigma)$ is the number of fixed points of $\sigma$. Thus, we find that

| | $1$ [1] | $x$ [2] | $x^2$ [1] | $y$ [2] | $xy$ [2] |
|---|---|---|---|---|---|
| $\chi_\rho$ | 4 | 0 | 0 | 2 | 0 |

Therefore, $\langle \chi_\rho, \chi_1 \rangle = \langle \chi_\rho, \chi_3 \rangle = 1$, $\langle \chi_\rho, \chi_2 \rangle = \langle \chi_\rho, \chi_4 \rangle = 0$ and $\langle \chi_\rho, \chi^{plane} \rangle = 1$. Thus, $\rho$ decomposes as

$$\rho = \rho_1 \oplus \rho_3 \oplus \rho^{plane}.$$

Here $\rho_1$ is the trivial representation and $\rho_3$ is the representation where $x^2$ and $y$ act trivially, but $x$ acts as multiplication by $-1$. Consequently, there is a coordinate system on $\mathbb{C}^4$ in which $D_4$ acts as follows

$$x \mapsto \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 0 & 1 \\ & & -1 & 0 \end{pmatrix}, \qquad y \mapsto \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & 0 \\ & & 0 & 1 \end{pmatrix}.$$

Also visible from these calculations is that there is a unique line that is fixed by the action of $D_4$. Indeed, the dimension of the invariants is the multiplicity of the trivial representation which is given by 1.

## 33. Proof of the main theorems

### 33.1. Schur's lemma.

**Lemma 33.1.1.** *Let $(\rho, V), (\tau, W)$ be two irreducible representations of $G$. Then,*

$$\mathrm{Hom}_G(V, W) \cong \begin{cases} \mathbb{C}, & \rho \cong \tau; \\ \{0\}, & \textit{else}. \end{cases}$$

*Proof.* First note that whether $V, W$, are irreducible or not, if $T \in \mathrm{Hom}_G(V, W)$ then both $\mathrm{Ker}(T)$ and $\mathrm{Im}(T)$ are sub-representations of $V$ and $W$, respectively.

In our situation, $\mathrm{Ker}(T)$ is either $\{0\}$ or $V$, so if $T$ is not the zero map then $\mathrm{Ker}(T) = \{0\}$, and so $T$ is injective. Then also $\mathrm{Im}(T)$ is not trivial. Thus, $\mathrm{Im}(T) = W$ and $T$ is therefore an isomorphism.

Fix one such $T$ and use it to identify $V$ with $W$. Then, we need to show that

$$\mathrm{End}_G(V) \cong \mathbb{C}.$$

Let $S \in \mathrm{End}_G(V)$ and let $\lambda$ be an eigenvalue of $S$ and $V_\lambda$ the corresponding (non-zero) eigenspace. Then, $S$ is a subrepresentation: If $g \in G$ and $v \in V_\lambda$ then $S(\rho(g)v) = \rho(g)(Sv) = \rho(g)\lambda v = \lambda \cdot \rho(g)v$; that is, $\rho(g)v \in V_\lambda$. As $V$ is irreducible, we must have$V_\lambda = V$. That is, $S = \lambda \cdot \mathrm{Id}$.

On the other hand, clearly every scalar matrix $\lambda \cdot \mathrm{Id}$ belongs to $\mathrm{End}_G(\rho)$. □

Let now $(\rho, V), (\tau, W)$ be any two representations of $G$ then

$$\mathrm{Hom}(V, W)$$

is a representation of $G$ as well. We wish to calculate its character. This is delicate calculation so we would like to reassure the reader that it is well worth the effort.

Let $\{e_1, \ldots, e_n\}$ be a basis for $V$, $\{e_1^*, \ldots, e_n^*\}$ the dual basis of $V^* = \mathrm{Hom}(V, \mathbb{C})$ and let $\{f_1, \ldots f_m\}$ be a basis for $W$. For a vector $\phi \in V^*$ and $w \in W$ we introduce the notation

$$\phi \otimes w$$

to denote a very particular element of $\mathrm{Hom}(V, W)$.[15] It is the linear transformation that takes

$$e_i \mapsto \phi(e_i) \cdot w.$$

**Lemma 33.1.2.** *The elements $e_i^* \otimes f_j, i = 1, \ldots, n, j = 1, \ldots, m$, are a basis of* $\mathrm{Hom}(V, W)$. *Assume that $\rho(g^{-1}) = (g_{ij})$ and $\tau(g) = (h_{ij})$ then*

$$\sigma(g)(e_i^* \otimes f_j) = \sum_{k,\ell} a_{k\ell}(g) e_k^* \otimes f_\ell,$$

*where*

$$a_{k\ell}(g) = g_{ik} h_{\ell j}.$$

[15] The symbol $\otimes$ is called "tensor". There is indeed a theory of tensor products lurking in the background which is the reason I chose this symbol, but we don't need to know it for this course.

*Proof.* In the bases $\{e_1, \dots, e_n\}$ and $\{f_1, \dots f_m\}$, the linear map $e_k^* \otimes f_\ell$ is the matrix $M = (m_{ij})$ having a unique non-zero entry, which is equal to 1, appearing in the $(\ell, k)$ place. Thus, from the identification $\mathrm{Hom}(V, W) \cong M_{m,n}(\mathbb{C})$ coming from the choice of bases, the independence claim is clear.

We need to figure out where does a vector basis $e_t$ goes under the linear map $\sigma(g)(e_i^* \otimes f_j)$ from $V$ to $W$. By definition,

$$\begin{aligned}\sigma(g)(e_i^* \otimes f_j)(e_t) &= \tau(g)((e_i^* \otimes f_j)(\rho(g^{-1})(e_t)) \\ &= \tau(g)((e_i^* \otimes f_j)(\sum_s g_{st} e_s)) \\ &= \tau(g)(g_{it} f_j) \\ &= \sum_s g_{it} h_{sj} f_s.\end{aligned}$$

On the other hand,

$$(\sum_{k,\ell} a_{k\ell}(g) e_k^* \otimes f_\ell)(e_t) = \sum_\ell a_{t\ell} f_\ell.$$

Whence,

$$a_{ts}(g) = g_{it} h_{sj}.$$

□

33.2. **Uniqueness of decompositions.** By Theorem 30.5.2, every representation $(\rho, V)$ decomposes as a direct sum of irreducible representations. Buy clamping together isomorphic irreducible representations, we may assume that

$$V \cong V_1^{a_1} \oplus \cdots \oplus V_s^{a_s},$$

where $(\rho_i, V_i)$ are irreducible representations that are not isomorphic to each other. Suppose we have another such decomposition. By allowing also exponents $a_i = 0$, we may assume that the other decomposition is also written as

$$V \cong V_1^{b_1} \oplus \cdots \oplus V_s^{b_s},$$

and our theorem is that $a_i = b_i$ for all $i$. To show that we calculate

$$\dim(\mathrm{Hom}_G(V_i, V)).$$

First, note the general fact that

$$\mathrm{Hom}(W, U \oplus V) = \mathrm{Hom}(W, U) \oplus \mathrm{Hom}(W, V),$$

and likewise

$$\mathrm{Hom}_G(W, U \oplus V) = \mathrm{Hom}_G(W, U) \oplus \mathrm{Hom}_G(W, V).$$

Therefore, by using Schur's Lemma, we conclude that

$$\mathrm{Hom}_G(V_i, V) = \oplus_{j=1}^s \mathrm{Hom}_G(V_i, V_j)^{a_i} = \mathrm{Hom}_G(V_i, V_i)^{a_i} = \mathbb{C}^{a_i},$$

and, in particular,

$$\dim(\mathrm{Hom}_G(V_i, V)) = \dim(\mathbb{C}^{a_i}) = a_i.$$

As the left hand side of this last equation "doesn't know" about the decomposition, it follows that $a_i = b_i$. We have proven:

**Theorem 33.2.1** (= Theorem 31.1.1 = Theorem A)**.** *Every representation of $V$ decomposes into a direct sum of irreducible representations. The irreducible representations and the multiplicities to which they appear are determined uniquely (up to isomorphism).*

33.3. **The character of** $\mathrm{Hom}(V, W)$**.**

**Corollary 33.3.1.** *The character $\chi$ of the representation* $\mathrm{Hom}(V, W)$ *is*

$$\chi(g) = \chi_\tau(g) \cdot \overline{\chi_\rho(g)}.$$

*Proof.* The formula we found in Lemma 33.1.2, $a_{ts}(g) = g_{it}h_{sj}$, should really be written as to indicate the dependence on $i$ and $j$ as the scalar $a_{ts}$ describe the action of $\sigma(g)$ on the particular basis element $e_i^* \otimes f_j$. Thus, to indicate this dependence on $i$ and $j$, we could write

$$a_{ts}^{ij}(g) = g_{it}h_{sj}.$$

In this notation,

$$\mathrm{Tr}(\sigma(g)) = \sum_{ij} a_{ij}^{ij}(g) = \sum_{ij} g_{ii}h_{jj} = (\sum_j h_{jj})(\sum_i g_{ii}) = \chi_\tau(g) \cdot \chi_\rho(g^{-1}) = \chi_\tau(g) \cdot \overline{\chi_\rho(g)}.$$

□

33.4. **The projection** $\pi$**.** Let $(\rho, V)$ be a representation of $G$. Let

$$\pi = \frac{1}{|G|} \sum_{g \in G} \rho(g).$$

Then $\pi \in \mathrm{End}_G(V)$ and is a projection onto the subspace $V^G$.

*Proof.* As $\pi$ is a sum of linear maps, it is a linear map itself. If $h \in G$ then

$$\rho(h) \circ \pi = \frac{1}{|G|} \sum_{g \in G} \rho(hg) = (\frac{1}{|G|} \sum_{g \in G} \rho(hgh^{-1}))\rho(h) = \pi \circ \rho(h),$$

because as $g$ ranges over $G$ and $h$ is fixed, also $hgh^{-1}$ ranges over $G$.

The image of $\pi$ is fixed by $G$: let $v \in V$ then

$$\rho(h)(\pi(v)) = (\frac{1}{|G|} \sum_{g \in G} \rho(hg))(v) = (\frac{1}{|G|} \sum_{g \in G} \rho(g))(v) = \pi(v),$$

where we have used that $g$ ranges over $G$ so does $hg$.

Finally, if $v \in V^G$ then $\pi(v) = \frac{1}{|G|} \sum_{g \in G} \rho(g)(v) = \frac{1}{|G|} \sum_{g \in G} v = v$. □

**Corollary 33.4.1.** *Let $(\rho, V)$ be a representation of $G$ and let $\chi_1$ be the character of the trivial one dimensional representation $(\rho_1, \mathbb{C})$ of $G$. Consider the decomposition of $\rho$ into irreducible representations*

$$\rho = \rho_1^{a_1} \oplus \cdots \oplus \rho_t^{a_t},$$

*where the $a_i$ are positive, except $a_1$ which is allowed to be zero and $(\rho_i, V_i)$ are non-isomorphic and irreducible. Then*

$$V^G = V_1^{a_1}$$

*and*

$$a_1 = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) = \langle \chi_\rho, \chi_1 \rangle,$$

*where $\chi_1 = \chi_{\rho_1}$ is the constant function* $1$.

*Proof.* Clearly $V_1^{a_1} \subseteq V^G$. Let $v \in V$ and suppose that $v = (v_1, \dots, v_t)$ with $v_i \in V_i^{a_i}$. Then, as $G$ acts diagonally, $v \in V^G$ if and only if each $v_i \in V^G$. But, any $x \in V^G \cap V_i^{a_i}$ gives a morphism of representations

$$V_1 \to V_i^{a_i}, \qquad \lambda \mapsto \lambda x.$$

However, for $i > 1$ by Schur's lemma,

$$\mathrm{Hom}_G(V_1, V_i^{a_i}) = \mathrm{Hom}_G(V_1, V_i)^{a_i} = \{0\}.$$

Thus, $x = 0$ and $V^G = V_1^{a_1}$.

Now, the projection operator $\pi \in \mathrm{Hom}_G(V, V)$ and in the decomposition above

$$\pi = id_{a_1} \oplus 0 \oplus \cdots \oplus 0.$$

Therefore,

$$\begin{aligned} a_1 = \mathrm{Tr}(\pi) &= \mathrm{Tr}(\frac{1}{|G|}\sum_{g\in G}\rho(g)) \\ &= \frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}(\rho(g)) \\ &= \frac{1}{|G|}\sum_{g\in G}\chi_\rho(g) \\ &= \langle \chi_\rho, \chi_1\rangle. \end{aligned}$$

□

33.5. **Irreducible characters are orthonormal functions.** Let $(\rho, V), (\tau, W)$ be irreducible representations. We apply the considerations of Corollary 33.4.1 to the representation

$$\mathrm{Hom}(V, W).$$

Recall that its invariants are $\mathrm{Hom}(V, W)^G = \mathrm{Hom}_G(V, W)$. On the one hand, by Schur's Lemma, the dimension of $\mathrm{Hom}_G(V, W)$ is 0 if $\rho \ncong \tau$ and 1 if $\rho \cong \tau$. On the other hand, by Corollary 33.3.1 and Corollary 33.4.1,

$$\dim\ \mathrm{Hom}(V, W)^G = \frac{1}{|G|}\sum_{g\in G}\bar{\chi}_\rho(g)\chi_\tau(g) = \langle \chi_\tau, \chi_\rho\rangle.$$

Therefore, we have obtained

**Theorem 33.5.1** (=Theorem 31.3.1 = Theorem B)**.** *Let $\rho, \tau$ be irreducible representations of $G$. Then*

$$\langle \chi_\rho, \chi_\tau\rangle = \begin{cases} 1, & \text{if } \rho \cong \tau \\ 0, & \text{if } \rho \ncong \tau \end{cases}.$$

We arrive the following remarkable result.

**Corollary 33.5.2.** *The characters of irreducible representations of $G$ form an orthonormal set in $Class(G)$. In particular, there are finitely many irreducible representations up to isomorphism, in fact at most* $\dim\ Class(G) = h(G)$.

We shall shortly see that there are precisely that many irreducible representations and so their characters are an orthonormal *basis* of $Class(G)$.

**Corollary 33.5.3.** *The character of a representation determines it up to isomorphism. More precisely, if*

$$\rho \cong \rho_1^{a_1} \oplus \cdots \oplus \rho_t^{a_t}$$

*then the $a_i$ may be found in terms of characters alone:*

$$a_i = \langle \chi_\rho, \chi_{\rho_i}\rangle.$$

*Proof.* Indeed, if $\rho \cong \oplus_i \rho_i^{a_i}$, where the $\rho_i$ are non-isomorphic irreducible representations then $\chi_\rho = \sum a_i \chi_{\rho_i}$ and by orthogonality we can retrieve the $a_i$ by

$$a_i = \langle \chi_\rho, \chi_{\rho_i}\rangle.$$

In addition, as the $\chi_{\rho_i}$ are linearly independent, the expression $\chi_\rho = \sum a_i \chi_i$ is unique. □

**Corollary 33.5.4.** *A representation $\rho$ is irreducible if and only if $\|\chi_\rho\| = 1$.*

*Proof.* This was already proven as Corollary 31.3.3. □

33.6. **Further study of the regular representation.** Recall the regular representation $\rho^{reg}$ of $G$ from § 30.3.3.

**Proposition 33.6.1.** *Any irreducible representation $\rho$ appears in $\rho^{reg}$. In fact, it appears in multiplicity equal to its dimension. In particular, if $\rho_1, \dots, \rho_t$ are the irreducible representations of G then*

$$|G| = \sum_{i=1} \dim(\rho_i)^2.$$

*Proof.* This is essentially 31.3.5; the last statement is obtained by consider the dimensions of the representation spaces on both sides. □

**Lemma 33.6.2.** *Let $\alpha \in Class(G)$. For any representation $(\rho, V)$*

$$\sum_{g\in G} \alpha(g)\cdot\rho(g) \in \mathrm{End}_G(V).$$

*Proof.* As a sum of linear maps, certainly $\sum_{g\in G}\alpha(g)\cdot\rho(g) \in \mathrm{End}(V)$. We only need to check that it commutes with the group action. Now, using that $\rho$ is a homomorphism, for $h \in G$

$$\begin{aligned}\rho(h)\circ(\sum_{g\in G}\alpha(g)\cdot\rho(g)) &= \sum_{g\in G}\alpha(g)\cdot\rho(hgh^{-1})\rho(h)\\ &= (\sum_{g\in G}\alpha(hgh^{-1})\cdot\rho(hgh^{-1}))\rho(h)\\ &= (\sum_{g\in G}\alpha(g)\cdot\rho(g))\circ\rho(h),\end{aligned}$$

because $\alpha(g) = \alpha(hgh^{-1})$ for all $g$ and $h$. □

**Theorem 33.6.3** (= the key part of Theorem 31.3.2 = Theorem C)**.** *The number of irreducible representations of $G$ is $h(G)$ and the characters of the irreducible representations form an orthonormal basis for $Class(G)$.*

*Proof.* We know that the characters of the irreducible representations are an orthonormal set in $Class(G)$. If they are not a basis, there is some function $\beta \in Class(G)$ that is orthogonal to all these characters. Let $\alpha$ be the function $\alpha(g) = \overline{\beta(g)}$; note that also $\alpha \in Class(G)$. We will show that $\alpha \equiv 0$ (namely, $\alpha$ is the zero function), thus $\beta \equiv 0$, and so the characters of irreducible representations are a basis for $Class(G)$. Consequently, their number is the class number of $G$.

Let $(\rho, V)$ be an irreducible representation of $G$ of dimension $d$. We claim that the operator

$$A_\rho : V \to V, \quad A_\rho = \sum_{g\in G}\alpha(g)\cdot\rho(g),$$

is the zero operator.

First, by Schur's lemma $\mathrm{End}_G(V) = \mathbb{C}$, where the isomorphism is given by $T \mapsto \frac{1}{d}\mathrm{Tr}(T)$. Second, $A_\rho \in \mathrm{End}_G((\rho, V))$ by Lemma 33.6.2. Therefore, we can determine whether $A_\rho$ is zero or not by calculating $\frac{1}{d}\mathrm{Tr}(A_\rho)$. Let us calculate:

$$\frac{1}{d}\mathrm{Tr}(A_\rho) = \frac{1}{d}\sum_{g\in G}\alpha(g)\cdot\chi_\rho(g) = \langle\chi_\rho, \beta\rangle = 0.$$

It follows that $A_\rho$ is zero.

Now, this holds for any irreducible representation $(\rho, V)$ and, therefore, for any sum of irreducible representations. In particular, it holds for the regular representation $\mathbb{C}[G]$ of $G$. (Note that for $\rho \oplus \tau$ we have naturally, $A_{\rho\oplus\tau} = A_\rho \oplus A_\tau$, etc. ) The last step in the proof is to realize that the linear operators $\{\rho^{reg}(g) \in \mathrm{Aut}(\mathbb{C}[G]) : g \in G\}$ are linearly independent and thus, $A_{\rho^{reg}} = 0$ implies that $\alpha \equiv 0$.

Suppose a linear dependence between the operators $\{\rho^{reg}(g)\}$; namely, suppose that we have $\sum_g \gamma(g)\rho^{reg}(g) = 0$ for some scalars $\gamma(g) \in \mathbb{C}$. Apply this operator to the vector $v_e \in \mathbb{C}[G]$ (where $e$ is the identity element of $G$). Then

$$\sum_g \gamma(g)\rho^{reg}(g)(v_e) = \sum_g \gamma(g)v_g = 0.$$

As $\{v_g : g \in G\}$ are a basis for $\mathbb{C}[G]$, we conclude that all $\gamma(g) = 0$. □

33.7. **The layout of the proofs.** As we have presented the theory in a non-linear way, first presenting the key theorems and easy consequences and examples of which, and then back paddling to actually provide the proofs, it may be useful to summarize the logical structure again.

(1) **Every representation** $(\rho, V)$ **is a sum of irreducible representations.**
(Key point: there is a $G$-invariant inner product on $V$; proved by "averaging").

(2) **Schur's Lemma: if** $\rho, \tau$ **are irreducible then** $\mathrm{Hom}(\rho, \tau)$ **is zero if** $\rho \ncong \tau$ **and is** $\mathbb{C}$ **otherwise.**
(Essentially an easy argument: we analyzed the kernel and the image of a map $T$ using irreducibility and when $\rho = \tau$ the kernel of $T - \lambda \cdot I$.)

(3) Key calculation: **the character of** $\mathrm{Hom}(\rho, \tau)$ **is** $\bar{\chi}_\rho \cdot \chi_\tau$**.**
(Just a careful complicated calculation).

(4) Introduced **the projection operator** $\pi : (\rho, V) \to V^G$ and concluded **concluded that** $\dim(V^G) = \frac{1}{|G|}\sum_{g\in G}\chi_\rho(g)$**.**
(The main point was after showing $\pi$ is a projection, to understand its effect in terms of the decomposition into irreducible representations.)

(5) **If** $\rho, \tau$ **are irreducible then** $\langle \chi_\rho, \chi_\tau\rangle = 1$ **if** $\rho \cong \tau$ **and** $0$ **otherwise.** (We combined Schur's Lemma and the fact that $\mathrm{Hom}(V, W)^G = \mathrm{Hom}_G(V, W)$ to find a formula for $\dim(Hom_G(V, W))$; This is a key result, from which many theorems and corollaries follow.)

(6) **Uniqueness of decomposition** follows immediately. That $\rho$ **is irreducible if and only if** $\|\chi_\rho\| = 1$ followed immediately. The formula for the **multiplicities** $a_i = \langle \chi_\rho, \chi_i\rangle$ followed immediately. That **a representation is determined by its character** followed immediately. The **decomposition of the regular representation** followed easily and in particular that **if** $\rho_1, \dots, \rho_t$ **are the irreducible representations of** $G$ **then** $|G| = \sum_{i=1}^t \dim(\rho_i)^2$.

(7) The last step was to established that the characters of irreducible representations are an orthonormal basis for $Class(G)$ and to conclude therefore that **the number of irreducible representations of** $G$ **is its class number** (so $t$ is really $h(G)$). We did that by associating to a class function $\alpha$ a linear operator $A_\rho$ on every representation $\rho$ and analyzed the effect of such operator, for a suitably chosen $\alpha$ on the regular representation.

## 34. Further examples and applications

34.1. **Representations of** $S_4$**.** To begin with, the number of conjugacy classes of $S_4$ is $p(4) = 5$. Thus, there are 5 irreducible representations. As the commutator of $S_4$ is $A_4$, $S_4^{ab} \cong \mathbb{Z}/2\mathbb{Z}$ and thus has precisely two 1-dimensional representations that must be the trivial one $\chi_1$ and the sign representation $\chi^{\rm sgn}$. We also know the 3-dimensional irreducible sub representation $\rho^{st,0}$ of the standard representation.

As we have

$$24 = 1^2 + 1^2 + 3^2 + x^2 + y^2,$$

we conclude that $S_4$ has a 2-dimensional irreducible representation $\rho$ and an additional 3 dimensional representation $\tau$ and this list ($\chi_1$, $\chi^{\rm sgn}$, $\rho^{st,0}$, $\rho$, $\tau$) is the full list of irreducible representations of $S_4$.

Recall the surjective homomorphism with kernel $K$

$$S_4 \to S_3,$$

by means of which we can pull-back the irreducible 2-dimensional representation of $S_3$. We get a representation $\rho$ whose character $\chi$ is

| | 1 [1] | (12) [6] | (123) [8] | (1234) [6] | (12)(34) [3] |
|---|---|---|---|---|---|
| $\chi$ | 2 | 0 | -1 | 0 | 2 |

Being a pull-back of an irreducible representation, it is of course irreducible, but one can also check that $\|\chi\|^2 = 1$.

Now consider the representation $\mathrm{Hom}(\rho^{\rm sgn}, \rho^{st,0})$. Its character, by Corollary 33.3.1, is $\chi^{st,0} \cdot \bar{\chi}^{\rm sgn} = \chi^{st,0} \cdot \chi_{\rm sgn}$ and thus is given by

| | 1 [1] | (12) [6] | (123) [8] | (1234) [6] | (12)(34) [3] |
|---|---|---|---|---|---|
| $\chi^{st,0}$ | 3 | 1 | 0 | -1 | -1 |
| $\chi^{st,0} \cdot \chi_{\rm sgn}$ | 3 | -1 | 0 | 1 | -1 |

One calculates that $\|\chi^{st,0} \cdot \chi_{\rm sgn}\|^2 = 1$ and so $\chi^{st,0} \cdot \chi_{\rm sgn}$ is the character of the missing irreducible representation $\tau$. We conclude that the character table of $S_4$ is the following:

| | 1 [1] | (12) [6] | (123) [8] | (1234) [6] | (12)(34) [3] |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi^{sgn}$ | 1 | -1 | 1 | -1 | 1 |
| $\chi$ | 2 | 0 | -1 | 0 | 2 |
| $\chi^{st,0}$ | 3 | 1 | 0 | -1 | -1 |
| $\chi_\tau$ | 3 | -1 | 0 | 1 | -1 |

TABLE 7. The character table of $S_4$.

34.2. **Representations of $A_4$.** The commutator of $A_4$ is the Klein group $V$. As $A_4/V$ is a group of order 3, $A_4$ has three 1-dimensional representations. Denote them $\chi_1, \chi_2, \chi_3$. On the other hand, it has 4 conjugacy classes that are represented by $1, (12)(34), (123), (132)$. We conclude from $12 = 1^2 + 1^2 + 1^2 + x^2$ that $A_4$ has precisely one more irreducible representation $\rho$ and it is 3 dimensional. One natural guess is that this representation is obtained from the action of $A_4$ on a tetrahedron, but here we proceed differently. We have

$$A_4 \to S_4 \to \mathrm{GL}_3(\mathbb{C}),$$

by means of $\rho^{st,0}$. We can easily calculate $\chi_\rho$:

| | 1 [1] | (12)(34) [3] | (123) [4] | (132) [4] |
|---|---|---|---|---|
| $\chi$ | 3 | -1 | 0 | 0 |

As $\|\chi\|^2 = 1$ this is an irreducible representation of $A_4$ too. The character table is therefore the following:

| | 1 [1] | (12)(34) [3] | (123) [4] | (132) [4] |
|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | 1 | $e^{2\pi i/3}$ | $e^{4\pi i/3}$ |
| $\chi_3$ | 1 | 1 | $e^{4\pi i/3}$ | $e^{2\pi i/3}$ |
| $\chi$ | 3 | -1 | 0 | 0 |

TABLE 8. The character table of $A_4$.

34.3. **Representations of $D_n$.** Our usual method falls short of finding all the irreducible representations. The commutator of $D_n$ is $\langle x^2 \rangle$ and so, if $n$ is odd, $D_n^{ab} \cong \mathbb{Z}/2\mathbb{Z}$ and if $n$ is even $D_n^{ab} \cong (\mathbb{Z}/2\mathbb{Z})^2$. It thus has two 1-dimensional representations if $n$ is odd and four if $n$ is even. We also know $\rho^{plane}$, an irreducible 2 dimensional representation. Note though that at best the sum of the squares of these irreducible representations is 8 that is almost negligent compared to $2n$ if $n$ is large. That is, (except for $D_3$ and $D_4$) we are missing most of the irreducible representations.

We will now construct irreducible representations of $D_n$ in a somewhat ad hoc way. The main tool here goes under the name "induced representations" but we will not discuss it in this course. Fix an $n$-th root of unity $\zeta$ and let

$$\rho_\zeta : \langle x \rangle \to \mathbb{C}^\times$$

be the 1-dimension character given by the homomorphism

$$\rho(x^a) = \zeta^a.$$

We now let $x^a$ act on $\mathbb{C}^2$ by

$$x^a \mapsto \begin{pmatrix} \zeta^a & 0 \\ 0 & \zeta^{-a} \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Note that we do have a homomorphism

$$\langle x \rangle \to \mathrm{GL}_2(\mathbb{C}).$$

To show that extends to a well-defined homomorphism

$$r_\zeta : D_n \to \mathrm{GL}_2(\mathbb{C}),$$

we need to check that $yxy$ and $x^{-1}$ map to the same element. Namely, that we have

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \zeta^a & 0 \\ 0 & \zeta^{-a} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \zeta^{-a} & 0 \\ 0 & \zeta^a \end{pmatrix}.$$

But this is straightforward. We have obtained $n$ representations $r_\zeta$ of dimension 2. The character of $\chi_\zeta$ of $\rho_\zeta$ is given by

$$\chi_\zeta(x^a) = \zeta^a + \zeta^{-a}, \quad \chi_\zeta(x^a y) = 0.$$

We see that $\chi_\zeta = \chi_{\zeta^{-1}}$ and otherwise the characters are distinct. This, for $n$ odd, gives us $(n-1)/2$ distinct two dimensional representations. They are, in fact, all irreducible – we leave that as an exercise. In addition, still for $n$ odd, we have two 1-dimensional representations. But, as

$$1^2 + 1^2 + \frac{n-1}{2} \cdot 2^2 = 2n,$$

we have found all the irreducible representations of $D_n$ for $n$ odd. Similar considerations apply for the case $n$ even.

## 35. Some of the applications of group representations

This is a very sketchy section that mainly contains pointers to the literature. I will leave it to you to chase these references down, if you are interested. First, there are the two survey articles by T. Y. Lam, *"Representations of Finite Groups: A Hundred Years, Part I, and Part II"*. You can find the articles here:
http://www.ams.org/notices/199803/lam.pdf
http://www.ams.org/notices/199804/lam2.pdf

Secondly, there is the following post on Math overflow about "Fun applications of representations of finite groups", from which I have learned a lot myself.

https://mathoverflow.net/questions/11784/fun-applications-of-representations-of-finite-groups

I don't know if I would have used the adjective "fun", but there are certainly diverse and interesting applications. You would note in particular applications to:

(1) *Chemistry and Physics*, specifically quantum chemistry and quantum physics. For example, one user mentions "The symmetry group of a molecule controls its vibrational spectrum, as observed by IR spectrosocopy. When Kroto et al. discovered C60, they used this method to demonstrate its icosahedral symmetry." They suggest *Group Theory and Chemistry* by David M. Bishop as a reference. Another post suggests the book *Group Theory and Physics* by S. Sternberg for the connections to Physics quoting Sternberg saying that "molecular spectroscopy is an application of Schur's lemma". Another very convincing book is *Group theory and its applications to physical problems* by M. Hamermesh.
(2) *Combinatorics*. A lot of this is done through representations of the symmetric group and related groups. This is a topic to which many books, book chapters, and articles are devoted. The symmetric group plays a crucial role in combinatorics, of course. Mathscinet returns 455 references for searching for "Representation" and "symmetric group" in title, among which 14 are books.
(3) *Probability and Statistics*. Here perhaps we can rest our case by referring to a book by one of the leading statisticians and probablists of our time *Group representations in probability and statistics* by P. Diaconis.

(4) Within *algebra*, the celebrated Feit-Thompson theorem uses the following theorem of Frobenius, to which the only known proofs use representation theory.

A finite group $G$ is called a **Frobenius group** with Frobenius kernel $K$ and Frobenius complement $H$ if $G$ has a subgroup $H$, such that for any $g \notin H$ we have

$$H \cap gHg^{-1} = \{1\}.$$

One lets in this case

$$K = \{1\} \cup (G - \bigcup_{g \in G} gHg^{-1}).$$

$K$ is called the Frobenius kernel.

An example of a Frobenius group is the group of affine linear transformations of the line $\{ax + b\}$ with $H$ being the linear transformations $\{ax\}$. We can also write this group as $\{ \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \}$.

**Theorem 1** (Frobenius' theorem) *Let $G$ be a Frobenius group with Frobenius complement $H$ and Frobenius kernel $K$. Then $K$ is a normal subgroup of $G$, and $G$ is the semidirect product $K \rtimes H$.*

The hard part is to show that $K$ is a group!

**Theorem 2** (Frobenius' theorem, equivalent version) *Let $G$ be a group of permutations acting transitively on a finite set $X$, with the property that any non-identity permutation in $G$ fixes at most one point in $X$. Then the set of permutations in $G$ that fix no points in $X$, together with the identity, is closed under composition.*

Apparently, there is still no proof of these theorems that avoids using group representations in an essential way. Although recently, Terrence Tao gave a proof that only uses character theory for finite groups. I have learned much about this from reading Tao's blog

https://terrytao.wordpress.com/2013/04/12/the-theorems-of-frobenius-and-suzuki-on-finite-groups/

Another very nice application within Algebra is the proof of Burnside's theorem already cited: *if $p, q$ are primes then a group of order $p^a q^b$ is solvable.* The proof is almost within our reach, but not quite. It uses several ideas from algebra that we hadn't discussed at all (such as the theory of modules and algebraic integers) and a little more than we had done regarding representations of groups. In particular, it uses an additional orthogonality relation: *the columns of the character table are orthogonal* in the following sense. Let $G$ be a finite group and $g, h \in G$ elements. Let $\chi_i$ be the irreducible characters of $G$ (that is, the characters of its irreducible representations) then:

(5) $$\sum_{\chi_i} \chi_i(g)\overline{\chi_i(h)} = \begin{cases} |Cent_G(g)|, & \text{if } g, h \text{ are conjugate} \\ 0 & \text{otherwise.} \end{cases}$$

(The summation extending over the irreducible characters.) The main idea here is the the rows are "essentially" a collection of orthonormal basis. Thus, if properly modified, one can make them into truly orthogonal matrix. That is, into a matrix $M$ that satisfies $MM^* = I_h$ ($h = h(G)$). But then also $M^*M = I_h$ and reading this information carefully gives the orthogonality of the columns.

Finally, but still within the real of pure Algebra, group representations have a lot to do with the study of simple groups. The classification of simple groups puts them in large families ($\mathbb{Z}/p\mathbb{Z}$, $A_n$, $\mathrm{PSL}_n(\mathbb{F}), \dots,$) but some escape this classification and fall into a category of themselves: the sporadic simple groups. There are finitely many such groups – 27, in fact. The largest simple group is the Monster group, its order is $808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000$.

Its existence is a non-trivial fact. Before constructing the Monster, mathematicians suspected its existence and in fact predicted the dimensions of some of its smallest irreducible representations as $1, 196883$ and $21296876$, and were able, more generally, to work out its character table. John McKay, of Concordia university, made the audacious observation that those numbers are related to Fourier coefficients of the $j$-function, a function appearing in the theory of elliptic curves, which is part of number theory. Following that, precise conjectures were made by Conway and Norton, going under the name of "Moonshine".

Some of the key aspects of these conjectures were proven by R. Borcherds, a work that got him the Fields prize in 1998.

## 36. What is missing

We have barely scratched the surface when it comes to group representations. But, I would say that at the very basic entry level to representations of finite groups there is one more topic that we could have discussed if we had more time. This is the subject of **induced representations** and **Frobenius reciprocity**. Besides it's theoretical importance it is a powerful computational tool. This subject is completely within reach and those wishing to have a more complete picture are encouraged to pursue it using any textbook dealing with group representations.

Besides this topic, other glaring omissions are some study of (i) the representations of symmetric group and their connections to Young tableaux, hook lengths and other mysterious terminology; (ii) Representations of nilpotent groups, and in particular $p$-groups (Blichfeldt's theorem). Once more, these topics would (or should) be covered in most textbooks dealing with representations of finite groups; (iii) Representations of finite matrix groups, for example $\mathrm{GL}_n(\mathbb{F}_p)$.

Blichfeldt's theorem asserts that every irreducible representation of a finite nilpotent group $G$, for example, every irreducible representation of a finite $p$-group, is induced from a 1-dimensional representation of a subgroup $H$ of $G$.

Going perhaps further back, some topics that should be covered in more detail as part of an introduction to finite groups are the topics: (i) Free groups and free products and the **Nielsen-Schreier theorem**; (ii) **Nilpotent groups** and the notions of **ascending** and **descending central series**. (iii) Simplicity of the groups $\mathrm{PSL}_n(\mathbb{F}_q)$. Once more, these topics are certainly accessible and it is only for reasons of time that we have omitted them.

## Part 9. Exercises

(1) Prove directly from the definitions that every group of order 3 is cyclic (and in particular commutative). Do the same for order 5.

(2) Let $G$ be a group of even order. Show, directly from the definitions, that $G$ has an element of order 2.

(3) Prove directly from the definitions that a group $G$ in which every element $a$ satisfies $a^2 = e$ is commutative. Prove further that if $G$ is finite then $G$ has $2^n$ elements for some integer $n$.

(4) Write down all the elements of $\mathrm{GL}_2(\mathbb{F}_2)$. Consider the action of this group on the set of non-zero vectors in $\mathbb{F}_2^2$ (the two dimensional vector space over $\mathbb{F}_2$). Show that this allows one to identify the group $\mathrm{GL}_2(\mathbb{F}_2)$ with the symmetric group $S_3$.

(5) Let $D_{2n}$, $n \geq 3$, be the dihedral group with $2n$ elements. It is generated by $x, y$, satisfying $x^n = y^2 = xyxy = 1$. Prove (algebraically) that every element not in the subgroup $\langle x \rangle$ is a reflection and find (geometrically) the line through which it is a reflection.

(6) Let $n \geq 2$. Prove that $S_n$ is generated by the set of all transpositions $\{(ij) : 1 \leq i < j \leq n\}$. Prove that in fact the transpositions $(12), (23), \dots, (n-1\ n)$ alone generate $S_n$.

(7) Let $\alpha \in \mathbb{R}^n$, $n \geq 2$, be a non-zero vector. We define a reflection in the hyperplane perpendicular to $\alpha$ by the formula

$$\sigma_\alpha(v) = v - \frac{2(v, \alpha)}{(\alpha, \alpha)} \cdot \alpha.$$

Here $(x, y)$ is the standard inner product on $\mathbb{R}^n$. Prove that $\sigma_\alpha$ is indeed a linear map that fixes the hyperplane orthogonal to $\alpha$ and sends $\alpha$ to $-\alpha$. Given $\alpha, \beta$ non-zero vectors, determine when the subgroup $\langle \sigma_\alpha, \sigma_\beta \rangle$ is infinite. Further, in case it is finite, determine it's order. (Suggestion: reduce to the case of $n = 2$.)

(8) Let $T$ be a non-empty set (possibly infinite) and define $\Sigma_T$ as the set of all functions $f \colon T \to T$ that are bijective. Show that $\Sigma_T$ is a group under composition of functions (if $T = \{1, 2, \dots, n\}$ we can identify $\Sigma_T$ with $S_n$). Show that for $T = \mathbb{Z}$ there are elements $\sigma, \tau \in \Sigma_T$, each of order 2, that generate a subgroup of infinite order.

(9) Find the lattice of subgroups of the groups $\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, S_3$, and $A_4$. Namely, write all the subgroups and determine which is contained in which. The following simple observation may help: Any subgroup of a finite group is generated by finitely many elements (for instance, all its elements). Thus, we can start by writing all the subgroups generated by one element - the cyclic subgroups, then all the subgroups generated by two elements, and so on. It is useful to note that if we find two subgroups $H_1 \subset H_2$ such that $|H_2|/|H_1|$ is prime, there is no subgroup strictly between $H_1$ and $H_2$ (why?).

(10) The Euler $\phi$-function,

$$\phi : \mathbb{Z}_{>0} \to \mathbb{Z},$$

defined by

$$\phi(n) = \sharp\{0 < a \leq n : \gcd(a, n) = 1\}.$$

Prove that it has the following properties:
- If $n$ and $m$ are relatively prime then $\phi(nm) = \phi(n)\phi(m)$.
- If $p$ is a prime $\phi(p^a) = p^a - p^{a-1}$.
- $\phi(n) = n \prod_{p|n}(1 - 1/p)$ (the product taken over the prime divisors $p$ of $n$).

(11) Let $p$ be an odd prime. Prove that for every $n \geq 1$ the group $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic. Suggestion: consider first the subgroup $B = \{a \in \mathbb{Z}/p^n\mathbb{Z} : a \equiv 1 \pmod{p}\}$.

(12) Prove that the group $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is trivial for $n = 1$, cyclic for $n = 2$ and isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$ for $n \geq 3$. Suggestion: for $n \geq 3$ consider the elements $-1$ and 5.

(13) (**Fermat primes**). Use group theory to prove the following: Let $h$ be an integer such that $p = 2^h + 1$ is prime. Prove that $h = 2^j$ for some non-negative integer $j$. (Prove first that the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$ is $2h$.) Thus, $p$ has the form $2^{2^j} + 1$. Such primes are called Fermat primes. [16]

(14) Use group theory to prove Wilson's theorem: For every prime $p$, $(p-1)! \equiv -1 \pmod{p}$.

(15) Let $G$ be a finite group. The **exponent** of $G$, $\exp(G)$, is defined as the minimal positive integer $m$ such that $x^m = 1$ for all $x \in G$. Prove:
  (a) If $G$ is abelian then $\exp(G) = \max\{\mathrm{ord}(x) : x \in G\}$.
  (b) If $G$ is not-abelian the previous statement may fail.

(16) Give an example of groups $H_1 \lhd G_1, H_2 \lhd G_2$, such that $H_1 \cong H_2$ and $G_1/H_1 \cong G_2/H_2$, but $G_1 \not\cong G_2$.

(17) Give an example of groups $A \lhd B \lhd C$ such that $A$ is not normal in $C$.

(18) Let $\sigma \in S_n$ be a permutation. Find a formula (in terms of the factorization of $\sigma$ into disjoint cycles) for the cardinality of $\mathrm{Cent}_{S_n}(\sigma)$. Fix $n$; for which permutations $\sigma$ the minimum is obtained?

(19) Give an example of a group $G$ and a subgroup $H$ of $G$ for which $H \cap \mathrm{Cent}_G(H) = \{1\}$ and $\mathrm{Cent}_G(H) \neq \{1\}$.

(20) Prove that if $N < G$ and $[G : N] = 2$ then $N \lhd G$. (This can be done without using group actions.)

(21) Let $m < n$ be positive integers. Calculate $N_{S_n}(S_m)$. In particular, find when $N_{S_n}(S_m) = S_m$.

(22) Let $G$ be a group and let $C \subset G$ be a left coset of some subgroup of $G$. Prove that $C$ is also a right coset of some (usually different) subgroup of $G$.

(23) *Characteristic subgroups*. A subgroup $H$ of a group $G$ is called **characteristic** if for every automorphism $f : G \to G$ we have $f(H) = H$.
  (a) Prove that a characteristic subgroup is a normal subgroup. (Hint: consider $x \mapsto gxg^{-1}$ for $g$ fixed.)
  (b) Prove that the centre of $G$, $Z(G)$ is a characteristic subgroup, as well as the commutator subgroup $G'$.
  (c) Give an example of a normal subgroup that is not characteristic.
  (d) Prove that if $H$ is normal in $G$ and $K$ is a characteristic subgroup of $H$, then $K$ is normal in $G$.

---

[16] For $j = 0, 1, 2, 3, 4$ we indeed get primes. They are the primes $3, 5, 17, 257, 65537$. To date (June 2020) no other Fermat prime is known. In particular, $2^{2^5} + 1 = 4294967297$ was famously factored by L. Euler as $641 \times 6700417$ and it known today that all numbers of the form $2^{2^j} + 1$ are composite for $5 \leq j \leq 32$. It is interesting to note that Fermat conjectured that all numbers of the form $2^{2^j} + 1$ are primes. Well, he did better with conjecturing Fermat's last theorem.
Fermat primes are interesting in the context of constructing a regular polygon with $n$ sides using only a straightedge and a compass. This is possible if and only if $n$ if of the form $n = 2^k p_1 p_2 \cdots p_s$, where $k$ is a non-negative integer and the $p_i$ are distinct Fermat primes.

(24) If $G, H$ are finite groups such that $(|G|, |H|) = 1$ prove that every group homomorphism $f : G \to H$ is trivial ($f(G) = \{1\}$).

(25) Find all possible homomorphisms $Q \to S_3$. Is there an injective homomorphism $Q \to S_4$? (As usual, $Q$ is the quaternion group of order 8).

(26) Prove that a non-abelian group of order 6 is isomorphic to $S_3$. Prove that every abelian group of order 6 is isomorphic to $\mathbb{Z}/6\mathbb{Z}$.

Here are some hints: start by showing that every group $G$ of order 6 must have an element $x$ of order 2 and an element $y$ of order 3. This in fact follows from some general theorems but I want you to argue directly using only what we covered in class. (A typical problem here is why can't all the elements different from 1 have order 3. If this is the case, show that there are two cyclic groups $K_1, K_2$ of $G$ of order 3 such that $K_1 \cap K_2 = \{1\}$. Calculate $|K_1K_2|$.)

Having shown that, if $G$ is abelian show it implies the existence of an element of order 6. In the non-abelian case show that we must have $xyx^{-1} = y^2$ and that every element in $G$ is of the form $x^a y^b$, $a = 0, 1$, $b = 0, 1, 2$. Show that the map $x \mapsto (1\ 2), y \mapsto (1\ 2\ 3)$ extends to an isomorphism.

(27) Let $G$ be a finite group with a unique maximal subgroup. Prove that $G$ is cyclic of prime power order.

(28) Prove that $\mathbb{Q}$, considered as an abelian group relative to addition, has no maximal subgroups.

(29) Let $G$ be a group. Let $\mathrm{Aut}(G)$ be the collection of automorphisms of $G$ (isomorphisms from the group onto itself). Show that $\mathrm{Aut}(G)$ is a group under composition. For every $g \in G$ let $\tau_g : G \to G$ be the map $\tau_g(x) = gxg^{-1}$. Prove that $\tau_g \in \mathrm{Aut}(G)$ and that the map $G \to \mathrm{Aut}(G), g \mapsto \tau_g$, is a homomorphism of groups whose kernel is the centre $Z(G)$ of $G$. The image is called the **inner automorphisms** of $G$ and is denoted $\mathrm{Inn}(G)$. Prove that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$. The quotient group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the **outer automorphism group** of $G$ and is denoted $\mathrm{Out}(G)$.

(30) Prove that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

(31) In this exercise we shall prove that $\mathrm{Aut}(S_n) = S_n$ for $n > 6$. (The results holds true for $n = 4, 5$ too and fails for $n = 6$.) Thus, $S_n$ is complete for $n > 6$.

   (a) Prove that an automorphism of $S_n$ takes an element of order 2 to an element of order 2.
   (b) For $n > 6$ use an argument involving centralizers to show that an automorphism of $S_n$ takes a transposition to a transposition.
   (c) Prove that every automorphism has the effect $(12) \mapsto (a\ b_2), (13) \mapsto (a\ b_3), ..., (1n) \mapsto (a\ b_n)$,for some distinct $a, b_2, ..., b_n \in \{1, 2, ..., n\}$. Conclude that $\sharp\mathrm{Aut}(S_n) \leq n!$.
   (d) Show that for $n > 6$ there is an isomorphism $S_n \cong \mathrm{Aut}(S_n)$.

(32) **Double cosets**. Let $G$ be a group and $A, B$ be subgroups of $G$. A double coset is a set of $G$ of the form $AgB$ for some $g \in G$.

   (a) Prove that double cosets are either equal or disjoint. Prove that $G$ is a disjoint union of double cosets.
   (b) Provide a necessary and sufficient condition for $AgB = AhB$.
   (c) Give a formula for $|AgB|$. Is it true that all double cosets have the same cardinality?
   (d) Interpret double cosets as orbits for a certain group action. (Make sure that your initial guess really defines a group action!)

(e) Let $A$ be a subgroup of $G$ such that every double coset $AgA$ of $A$ is equal to some coset $hA$ of $A$. Prove that $A$ is normal, and vice-versa.

(33) Let $G$ be a finite group consisting of linear transformations of a finite dimensional vector space $V$ over the field $\mathbb{F}_p$ of $p$ elements ($p$ prime). Suppose that the order of $G$ is a power of $p$. Show that there is a vector $v \in V, v \neq 0$ that is an eigenvector with eigenvalue 1 for the elements of the group $G$.

Arguing inductively, show that there is a basis in which $G$ consists of upper-triangular unipotent matrices. (Suggestion: let $W$ be the span of $v$ and consider $V/W$.)

(34) Let $H, K$ be subgroups of a group $G$. Prove that

$$[G : H \cap K] \leq [G : H] \cdot [G : K].$$

(35) Find the number of necklaces with 16 beads, 8 of them blue, 4 red and 4 white, up to symmetries by $D_{16}$.

(36) Find the number of necklaces with 12 beads, 2 red, 4 green, 3 blue and 3 yellow.

(37) Let $G$ be a finite group. Let $p$ be the minimal prime dividing the order of $G$ and suppose that $G$ has a subgroup $K$ of index $p$. Prove that K is normal. (Hint: use the coset representation.)

(38) Let $A$ be a proper subgroup of a finite group $G$. Prove that $G \neq \cup_{g \in G} gAg^{-1}$. Prove that this statement may fail for infinite groups (suggestion: Try $G = \mathrm{GL}_2(\mathbb{C})$ for the second part).

(39) Let $S_3$ act on $\mathbb{F}^3$, where $\mathbb{F}$ is a finite field with more than two elements, by permuting the coordinates. Find the number of orbits for this action. The size of an orbit is a divisor of 6 (why?). For each such divisor determine if there is an orbit of that size or not. (Either provide an example, or prove that none exists). Consider the action of $S_3$ on the subspace given by $x_1 + x_2 + x_3 = 0$. How many orbits are there?

(40) Let $G$ be a group and $H$ a subgroup of $G$ and let $[G : H] = n$. We consider here the question of whether there is an element in $g \in G$ such that $\{H, gH, \dots, g^{n-1}H\}$ are *all* the cosets of $H$ in $G$.
   (a) Show that if $n$ is not prime this may fail.
   (b) Show that if $n$ is prime such $g$ always exists. (Suggestion: Show first that a transitive subgroup of $S_n$ has order divisible by $n$. Show then that if $p$ is prime, a transitive subgroup of $S_p$ has an element of order $p$. Use the coset representation to finish the proof. )

(41) Let $G$ be a group acting transitively on a set $S$ and let $s \in S$ be some element. Let $K$ be a normal subgroup of $G$. Prove that the number of orbits for $K$ in its action on $S$ is the cardinality of $G/(K\,\mathrm{Stab}_G(s))$.

(42) Show that if $G$ acts transitively on a set of size $n$ then $G$ has a subgroup of index $n$ and, conversely, if $G$ has a subgroup of index $n$ then $G$ acts transitively on some set with $n$ elements.

For example, suppose we didn't know that the group $\Gamma$ of rigid transformation of the cube was isomorphic to $S_4$. We can deduce that $\Gamma$ has a subgroup of index 8 by its action on the vertices, a subgroup of index 12 by its action on the set of edges, a subgroup of index 6 by its action on the faces and a subgroup of index 4 by its action on the long diagonals; a subgroup of index 3 by its action on the 3 pairs of opposite faces and a subgroup of index 2 by doing a similar construction with the long diagonals.

(43) If there are $a$ colours available, prove that there are $\frac{1}{n}\sum_{d|n}\varphi(n/d)a^d$ coloured roulette wheels with $n$ sectors. (One puts no restriction on how many sectors are painted by a particular color.)

(44) Prove that the free group on 2 elements, $\mathscr{F}_2$ has a subgroup of index $n$ for every positive integer $n$.

(45) Prove that for $n \geq 5$, $A_n$ is the unique normal subgroup of $S_n$.

(46) Let the symmetric group $S_n$ act transitively on a set of $m$ elements. Assume that $n \geq 5$ and that $m > 2$. Show that $m \geq n$. Show that for every $1 \leq a \leq n$ there is a transitive action of $S_n$ on a set with $\binom{n}{a}$ elements.

(47) For which $n$, if any, is there an injective homomorphism $S_n \to A_{n+1}$?

(48) Prove that for $n \geq 5$ the commutator subgroup of $S_n$ is $A_n$.

(49) Let $n \geq 5$. Prove that $A_n$ is generated by the 3-cycles (namely, permutations of the form $(i\ j\ k)$, where $i, j, k$, are distinct). Prove that $A_n$ is generated by 5-cycles too.

(50) Write the conjugacy classes of $S_4$. For each conjugacy class choose a representative $x$ and calculate its centralizer $\mathrm{Cent}_{S_4}(x)$. Verify the class equation. Do the same for $A_4$. Use the results to find the normal subgroups of $A_4$ and, in particular, deduce that $A_4$ does not contain a subgroup of order 6.

(51) There is an obvious embedding of $S_3$ in $S_6$, the one in which $S_3$ acts on $\{1,2,3\} \subset \{1,2,3,4,5,6\}$. This embedding is not transitive, that is, given $1 \leq i < j \leq 6$ we cannot always find an element of $S_3$ that takes $i$ to $j$. Prove that there is a transitive embedding $S_3 \hookrightarrow S_6$ (i.e., such that the image acts transitively on the 6 elements). Given such embedding, write the image of $(12)$ and $(123)$.

(52) Write the conjugacy classes of $A_6$. Devise a direct proof that $A_6$ is simple.

(53) Let $G$ act transitively on a set $S$. We say that $G$ acts **primitively** if no partition of $S$, except for the trivial partitions $S = S$ and $S = \coprod_{s\in S}\{s\}$, is preserved by the action of $G$. Prove $G$ acts primitively if and only if the point stabilizer of a point of $S$ is a proper maximal subgroup of $G$.

(54) A group $G$ acts on a set **doubly transitively** if for any two elements $a \neq b$ and for any two elements $c \neq d$ there is $g \in G$ such that $ga = c$ and $gb = d$. Prove that if $G$ acts doubly transitively then it acts primitively. Give an example of a group $G$ acting on a set primitively, but not 2-transitively.

(55) In the class equation for finite groups, the number of conjugacy classes is called the class number of $G$. Thus, for example, if $G$ is abelian of order $n$ its class number is $n$. The group $S_3$ has class number 3, and more generally $S_n$ has class number $p(n)$ (the number of possible cycle structures). What is the class number of the quaternions $Q$? Of $A_n$ for $n \leq 7$? Of $A_n$ in general? Prove that if $G$ has even class number then $G$ has even order and provide a counter example for the converse.

(56) Let $G$ be a finite non-trivial $p$-group. Prove that $G'$ (the commutator subgroup of $G$) is a proper subgroup of $G$.

(57) Let $G$ be a finite $p$-group and $H \lhd G$ a non-trivial normal subgroup. Prove that $H \cap Z(G) \neq \{1\}$.

(58) Let $G$ be a finite $p$-group and $H$ a normal subgroup of $G$ with $p^a$ elements, $a > 0$. Prove that $H$ contains a subgroup of order $p^{a-1}$ that is normal in $G$. (Hint: use the previous exercise to prove the result by induction.)

(59) Let $G = \mathrm{GL}_n(\mathbb{F}_q)$, where $\mathbb{F}_q$ is a finite field, $q = p^r$ where $p$ is prime.

(a) Prove that the upper unipotent matrices $N := \left\{ \begin{pmatrix} 1 & * & * & \dots & * \\ 0 & 1 & * & \dots & * \\ \vdots & & & & \vdots \\ 0 & \dots & & & 1 \end{pmatrix} \right\}$ are a $p$-Sylow subgroup $P$ of $G$ by calculating the order of $P$ and $G$.

(b) Find conditions so that every element of $P$ has order dividing $p$. (Hint: use the binomial theorem for $(I+N)^p$, where $I$ is the identity matrix.)

(c) In particular, deduce that for any $p \neq 2$ there are non-abelian $p$-groups such that every element different from the identity has order $p$.

(d) Prove that a group $G$ in which $a^2 = 1$ for all $a \in G$ is an abelian group.

(60) There are up to isomorphism precisely two non-abelian groups of order 8; they are the dihedral group $D_4$ and $Q$ the quaternion group. $Q$ is the group whose elements are $\{\pm 1, \pm i, \pm j, \pm k\}$, where $-1$ is a central element and the relations $ij = k, jk = i, ki = j$, $i^2 = j^2 = k^2 = -1$ hold (in addition to the implicit relations such as $-1^2 = 1$, $-1 \cdot j = -j$, $\dots$). Prove the following

(a) $D_4$ is not isomorphic to $Q$.

(b) $D_4$ and $Q$ are non-abelian. (Calculate, for instance what is $ji$.)

(c) Let $P$ be the 2-Sylow subgroup of $\mathrm{GL}_3(\mathbb{F}_2)$. Find whether $P$ is isomorphic to $D_4$ or to $Q$.

(61) In Exercise 59 we found a $p$-Sylow subgroup $N$ of $G = \mathrm{GL}_n(\mathbb{F})$ where $\mathbb{F}$ is a finite field with $q = p^r$ elements. Prove that given a $p$-subgroup $H$ of $G$, viewed as a group of linear transformations, there is a basis to the vector space in which the elements of $H$ are upper-unipotent (this is, essentially, Exercise 33). Conclude that every maximal $p$-subgroup of $\mathrm{GL}_n(\mathbb{F})$ has $q^{n(n-1)/2}$ elements and that they are all conjugate.

Improve your argument to show that to give a $p$-Sylow subgroup of $\mathrm{GL}_n(\mathbb{F})$ is equivalent to giving a chain of subspaces $\{0\} \subsetneqq V_1 \subsetneqq V_2 \subsetneqq \cdots \subsetneqq V_n = \mathbb{F}^n$. Find how many $p$-Sylow subgroups there are.

(62) **Frattini's argument**. Let $G$ be a finite group, $H$ a normal subgroup of $G$ and $p$ a prime dividing the order of $H$. Let $P$ be a $p$-Sylow subgroup of $H$. Prove that $G = HN_G(P)$.

Use Frattini's argument to show that if $J$ is a subgroup of $G$ such that $J \supseteq N_G(P)$, where now $P$ is a $p$-Sylow of $G$, then $N_G(J) = J$. In particular, $N_G(N_G(P)) = N_G(P)$.

(63) Let $G$ be a finite group and $H$ a normal subgroup of $G$. Let $P$ be a $p$-Sylow subgroup of $G$ for some prime $p$. Show that $P \cap H$ is a maximal $p$-subgroup of $H$ (where here we allow that $P \cap H = \{1\}$ which is not technically a $p$-subgroup...). Further, show that $HP/H$ is a $p$-Sylow subgroup of $G/H$.

(64) Let $p$ be an odd prime. Find the order and generators for a $p$-Sylow subgroup of $S_p$ and $S_{2p}$.

(65) Find all Sylow subgroups, up to conjugation, for the groups $S_3$, $S_5$ and $\mathrm{GL}_3(\mathbb{F}_2)$.

(66) If the order of $G$ is 231, show that the 11-Sylow subgroup of $G$ is contained in the centre of $G$. (After establishing it's normal you would need eventually to use exercise 30.)

(67) If the order of $G$ is 385, show that the 7-Sylow subgroup of $G$ is contained in the centre of $G$ and the 11-Sylow is normal.

(68) Let $p$ be an odd prime. In this exercise we show that a non-abelian group $G$ of order $p^3$ that has an element $x$ of order $p^2$ is isomorphic to the group we have constructed in class. It is enough to show it is a semi-direct product $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

(a) Show that $Z(G) = G'$ is a subgroup of order $p$ and that $G/Z(G) \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. In particular, any commutator is in the centre of $G$ and is killed by raising to a $p$ power.
(b) Prove that $x^p$ generates the centre of $G$.
(c) Prove that to show that $G$ is a semi-direct product $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$, it is enough to show that there is an element $y \in G$ such that $y^p = 1$ and $y \notin Z(G)$.
(d) Let $y \notin \langle x \rangle$ and suppose that $y$ is of order $p^2$. Show that $G$ is generated by $x$ and $y$. We want to show that we can find an element $\tilde{y}$ of order $p$ such that $\tilde{y} \notin Z(G)$. We show that by counting how many elements of order $p$ the group $G$ has.
(e) Prove the surprising property, that the function $f : G \to G$, $f(t) = t^p$, is a homomorphism of groups. For that, explain why it is enough to prove the identity $x^p y^p = (xy)^p$ and proceed to prove this property by making use of identities of the form $xyxy = x[y,x]xyy = [y,x]x^2y^2$, etc.
(f) By estimating the image and the kernel of $f$ show that there exists an element $\tilde{y}$ as wanted.

(69) Let $G$ be a finite $p$-group. An element $g$ of $G$ is called a **non-generator** if whenever $S \cup \{g\}$ is a set of generators of $G$, so is $S$. Prove that $\Phi(G)$ is the set of non-generators of $G$. Prove further that the minimal number of generators of $G$ is $\dim_{\mathbb{F}_p}(G/\Phi(G))$ and that, in fact, any minimal set of generators has $\dim_{\mathbb{F}_p}(G/\Phi(G))$ generators.

(70) Calculate the Frattini subgroup of the upper unipotent matrices $N$ in $\mathrm{GL}_3(\mathbb{F}_p)$. Conclude that $N$ is generated by 2 elements. Find such 2 elements.

(71) Let $G$ be a solvable group. Prove that $G \neq G'$.

(72) Consider the groups of order bigger than 60 and less than 100. Prove that they are all solvable. (The choice of 100 is random. In fact, the next non-abelian simple group has 168 elements.)

(73) Let $\mathbb{F}$ be a field and consider the invertible matrices of the form $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ with $a, b \in \mathbb{F}$. Exhibit this group as a semi-direct product.

(74) Let $G = N \rtimes_\phi B$. Prove that $G$ is abelian if and only if both $N$ and $B$ are abelian and $\phi : B \to \mathrm{Aut}(N)$ is the trivial homomorphism.

(75) Construct a non-abelian group of order 75 as a semi-direct product. (Hint: at some point you may wish to use the matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$.)

(76) Find a composition series for $A_4$ and find the composition factors. Prove that $A_4$ doesn't have a composition series $A_4 = G_0 \rhd G_1 \cdots$ such that $G_0/G_1 \cong \mathbb{Z}/2\mathbb{Z}$. Thus, although the Jordan-Hölder theorem tells us that two composition series have the same quotients up to isomorphism and permutation, the converse is not true. Namely, given the composition factors we cannot necessarily find them arising from a composition series in any way we want.

(77) If $G = H_1 \times \cdots \times H_m = K_1 \times \cdots \times K_n$, where each $H_i$ and $K_j$ are simple groups then $m = n$ and there is a permutation $\sigma \in S_n$ such that $H_i \cong K_{\sigma(i)}$ for all $i = 1, 2, \dots, n$.

(78) Let $A, B$ be solvable subgroup of a group $G$. Suppose that $B \subseteq N_G(A)$ (and so $AB$ is a group). Prove that $AB$ is also solvable.

(79) Prove that a group of order $pqr$ is solvable, where $p < q < r$ are distinct primes.

(80) Prove that for every positive integer $n$, the group $\mathscr{F}(2)$ has a subgroup of index $n$. (Hint: think of transitive group actions on $n$ elements instead of subgroups of index $n$.)

(81) Let $n \geq 3$. Show that $\langle x, y | x^n, y^2, xyxy \rangle$ is a presentation of the dihedral group $D_n$.

(82) Find a presentation for the group $Q$ of quaternions of order 8.

(83) Prove that $\langle x, y | x^2, y^2 \rangle$ is an infinite group.

(84) Let $G$ be a finite abelian group and let $H$ be a subgroup of $G$. Prove that there is a subgroup $N$ of $G$ such that $G/N \cong H$. Prove also that there is a subgroup $M$ of $G$ such that $M \cong G/H$. (Hint: use $G^*$). Already $S_3$ shows that those properties are not necessarily true for non-abelian groups.

(85) Let $p(\cdot)$ be the **partition function**. That is, $p$ is defined on positive integers and $p(a)$ is the number of distinct partitions $a = \lambda_1 + \lambda_2 + \cdots + \lambda_s, \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_s > 0$, of $a$ into positive integers ($s$ is allowed to vary at will). Prove that if $n = p_1^{a_1} \cdots p_r^{a_r}$, where the $p_i$ are distinct primes, then there are precisely $p(a_1) \cdots p(a_s)$ isomorphism classes of abelian groups of order $n$. Find their structure for $n = 10800$.

(86) Let $S^1 = \{z \in \mathbb{C} : |z| = 1\}$, which is a group under multiplication. For a finite group $G$ define
$$G^* = \mathrm{Hom}(G, S^1),$$
the **character group** of $G$. Prove that $G^*$ is indeed a group under multiplication of functions. Prove:
 (a) $(A \oplus B)^* \cong A^* \oplus B^*$.
 (b) If $G$ is a finite abelian group then $G \cong G^*$.
 (c) Let $G$ be a finite abelian group and $H$ a subgroup of $G$. Show that there is a subgroup $N$ of $G$ such that $G/N \cong H$. Similarly, if $H$ is isomorphic to a quotient group of $G$ then $H$ is isomorphic to a subgroup of $G$. (Hint: use duality arguments using the character group $G^*$.)
 (d) Show that if $G$ is a finite abelian group, then any $n$-dimensional representation of $G$ is of the form $\alpha_1 \oplus \cdots \oplus \alpha_n$ for some $\alpha_i \in G^*$. Cf. §30.3.4.

(87) (a) Find the four 1-dimensional representations of the quaternion group $Q$ and calculate for each its character.
 (b) The quaternion group $Q$ acts on $\mathbb{C}^2$ via its embedding $Q \subseteq \mathrm{GL}_2(\mathbb{C})$. Write the character $\chi$ for this action and calculate $\|\chi\|^2$.
 (c) Write the character table of $Q$.

(88) Let $(\rho, V)$ be a 3-dimensional representation of the quaternion group $Q$. Show that there is a vector $v \neq 0$ that is an eigenvector for every $\rho(g), g \in Q$.

(89) The group $A_4$ acts on $\mathbb{R}^3$ via its action on a regular tetrahedron. Write the character $\chi$ for this action and calculate $\|\chi\|^2$. (Hint: you don't have to work with the usual basis. There is a another basis for $\mathbb{R}^3$ in which the computations are much easier!)

(90) Find the decomposition of the representation $\mathbb{Z}/4\mathbb{Z} \to \mathrm{GL}_2(\mathbb{C})$, $a \mapsto \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)^a$ into a sum of irreducible representations.

(91) Let $G$ be a finite group of order $n$ and class number $h$ and consider its character table. Modify the rows of the character table suitably so as to obtain genuine orthogonal rows and so a $h \times h$ orthogonal matrix. Use this modified matrix to prove that the columns of the character table are orthogonal too and so for $g, h \in G$ and $\{\chi_i\}$ the irreducible characters of $G$:
$$\sum_{\chi_i} \chi_i(g)\overline{\chi_i(h)} = \begin{cases} |Cent_G(g)|, & \text{if } g, h \text{ are conjugate;} \\ 0, & \text{otherwise.} \end{cases}$$
(The summation extending over the irreducible characters.)

(92) The group $S_n$ acts $\{1,2,\dots,n\}$. Consider all pairs of distinct elements in $\{1,2,\dots,n\}$. There are $n(n-1)/2$ such. The group $S_n$ acts on these elements by

$$\sigma * \{i,j\} = \{\sigma(i), \sigma(j)\}.$$

Consider now a vector space of dimension $n(n-1)/2$ with basis

$$\{v_{\{i,j\}}, \quad i \neq j\}.$$

Or, put differently, let $T$ be the set whose elements are the $n(n-1)/2$ subsets $\{i,j\}$. Then $S_n$ acts on $T$. And we take a vector space with basis

$$\{v_t, \quad t \in T\}.$$

There is a linear representation $\rho$ of $S_n$ on this vector space such that

$$\rho(\sigma)(v_t) = v_{\sigma(t)}.$$

Nothing to prove so far. Now, specialize all this to the case $n = 4$. Write the character of the representation $\rho$. Using the character table of $S_4$ (it appears in the course notes) decompose the 6-dimensional representation $\rho$ into irreducible representations. You are not required to decompose the vector space itself, only to find the abstract decomposition of $\rho$ into a sum of irreducible representations.

Now view $\rho$ merely as representation of the Klein group. Factor it into irreducible representations (in the same sense as above).

(93) Show that for $n \geq 4$, $\rho^{st,0}$, viewed as a representation of $A_n$, is irreducible.

(94) Let $z$ be a central element of a finite group $G$ and $V$ an irreducible representation of $G$. Show that $z$ acts on $V$ as a multiple of the identity endomorphism. (Hint: use Schur's lemma.)

(95) One of the first, and fundamental, results we proved about representations of finite groups is their decomposition into irreducible representations, provided that we are dealing with representations on finite dimensional complex vector spaces. In this exercise we show that this fails in characteristic $p$.

Let $\mathbb{F}$ be a field of characteristic $p$, hence we may assume that $\mathbb{Z}/p\mathbb{Z} \subset \mathbb{F}$. Consider the group of upper unipotent matrices in $\mathrm{GL}_n(\mathbb{Z}/pZZ)$, which acts naturally of $\mathbb{F}^n$, thought of as columns vectors of length $n$ with coordinates in $\mathbb{F}$. Call this representation $(\rho, \mathbb{F}^n)$.

For every $1 \leq a \leq n-1$, find an $a$-dimensional sub-representation $U$ of $(\rho, \mathbb{F}^n)$ and prove that it doesn't have a complement; that is, prove that there is no other sub-representation $V$ of $(\rho, \mathbb{F}^n)$ such that $U \oplus V = \mathbb{F}^n$.

**Additional and challenging exercises about groups:**

(96) A group $G$ is called **complete** if $Z(G) = \{1\}$ and $\mathrm{Out}(G) = \{1\}$. Otherwise said, if $G \cong \mathrm{Aut}(G)$ via the natural homomorphism $G \to \mathrm{Aut}(G)$. Prove that if $G$ is a simple non-abelian group then $\mathrm{Aut}(G)$ is complete.

(97) Let $G$ be a finite group and $K$ a normal subgroup of $G$. Suppose that $K$ is a simple group and that $|K|^2 \nmid |G|$. Prove that $G$ doesn't have any subgroup that is isomorphic to $K$ besides $K$. In particular, conclude that $K$ is a characteristic subgroup.

(98) Let $G$ be a finite simple group. Let $H$ be a subgroup of $G$ whose index is a prime $p$. Prove that $p$ is the maximal prime dividing the order of $G$ and that $p^2 \nmid |G|$.

# Index