ALGEBRA 3 (MATH 456)
COURSE NOTES
FALL 2021
VERSION: January 21, 2022

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 this 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 a product is done by successively multiplying two elements at the time, e.g. $(((g_1g_2)(g_3g_4))g_5)g_6$ is a way to compute $g_1g_2g_3g_4g_5g_6$.

[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 it 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_α or g_α^{-1}.*

Proof. Clearly $\langle\{g_\alpha : \alpha \in I\}\rangle$ contains each g_α hence all the expressions $h_1 \cdots h_t$ where each h_i is some g_α or g_α^{-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_α or g_α^{-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 called **Euler's phi function**; See Exercise 17 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 we do indeed 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 integers 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 for $\mathbb{R}^2$) and that it takes these vertices, respectively, 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 to 2 and 2 to 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 in this group are consequences of these. For example, one proves that $x^a y = yx^{-a}$ for any power a.

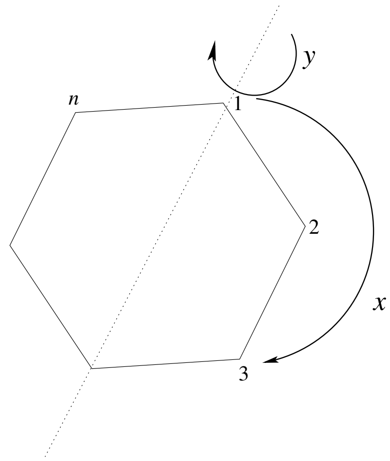


FIGURE 1. Symmetries of a regular Polygon with n vertices.

The **Dihedral group** D_n, the group consisting 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. If n is odd, each such reflection has a unique fixed vertex. If n is even, half the reflections have no fixed vertices and half the reflections have 2 fixed vertices.

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 multiplication by

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

This makes S_n into a group, whose identity 1 is the identity function $1(i) = i, \forall i$.

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 σ 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 σ 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 Σ_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 σ is just the inverse function σ^{-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 Σ_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 $\left(\begin{smallmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{smallmatrix}\right)$ 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 $\left(\begin{smallmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{smallmatrix}\right)$. 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 σ, τ,

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

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 σ, 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 σ we have

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

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

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

This gives

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

□

Calculating sgn **in practice.** Recall that every permutation σ 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 σ 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_σ is the matrix (a_{ij}) with $a_{ij} = 0$ unless $i = \sigma(j)$ and $a_{\sigma(i)\,i} = 1$. 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_σ 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 (Exercise 10).

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 σ^{-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** σ by τ). If σ is written as a product of cycles then the permutation $\tau\sigma\tau^{-1}$ is obtained by applying τ to the numbers appearing in the cycles of σ. That is, if σ 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 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 also 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 $A^{-1}A = I_n$ 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. □

Example 2.5.3. It is not hard to prove that the set of upper triangular matrices in $\mathrm{GL}_n(\mathbb{F})$, where $\mathbb{F}$ is any field, forms a subgroup of $\mathrm{GL}_n(\mathbb{F})$. It is also called a **Borel subgroup**. Likewise, 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 $\mathrm{GL}_n(\mathbb{F})$. 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

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

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 these matrices. We then 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 finite cyclic groups whose orders are co-prime then $G \times H$ is also a cyclic group. More precisely, if g generates G and h generates H, $\mathrm{ord}(g) = a$, $\mathrm{ord}(h) = b$ and $(a, b) = 1$, then the order of the element $(g, h) \in G \times H$ is ab, which is equal to the order of $G \times H$. Thus, (g, h) is a generator of $G \times H$.

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. See also Exercise 146.

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
13	$\mathbb{Z}/13\mathbb{Z}$	
14	$\mathbb{Z}/14\mathbb{Z}$	D_7
15	$\mathbb{Z}/15\mathbb{Z}$	

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 groups of order 2^n for small values of n (from Wikipedia and Groupprops, September 2021)

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	2048
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 only discuss 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:

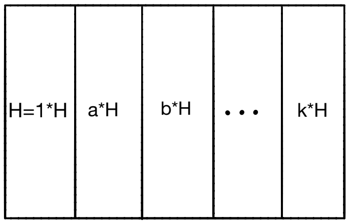


FIGURE 2. Cosets of a subgroup H.

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.

Example 3.1.4. When the group G is commutative and we choose to write the group law additively then the cosets of a subgroup H are of the form

$$x + H = \{x + h : h \in H\}$$

and

$$x + H = y + H \;\Leftrightarrow\; y - x \in H.$$

For example, if $G = \mathbb{Z}$ and $H = n\mathbb{Z}$, where n is a positive integer, the cosets are of the form $x + H = \{x + nt : t \in \mathbb{Z}\}$ and so the cosets correspond to congruence classes modulo n. We have $x + H = y + H$ if and only if $y - x \in H$. This is equivalent to $n|(y-x)$, i.e. $x \equiv y \pmod{n}$.

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,

$$G = \uplus_{i=1}^{s} g_i H,$$

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

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

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 $f' \colon yH \to xH$, $f'(g) = xy^{-1}g$ 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* $\mathrm{ord}(g) \mid |G|$ *for all $g \in G$.*

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

Remark 3.2.5. The converse does not hold. That is, if $n | |G|$ 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 $\mathrm{ord}(g) = |G|$.

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. □

Example 3.2.7. Consider the group S_4 and its subgroup D_4. There is no subgroup J of S_4 such that $S_4 \supsetneqq J \supsetneqq D_4$. 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, $G = \langle g \rangle = \{1, g, \dots, g^{n-1}\}$.

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 $\frac{n}{\gcd(a,n)}$ divides $\frac{a}{\gcd(a,n)} \cdot r$. Because $\frac{n}{\gcd(a,n)}$ and $\frac{a}{\gcd(a,n)}$ are relatively prime, $\frac{n}{\gcd(a,n)}$ must divide r. □

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 $\varphi(n) := \sharp\{1 \leq a \leq n : (a, n) = 1\}$, where φ 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 $0 \leq k' < a$. 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 α, β, 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 $g^{n/b}$. □

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 φ 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

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

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 $n = \sharp G = \sum_{d|n} \sharp\{\text{elements of order } d\} = \sum_{d|n} \varphi(d)\epsilon_d$, where ϵ_d is 1 if there is an element of order d in G and is zero otherwise. On the other hand, 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 needs to verify that this set is closed under addition, multiplication and inverse (multiplicative and additive). The only tricky one to check is closure under addition. But, 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 R. 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, using $[x, y]^{-1} = [y, x]$, we see that every element of G' is a product of commutators.

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

Taking $H = G$, the subgroup $\mathrm{Cent}_G(G)$ 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 $G = Z(G) = \mathrm{Cent}_G(H)$ for any subgroup $H < G$. If $H_1 \subseteq H_2 \subset G$ then $\mathrm{Cent}_G(H_2) \subseteq \mathrm{Cent}_G(H_1)$. If $G = G_1 \times G_2$ then $\mathrm{Cent}_{G_1 \times G_2}(G_1 \times \{1\}) = Z(G_1) \times G_2$ and, more generaly, $\mathrm{Cent}_{G_1 \times G_2}(H_1 \times H_2) = \mathrm{Cent}_{G_1}(H_1) \times \mathrm{Cent}_{G_2}(H_2)$.

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 σ by changing its entries according to τ. 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 $H \subset N_G(H), \mathrm{Cent}_G(H) \subset N_G(H)$ and $H \cap \mathrm{Cent}_G(H) = Z(H)$.

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 τ 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 $\mathrm{sgn}(\tau)\mathrm{sgn}(\sigma)\mathrm{sgn}(\tau^{-1}) = \mathrm{sgn}(\tau)^2\mathrm{sgn}(\sigma) = 1$. 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 $(13)(12)(13)^{-1} = (32)$.

Example 6.0.2. If G is abelian every subgroup of G is normal. The converse does not hold. Every subgroup of the quaternion group Q is normal, but Q is not abelian.

6.1. **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 $(gN)^{-1} = g^{-1}N$.

Definition 6.1.1. A non-trivial group G is called **simple** if its only normal subgroups are the trivial ones: $\{e\}$ and G.

Remark 6.1.2. 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.

6.2. **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 6.2.1. *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 6.2.2. *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^{ab} has order 2 and so is isomorphic[5] to $\mathbb{Z}/2\mathbb{Z}$. For n even, the group D_n^{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 6.2.3. *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

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

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).

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

6.3. Some lemmas about product and intersection of subgroups.

Lemma 6.3.1. *Let B and N be subgroups of G, $N \lhd G$.*

(1) $B \cap N$ is a normal subgroup of B.
(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) If $B \lhd G$ then $BN \lhd G$ and $B \cap N \lhd G$.
(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 $BN = \cup_{b \in B} bN = \cup_{b \in B} Nb = NB$.

(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*,

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

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 $bn = b_1n_1$ 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 6.3.2. 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 $\langle B, N\rangle \supset BN$ and equality does not hold. We can deduce though that

$$|\langle B, N\rangle| \geq \frac{|B| \cdot |N|}{|B \cap N|}.$$

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 $|\langle B, N\rangle| \geq |B| \cdot |N|$. 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 fall 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, famous for the discovery of the game of life, and who passed away in 2020 from COVID-19 complications, discovered

[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.

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 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 scalars, 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 $f(s_1) < f(s_2)$. And so on. 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 $K = \{1, (12)(34), (13)(24), (14)(23)\}$ 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* $h \in H$, *in the image of* f, *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 $a \in G$, π is surjective. Finally, $a \in \mathrm{Ker}(\pi)$ iff $\pi(a) = aN = N$ (the identity element of G/N), iff $a \in N$. □

The following Corollary is perhaps the best motivation for the introduction of the concept of normal groups. In light of it, we can say that this is a natural concept.

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 permutation $\sigma \in S_4$ we have the identity

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

and so S_4 acts on T by conjugation. As such, every σ 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 $\mathrm{Ker}(f)$ of this homomorphism consists of permutations σ 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 $K = \{1\} \cup T$ acts trivially on the elements of T and so $K \subset \mathrm{Ker}(f)$. It will follow from the first isomorphism theorem that $\mathrm{Ker}(f)$ has 4 elements and so one concludes that $K = \mathrm{Ker}(f)$.

7.2. **Behaviour 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. □

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, 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.

8.1.

Theorem 8.1.1. (**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]

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi_K"'] & & H . \\ & G/K \arrow[ur, "F"'] & \end{tikzcd}$$

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 π_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, $\mathrm{Ker}(F) = N/K$. □

Corollary 8.1.2. *Let $f\colon G \to H$ be a surjective homomorphism of groups. Then*

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

Proof. Indeed, from the commutativity of the diagram we conclude that $F\colon G/\mathrm{Ker}(f) \to H$ 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. □

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

Example 8.1.3. 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**:

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

Example 8.1.4. Let $\mathbb{F}$ be a field and consider the 3×3 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 6.2.3). At any rate, we find that

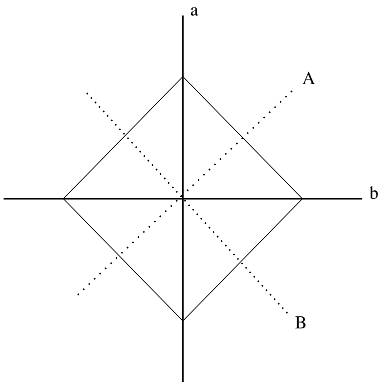
$$N/K \cong \mathbb{F} \times \mathbb{F}.$$

Example 8.1.5. 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 K. Thus, $\mathrm{Ker}(f) = K$.

Example 8.1.6. Let us construct two homomorphisms

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

We get the first homomorphism f_1 by looking at the action of the symmetries coming from D_4 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 point-wise). Similarly, if we let A, B be the lines indicated in the diagram,



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 8.1.7. 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 8.1.8. 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 8.1.9. 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. 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.

Proposition 8.1.10. *Let G be a group and let A be an abelian group. Any group homomorphism $f\colon G \to A$ factors uniquely through G^{ab}. If $\pi\colon G \to G^{ab}$ is the quotient map then there is a bijection between $\mathrm{Hom}(G^{ab}, A)$ and $\mathrm{Hom}(G, A)$ provided by $F \mapsto F \circ \pi$.*

Proof. Let $f\colon G \to A$. Since A is abelian, for any $x, y \in G$ we have $f([x, y]) = [f(x), f(y)] = 1$. Thus, every commutator is in the kernel of f and it follows that $G' \subseteq \mathrm{Ker}(f)$. By the First Isomorphism Theorem, f factors uniquely as

$$\begin{tikzcd}
G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & A . \\
& G/G' = G^{ab} \arrow[ur, "F"'] &
\end{tikzcd}$$

And, conversely, any $F\colon G^{ab} \to A$, where A is an abelian group induces a homomorphism $f\colon G \to A$ by $f = F \circ \pi$.

As the factorization and composition are inverse constructions, we get the bijection between $\mathrm{Hom}(G^{ab}, A)$ and $\mathrm{Hom}(G, A)$. □

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 6.3.1 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, 8.1.5. We have $f(S_3) \cong S_3/K \cap S_3$ where K is the Klein group and equal to the kernel of f. As every non-trivial element of K moves 4, we have $S_3 \cap K = \{1\}$. 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:*

$$\{\text{subgroups of } G \text{ containing } \mathrm{Ker}(f)\} \quad \longleftrightarrow \quad \{\text{subgroups of } H\}.$$

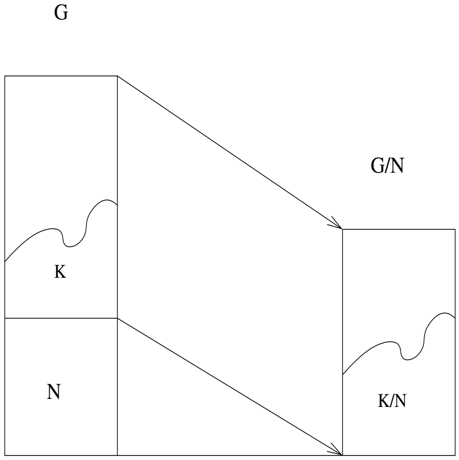
Given by $G_1 \mapsto f(G_1)$, $G_1 < G$, and in the other direction by $H_1 \mapsto f^{-1}(H_1)$, $H_1 < H$.

(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 (Proposition 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.

Finally, 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 8.1.6. 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:

$$\begin{tikzcd}
 & D_4 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
K_1 \arrow[dr, dash] & K_2 \arrow[d, dash] & K_3 \arrow[dl, dash] \\
 & \langle x^2 \rangle \arrow[d, dash] & \\
 & \{1\} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & S_2 \times S_2 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
H_1 \arrow[dr, dash] & H_2 \arrow[d, dash] & H_3 \arrow[dl, dash] \\
 & \{e\} &
\end{tikzcd}$$

We will see later that this does not exhaust the list of subgroups of D_4. Here we have
$K_1 = \langle x \rangle$,
$K_2 = \langle y, x^2 \rangle$,
$K_3 = \langle xy, x^2 \rangle$
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 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 8.1.4. 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 $\mathbb{F}\times\mathbb{F}$, which 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.

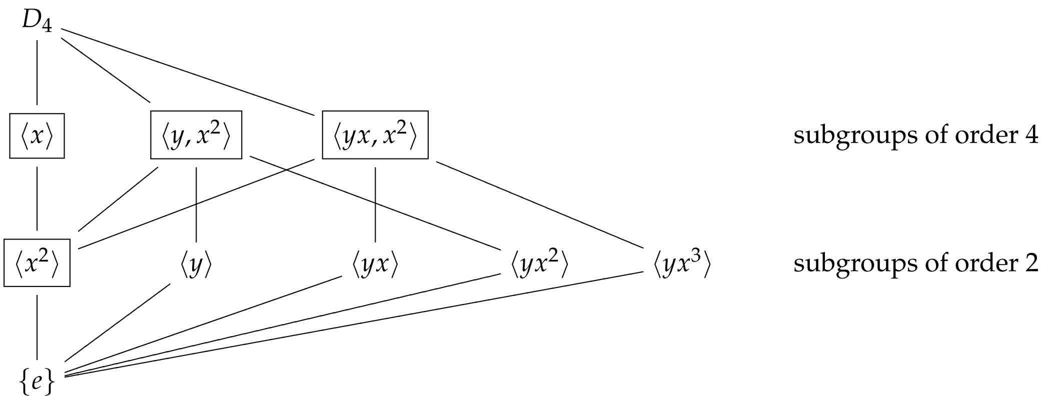
11. The lattice of subgroups of a group

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

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

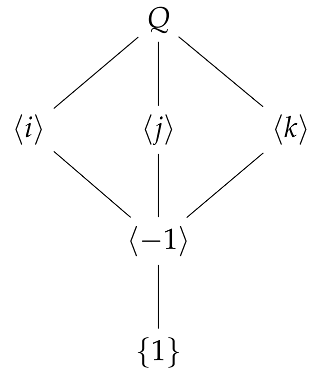
Here is the lattice of subgroups of D_4. Normal subgroup are boxed.



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.

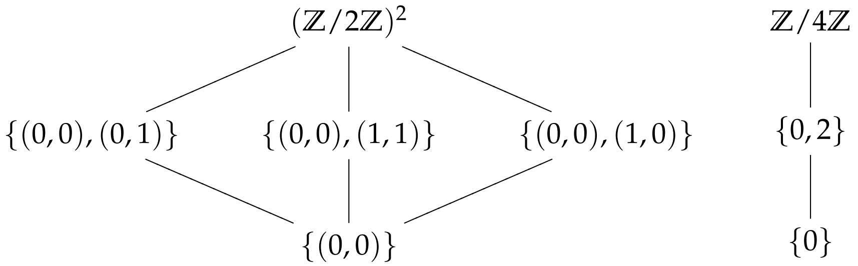
There are at least two ways in which one uses this concept:

- *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, $\mathrm{Orb}(s_1)$.

(2) Let $H = \mathrm{Stab}(s)$. We have to show that: (i) $e \in H$; (ii) 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,

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

Define a function

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

by

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

We claim that ϕ is a well defined bijection. First

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

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

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

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

and we get that ϕ is surjective.

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

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

□

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 $G/\mathrm{Stab}(s) \leftrightarrow \mathrm{Orb}(s)$. Thus, the picture of S is as follows

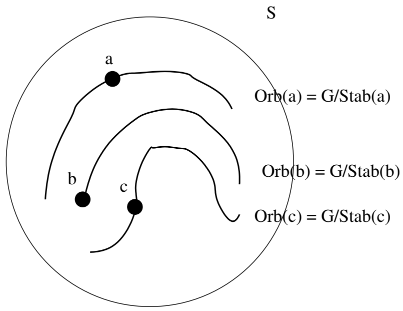


FIGURE 3. S decomposes into disjoint orbits.

Remark 13.0.3. 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).

Remark 13.0.4. We say that G acts **transtively** on S, or that the action is **transitive** if G has one orbit in S. Namely, if for all s_1, s_2 in S there is some $g \in G$ such that $g * s_1 = s_2$. In this case the number of elements of S is given by $\sharp G/\sharp\mathrm{Stab}(s)$ (for any choice of element $s \in S$).

14. SOME EXAMPLES

Example 14.0.1. The symmetric 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 on $\mathbb{F}^n - \{0\}$. 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 (that is, subsets of G of the form Hg) and the stabilizers are trivial.

Since $G = \coprod \mathrm{Orb}(g_i) = \coprod Hg_i$, where the union is over representatives for the orbits, we conclude that $|G| = \sum_i |\mathrm{Orb}(g_i)| = \sum_i |H|/|\mathrm{Stab}(g_i)| = \sum_i |H|$. Therefore, $|H| \mid |G|$ 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 θ 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.

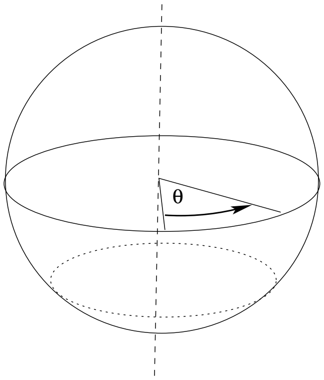


FIGURE 4. Action on the sphere by rotation.

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

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

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 $16 = |D_8|$. 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.

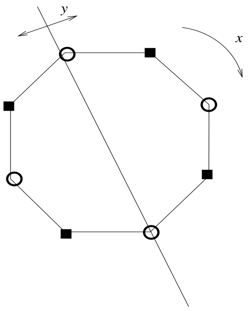


FIGURE 5. A necklace with 4 rubies and 4 sapphires.

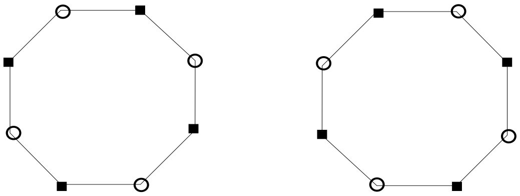


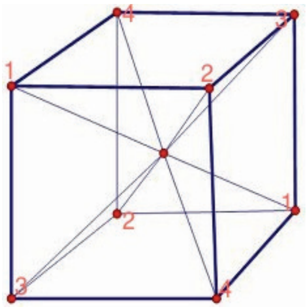
FIGURE 6. The orbit of the necklace.

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

Let's see a clever way to count the number of elements in Γ: It is easy to see that Γ 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 $\sharp\Gamma = 24$.

The action of Γ on the 6 faces of the cube gives a homomorphism $\Gamma \rightarrow S_6$. By considering the action of Γ on two adjacent faces we see that the homomorphism $\Gamma \rightarrow S_6$ must be injective, because if a symmetry preserves two adjacent faces, it must be the trivial symmetry.

We obtain that Γ 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 Γ is a "tiny" subgroup of S_6. So consider the action of Γ on the 4 long diagonals of the cube which we number $\{1, 2, 3, 4\}$. This gives a homomorphism $f \colon \Gamma \rightarrow S_4$.



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, Σ_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. *Giving 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 defines a function $\phi_g \colon A \to A$ by $\phi_g(a) = ga$. We have ϕ_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 ϕ_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 ϕ, define a group action by $g * a := \phi_g(a)$.)

The kernel of this homomorphism consists of the elements g such that ϕ_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 ϕ 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 8.1.5. 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 K.

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 $g * s_1 = s_2$.

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 17.1.3. *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 17.1.4. The symmetry group Γ of the cube acts transitively on the 6 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 17.1.5. 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 K, $\langle(1234)\rangle$, 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 obtained 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 coloured! 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 colours of the elements that belong to one 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 and 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 (or red and blue). 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 $i = 0, \dots, 7$	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 blue).
- 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 blue, 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 blue 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 coloured. There are thus $\binom{4}{2} = 6$ possibilities (Choosing which 2 out of the four cycles would be blue).
- 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 the number of distinct necklaces is

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

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^a has length 3. Such a power of x exists if and only if $3|n$, and then there are precisely two such powers of x in $\langle x\rangle$ (recall our discussion in §4 of cyclic groups – the number of elements of order $d|n$ is $\varphi(d)$). Every such element x^a will have precisely one of its $n/3$ cycles coloured red and we may choose which. Namely, such x^a 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 $3|n$ 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.** [8]

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

[8] Also known as the Hungarian cube.

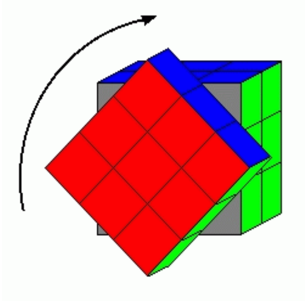


FIGURE 7. The Rubik Cube.

(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 τ 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 τ^{-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 of G – see below – relative to the generators $\{a^{\pm 1}, b^{\pm 1}, c^{\pm 1}, d^{\pm 1}, e^{\pm 1}, f^{\pm 1}\}$? 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.

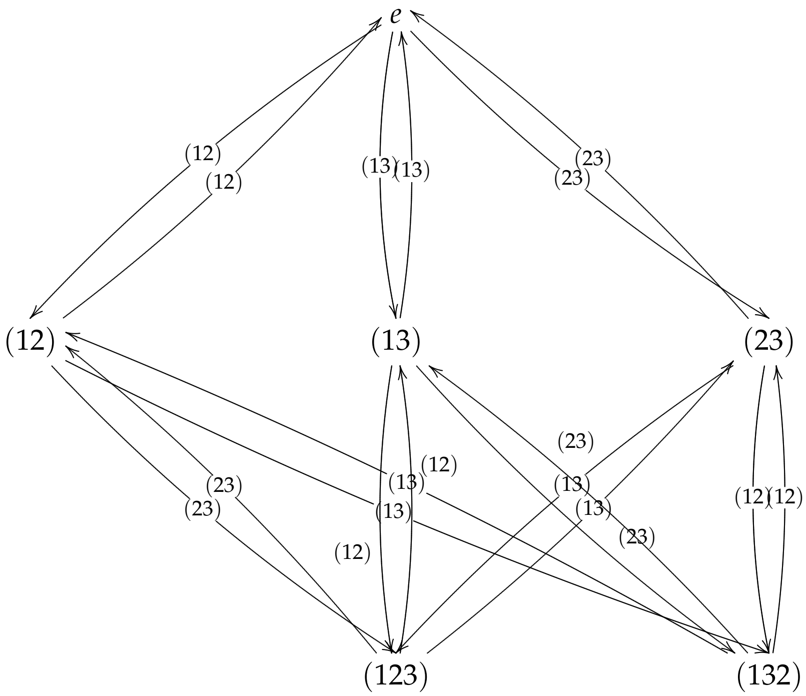
The cube group is a rather complicated subgroup of S_{54}. For example, it has an element of order $1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$. Usually, one denotes the moves not as we did, but by the letters u, d, l, r, f, b for *up, down, left, right, front, back*. The letter u signifies then rotating the upper face 90^0 clockwise if one looks straight at the face. Similarly, r means rotating the right face 90^0 clockwise if one looks straight at the face. In this notation, the element of order 1260 is $ru^2d^{-1}bd^{-1}$. Note that if we enumerated the 54 faces and performed this element we could encode it as a permutation and by decomposing it into a product of disjoint cycles easily check its order.

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_α. 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 gives, in turn, 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 of 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.[9] The actual number is surprisingly close to this simple estimate. It was found that the cube can always be solved by at most 26 moves.

If one adds as generators also $a^2, b^2, c^2, d^2, e^2, f^2$ (corresponding to twisting a "third of the cube" by 180^o) then one can solve every position of the cube by at most 20 moves and, as there are positions that require 20 moves to be solved, this is optimal.

[9] 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 pieces. 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 σ 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** $p(\sigma)$[10] 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 σ.

Lemma 18.0.1. *Two permutations, σ and ρ, are conjugate (namely there is a τ 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

$$\begin{aligned}\sigma &= \sigma_1\sigma_2 \dots \sigma_r \\ &= (i^1_1 \dots i^1_{t(1)})(i^2_1 \dots i^2_{t(2)}) \dots (i^r_1 \dots i^r_{t(r)}),\end{aligned}$$

and

$$\begin{aligned}\rho &= \rho_1\rho_2 \dots \rho_r \\ &= (j^1_1 \dots j^1_{t(1)})(j^2_1 \dots j^2_{t(2)}) \dots (j^r_1 \dots j^r_{t(r)}).\end{aligned}$$

Define τ by

$$\tau(i^a_b) = j^a_b.$$

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.

[10] Another common notation is $\lambda(\sigma)$.

[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 σ and it decomposes into two A_n-conjugacy class if there is no odd permutation commuting with σ. In the latter case, the S_n-conjugacy class of σ is the disjoint union of the A_n-conjugacy class of σ and the A_n-conjugacy class of $\tau\sigma\tau^{-1}$, where τ 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 σ. 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_α is the A_n-conjugacy class of σ_α, 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 σ'_α is another representative for the A_n-conjugacy class of σ_α 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 σ 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 σ. 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 σ 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 σ be a permutation and write σ as a product of disjoint cycles of non-increasing length:*

$$\sigma = c_1 c_2 \cdots c_a = (i^1_1, i^1_2, \dots, i^1_{r_1})(i^2_1, \dots, i^2_{r_2}) \cdots (i^a_1, \dots, i^a_{r_a}).$$

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 σ 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 σ 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 $c_j c_i c_j^{-1} = c_i$ and so

$$c_j \sigma c_j^{-1} = (c_j c_1 c_j^{-1})(c_j c_2 c_j^{-1}) \cdots (c_j c_a c_j^{-1}) = c_1 \cdots c_a = \sigma.$$

Thus, the centralizer of σ 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 $\tau = (i^1_1 i^2_1)(i^1_2 i^2_2) \cdots (i^1_{r_1} i^2_{r_1})$. Then τ is an odd permutation and we find $\tau\sigma\tau^{-1} = \sigma$.

The case left at this point is when σ 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

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

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 τ 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 τ be a permutation commuting with (12345). Then

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

and so τ 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 some i, $1 \leq i \leq n$, 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 σ_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 σ_i is a transposition. Then, if $\sigma = (i_1 i_2)(i_3 i_4)$ then σ 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 $N \supseteq \langle G_1, G_2, \dots, G_n \rangle$. Now, every element in S_n is a product of (usually not disjoint) transpositions and so every element σ in A_n is a product of an even number of transpositions, $\sigma = \lambda_1\mu_1 \dots \lambda_r\mu_r$ (λ_i, μ_i transpositions). Since $n > 4$ every product $\lambda_i\mu_i$ belongs to some G_j and we conclude that $\langle G_1, G_2, \dots, G_n \rangle = A_n$, 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 number of conjugacy classes is called the **class number** of G and will be denoted $h(G)$. 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,

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

The stabilizer of $x \in G$ is $\mathrm{Cent}_G(x) := \{g \in G : gxg^{-1} = x\}$ and so the orbit of x 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 thus 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

$$m \colon X \times X \to X.$$

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 $(n_1, \dots, n_{N-1})$ 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^2.

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 52 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, $gg_1 = g_{i+1}$, $g^2g_1 = gg_{i+1} = g_{2i+1}, \dots, g^pg_1 = \dots = g_{pi+1} = g_1$ (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 that are 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, and additional properties appear in the exercises. Thus, at a (somewhat 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. Sylow's theorem: statement and proof.

Let G be a finite group and let p be a prime dividing its order. Write $|G| = p^rm$, where $(p, m) = 1$. By a p-subgroup of G we mean a subgroup of G 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 $|G| = p^rm$, 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 a subgroup P is conjugate to a subgroup 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

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

As p divides $|G|$ and not $|Z(G)|$, we see that for some $x \notin Z(G)$ we have that p does not divide $\frac{|G|}{|\mathrm{Cent}_G(x)|}$. Thus, p^r divides $\mathrm{Cent}_G(x)$. The subgroup $\mathrm{Cent}_G(x)$ is a *proper* subgroup of G because $x \notin Z(G)$. Thus, by induction, $\mathrm{Cent}_G(x)$, 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, thus 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, $\mathrm{ord}(x) = p^b$ 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 $P \lhd N_G(P)$ 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 p-Sylow 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 $Orb(P_i)$ under Q is $|Q|/|\mathrm{Stab}_Q(P_i)|$. Now $\mathrm{Stab}_Q(P_i) = Q \cap N_G(P_i) = Q \cap P_i$ 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 orbits under Q all having size a proper power of p. Thus, $p|a$. This is a contradiction. □

23.2. **Sylow's theorem: 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 $< 2 >$.

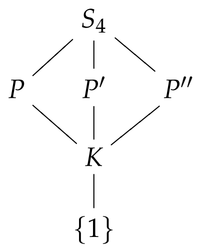
23.2.3. S_3. Consider the symmetric group S_3. Its 2-Sylow subgroups are given by $\{1, (12)\}$, $\{1, (13)\}, \{1, (23)\}$. There are thus three of them and note that indeed $3|m = 3!/2 = 3$ in this case, and $3 \equiv 1 \pmod 2$. The group S_3 has a unique 3-Sylow subgroup $\{1, (123), (132)\}$. This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

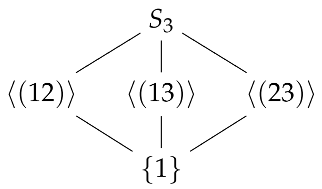
23.2.4. S_4. We want to find the 2-Sylow subgroups. Their number is given by $n_2|3 = 24/8$ and is congruent to 1 modulo 2. It is thus either 1 or 3. Using the expression of a permutation as a product of disjoint cycles, we see that every element of S_4 has order $1, 2, 3$ or 4. The number of elements 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 that 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 Klein group K. We will use that to understand in a different way what are the 2-Sylow subgroups of S_4.

The group K is contained in P and is normal in S_4. Thus, it is also contained in all the conjugates of P; namely, in all the 2-Sylow subgroups. We therefore have the following picture that relates the 2-Sylow subgroups of S_4 to the 2-Sylow subgroups of S_3:





As $S_4/K \cong S_3$, 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 subgroup P, 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. As this is often used, we record this result.

Corollary 23.2.2. *Let $p < q$ be primes such that $p \nmid (q-1)$. Any group of order pq is cyclic and so there is a unique such group up to isomorphism.*

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 to our previous count. Altogether 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 $n_p = 1$; that is, the p-Sylow subgroup is normal.

Remark 23.2.3. A theorem of Burnside states that a group of order p^aq^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.

However, 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 a 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 subgroup has order $q^{(n-1)n/2}$. One such subgroup consists of the upper triangular matrices with 1 on the diagonal (the unipotent group):

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

Note that it follows from Sylow's theorem that any p-group of $\mathrm{GL}_n(\mathbb{F})$ can be conjugated into the unipotent subgroup. See the Exercise 48 for an alternative proof and Exercise 79 for a further discussion 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 $48 = 2^43$, 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 $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ to see that there is more than one 2-Sylow subgroup).

23.2.8. *More examples.*

Example 23.2.4. 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 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 this estimate, 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 1.62×10^{44}. On the other hand, there are precisely 5 groups of order 12 up to isomorphism, so we may conclude that the number of Latin squares arising as multiplication tables is tiny in comparison to 1.62×10^{44} (even taking into account that there are 11! ways to name the elements of a group G of order 12 as $G = \{g_0 = 1, g_1, \dots, g_{11}\}$). 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 by CRT 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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ (again by CRT). 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 four 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, $P \cap (\cup_i Q_i) = \{1\}$. As $G - \cup Q_i$ has 3 elements and P has 4 elements, we must have

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

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 43.

Lemma 23.2.5. *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, τ induces a homomorphism

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

Proof. We will be brief here, as part of it is Exercise 43. 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 τ of the lemma is really $\tau_g|_P$ (the restriction of τ_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 τ 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.

Example 23.2.6. Let d, n be positive integers.

$$\mathrm{Aut}((\mathbb{Z}/n\mathbb{Z})^d) \cong \mathrm{GL}_d(\mathbb{Z}/n\mathbb{Z}) = \{(a_{ij})_{i,j=1}^d : a_{ij} \in \mathbb{Z}/n\mathbb{Z}, \det(a_{ij}) \in \mathbb{Z}/n\mathbb{Z}^\times\}.$$

Let's 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.

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 $P = K$ 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 it T; we will later construct it using the theory of semi-direct product.)

Example 23.2.7. 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

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

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

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

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, on 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, on 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 one usually defines the property of nilpotent completely differently, but it is a theorem that the other (more common) 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 $N \rtimes H$. For illustration, one has the following remarkable theorem:

Theorem 24.1.1 (Schur-Zassenhaus Theorem). *Let G be a finite group with a normal subgroup N such that $\sharp N$ and $\sharp G/N$ are coprime. Then the extension G splits over N ; i.e. there is a subgroup H of G with $G = NH$ and $N \cap H = \{1\}$. Moreover if either N or G/N is a solvable group, then all complements to N in G are G-conjugate.*

The subgroup H is called a **complement** of N; note that it maps isomorphically onto G/N. Using terminology to be introduced later, we conclude that G is a semi-direct product of N and H.

The theorem illustrates well how the Jordan-Hölder philosophy can be realized in practice. Under favourable situations, such as in the theorem above, we can write $G = NH$, where $N \lhd G$ and $H \cap N = \{1\}$. Conjugation by elements of H provide automorphisms of N and they determine G: every element of G has the form hn, $h \in H, n \in N$, and $(h_1n_1)(h_2n_2) = (h_1h_2)((h_2^{-1}n_2h_2)n_1)$. Thus, giving G is equivalent to giving a homomorphism $H \to \mathrm{Aut}(N)$. Those, can be classified once H and N are known.

For example, suppose that the order of G is 420 and we know that the normal subgroup N has 7 elements and that its complement H is simple. From the classification of simple groups (just of order 60, which is not too hard!) we have $H \cong A_5$. Any homomorphism $H \to \mathrm{Aut}(N) = (\mathbb{Z}/7\mathbb{Z})^\times$ must be trivial (consider the kernel and use simplicity). Thus, every such group is isomorphic to $\mathbb{Z}/7\mathbb{Z} \times A_5$.

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

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

[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.

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

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 $H \supset G_i$ 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 $(G_{i-1}/G_i) \rhd H' \rhd \{1\}$, it holds that $G_{i-1} \rhd H \rhd G_i$, 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-Hölder 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

$$\frac{B(B^* \cap A^*)}{B(B^* \cap A)} \cong \frac{A^* \cap B^*}{D}.$$

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 that, 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 $x = b_1c_1$ then $c_1c^{-1} = b_1^{-1}b \in (B^* \cap A^*) \cap B \subset D$. As $D \lhd (B^* \cap A^*)$ and $c_1 \in (B^* \cap A^*)$ also $c^{-1}c_1 \in D$, and so $cD = c_1D$. Next, f is a homomorphism. Suppose that $x = bc, y = b_1c_1$ and so $xy = bcb_1c_1$. Note that $cb_1c^{-1} \in B$ (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 $x = bc \in \operatorname{Ker}(f)$? 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 quotients (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,

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

[13] Our proof follows Rotman's in *An introduction to the theory of groups*.

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 cyclic, 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, note that automatically groups of order p^2 and of order q are abelian.

Example 25.3.5. By Exercise 103, a group of order pqr, where p, q, r are distinct primes, is solvable.

Example 25.3.6. 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 25.3.7. *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. □

Before continuing, it will convenient to introduce some terminology. A sequence of groups and homomorphisms

$$\begin{tikzcd} \cdots \arrow[r] & G_a \arrow[r, "f_a"] & G_{a+1} \arrow[r, "f_{a+1}"] & G_{a+2} \arrow[r, "f_{a+2}"] & \cdots \end{tikzcd}$$

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

$$\begin{tikzcd} 1 \arrow[r] & G_1 \arrow[r, "f"] & G_2 \arrow[r, "g"] & G_3 \arrow[r] & 1 \end{tikzcd},$$

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 25.3.8. *Let*

$$1 \to K \overset{f}{\to} G \overset{g}{\to} H \to 1$$

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

$$J_i = \begin{cases} g^{-1}(H_i), & 0 \leq i \leq n \\ f(K_{i-n}), & n \leq i \leq m+n. \end{cases}.$$

(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:

$$J_{i-1}/J_i \cong \begin{cases} H_{i-1}/H_i, & 0 \leq i \leq n \\ K_{i-n-1}/K_{i-n}, & n < i \leq m+n. \end{cases}.$$

□

Example 25.3.9. *Let G be a group of order $p^a q^b$, where p, q is are distinct primes, a, b positive integers, and $p^a! < p^a q^b$. Then G 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 25.3.10. *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 25.3.8, 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 ≤ 4; every group that can possibly arise as G_f has order less than 60, hence is solvable. On the other hand, one can easily produce 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 25.3.11. Here are two theorems concerning solvable groups. The first is hard, but can be done in a graduate course in algebra; the proof relies on the theory of representation of groups we will begin developing in the last part of the course. The second theorem is among the most difficult proofs in algebra ever written. (Please do not use these theorems in the assignments.)

Theorem 25.3.12 (Burnside). *Let p, q be primes. A finite group of order $p^a q^b$ is solvable.*

Theorem 25.3.13 (Feit-Thompson). *Every finite group of odd order is solvable.*

As an easy consequence of the Feit-Thompson theorem, and a nice application of Cayley's theorem, we prove the following.

Theorem 25.3.14. *Let G be a group whose order is either m, or $2m$, where m is an odd integer. Then G is a solvable group.*

Proof. The Feit-Thompson theorem gives that when the order of G is m. In general, arguing by induction on the order of the group G, it is enough to prove that if G is a simple non-abelian group of even order then $4|\sharp G$. Indeed, this implies that the group G in the theorem statement is not simple and so has a non-trivial normal subgroup K such that the order of K and of G/K are of the same form: either odd integers or twice an odd integer. By induction, K and G/K are solvable, hence so is G.

Suppose then that the order of G is $2m$. We will actually prove that G has a normal subgroup of index 2. Consider the homomorphism

$$f : G \hookrightarrow S_{2m} = \Sigma_G,$$

provided by the action of G on itself by left multiplication. Let $x \in G$ be an element of order 2. We claim that $f(x)$ is an odd permutation. Indeed, $f(x)$ is a product of m transpositions and m is odd. To ease notation, identify G with $f(G)$.

The sign homomorphism $\mathrm{sgn}\colon G \to \{\pm 1\}$ is non-trivial because $x \in G$ is odd. Thus, its kernel $G \cap A_{2m}$ is a normal subgroup of G of index 2. □

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 course 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 later 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 sometimes denoted G_{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 then has the form $a_1x_1 + \cdots + a_rx_r$ 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

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{a_s}\mathbb{Z}.$$

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 distinct primes $p_1, \dots, p_s$ ($s \geq 0$), and for each prime p_a unique integers $0 < b_{a,1} \leq \cdots \leq b_{a,n_a}$, such that*

$$G \cong \mathbb{Z}^r \times \prod_{a=1}^{s} \mathbb{Z}/p_a^{b_{a,1}} \times \cdots \times \mathbb{Z}/p_a^{b_{a,n_a}}.$$

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 $f\colon H \to G$ 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 $f(y_i) = n_ix_i$.*

Example 26.2.5. Let G be a finite abelian p-group, $|G| = p^n$. Then $G \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{a_s}\mathbb{Z}$ for unique a_i satisfying $1 \leq a_1 \leq \cdots \leq a_s$ and $a_1 + \cdots + a_s = n$. 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 often appear 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:

1. $N \lhd G$;
2. $G = NB$;
3. $N \cap B = \{1\}$.

Then we say that G is a **semi-direct product** of N and B.

Note that the conditions imply that every element of G can be written in the form nb, $n \in N, b \in B$ in a *unique* way. Indeed, if $nb = n_1b_1$ then $n_1^{-1} = b_1b^{-1} \in N \cap B$. So $n_1^{-1} = b_1b^{-1} = 1$, giving us $n = n^{-1}, b = b^{-1}$.

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 G, called the **semi-direct product of** N **and** B **relative to** ϕ and denoted

$$G = N \rtimes_\phi B,$$

as follows: as a set $G = N \times B$, but the group law is defined as

$$(n_1, b_1)(n_2, b_2) = (n_1 \cdot \phi_{b_1}(n_2), b_1 b_2).$$

We check associativity:

$$\begin{aligned}[(n_1, b_1)(n_2, b_2)](n_3, b_3) &= (n_1 \cdot \phi_{b_1}(n_2), b_1 b_2)(n_3, b_3) \\ &= (n_1 \cdot \phi_{b_1}(n_2) \cdot \phi_{b_1 b_2}(n_3), b_1 b_2 b_3) \\ &= (n_1 \cdot \phi_{b_1}(n_2 \cdot \phi_{b_2}(n_3)), b_1 b_2 b_3) \\ &= (n_1, b_1)(n_2 \cdot \phi_{b_2}(n_3), b_2 b_3) \\ &= (n_1, b_1)[(n_2, b_2)(n_3, b_3)].\end{aligned}$$

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 easily checked to be group isomorphisms onto their images. We identify N and B with their images $N \times \{1\}, \{1\} \times B$ in G. We claim that G is indeed a semi-direct product of N and B: Clearly the last 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 $(n_1 \cdot \phi_{b_1}(n_2), b_1 b_2) \mapsto n_1 \phi_{b_1}(n_2) b_1 b_2 = n_1 b_1 n_2 b_1^{-1} b_1 b_2 = (n_1 b_1)(n_2 b_2)$. 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 $(n_1 \phi_{b_1}(n_2), b_1 b_2) = (n_1 n_2, b_1 b_2)$. 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, ϕ 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 $\phi_1 = -1$, where by -1 we mean the automorphism of N given by $x^a \mapsto (x^a)^{-1} = x^{-a}$.

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 assume $Q = \mathbb{Z}/q\mathbb{Z}, P = \mathbb{Z}/p\mathbb{Z}$. We prove a lemma that is a bit more general than what we need.

Lemma 27.1.2. $\mathrm{Aut}(\mathbb{Z}/N\mathbb{Z}) = (\mathbb{Z}/N\mathbb{Z})^\times$.

Proof. Let $a \in (\mathbb{Z}/N\mathbb{Z})^\times$. Define a function

$$f_a \colon \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}, \quad f_a(x) = ax.$$

It is easy to check that f is a homomorphism whose image is the cyclic group $\langle a \rangle$, which is equal to $\mathbb{Z}/N\mathbb{Z}$, because a is a generator of $\mathbb{Z}/N\mathbb{Z}$. Since the source and target have the same number of elements, it follow that f_a is injective too, hence $f_a \in \mathrm{Aut}(\mathbb{Z}/N\mathbb{Z})$. Moreover, $f_a \circ f_b = f_{ab}$, because the value on any x is $f_a(f_b(x)) = f_a(bx) = abx = f_{ab}(x)$. That is, we have a group homomorphism

$$f \colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/N\mathbb{Z}), \quad a \mapsto f_a.$$

As $f_a(1) = a$, we can recover a from f_a, showing that f is an injective homomorphism. We claim that f is surjective too, and hence $(\mathbb{Z}/N\mathbb{Z})^\times \cong \mathrm{Aut}(\mathbb{Z}/N\mathbb{Z})$.

Let $\psi \in \mathrm{Aut}(\mathbb{Z}/N\mathbb{Z})$. Let $a = \psi(1)$. Then $\psi(b) = \psi(b \cdot 1) = b\psi(1) = ab$, for any integer b. That is, $\mathrm{Im}(\psi) = \langle a \rangle$. Since ψ is surjective, a must be a generator of $\mathbb{Z}/N\mathbb{Z}$, meaning $a \in (\mathbb{Z}/N\mathbb{Z})^\times$. Now, for every b,

$$f_a(b) = ab = \psi(b),$$

and so $\psi = f_a$. □

We apply the lemma to the group $Q = \mathbb{Z}/q\mathbb{Z}$. 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 $\phi \colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ be the homomorphism determined by $\phi_1 = f_h$ (thus, $\phi_a = f_{ah}$) and let

$$G = Q \rtimes_\phi P.$$

We claim that G is not abelian. Note that

$$(n, 0)(0, b) = (n, b), \quad (0, b)(n, 0) = (\phi_b(n), b).$$

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. Therefore, we constructed a non-abelian group of order pq.

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 $\psi \colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ is a non-trivial homomorphism, else $H = \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and H is abelian. In particular ψ_1 must be an element of order p in $(\mathbb{Z}/q\mathbb{Z})^\times$ and, making use of our knowledge of cyclic groups, we conclude that $\psi_1 = \phi_1^r = \phi_r$ for some r prime to p. This implies the more general relation

$$\psi_a = \phi_{ar}.$$

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 and the homomorphism property follows. 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 52). Since there is always a 3-Sylow, we conclude that G is a semi-direct product $\mathbb{Z}/55\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ and is therefore determined by a homomorphism $\mathbb{Z}/3\mathbb{Z} \rightarrow \mathrm{Aut}(\mathbb{Z}/55\mathbb{Z}) \cong (\mathbb{Z}/55\mathbb{Z})^\times$. The right hand side has order $\varphi(55) = 4 \cdot 10$, which is prime to 3 and so the homomorphism homomorphism $\mathbb{Z}/3\mathbb{Z} \rightarrow \mathrm{Aut}(\mathbb{Z}/55\mathbb{Z}) \cong (\mathbb{Z}/55\mathbb{Z})^\times$ must be trivial (Exercise 36), and G is a direct product. It follows that G must be commutative.

Suppose that G is non-commutative of order 165. The 11-Sylow P is normal because $n_{11}|15, n_{11} \equiv 1 \pmod{11}$ and G has some 5-Sylow Q. Let $N = PQ$, a subgroup of G with 55 elements. It is not abelian, because if it were it would be cyclic and we saw this implies that G is abelian. But such N has order of type pq and so it is unique up to isomorphism.

Since the index of N is the minimal prime dividing the order of the group N is normal. Let B be a 3-Sylow subgroup. Then G is the semidirect product $G = N \rtimes_\phi B$ for some $\phi : B \rightarrow \mathrm{Aut}(N)$.

We claim that ϕ must be trivial. Suppose not, then $\alpha = \phi_1$ is an automorphism of N of order 3. N, being non-abelian has 11 5-Sylow subgroups. If Q is one of them, the $\alpha(Q)$ is another. Thus, α acts on the set of 11 5-Sylow subgroups. By the orbit stabiizer formula, orbits for α have size 1, or 3, and since 11 is not divisible by 3, there is some 11-Sylow subgroup Q' such that $\alpha(Q') = Q'$. Since $Q' \cong \mathbb{Z}/5\mathbb{Z}$ has an automorphism group of size 4 and $\alpha^3 = Id$, $\alpha : Q' \rightarrow Q'$ is trivial. Since P is the unique 11-Sylow subgroup of N, also $\alpha(P) = P$ and for similar reasons $\alpha : P \rightarrow P$ is trivial. Now, every element in N can be written as $xy, x \in Q', y \in P$ and $\alpha(xy) = \alpha(x)\alpha(y) = xy$. Thus, α is trivial. It follows that

$$G \cong \mathbb{Z}/3\mathbb{Z} \times N,$$

where N is the unique up-to-isomorphism non-abelian group of order 55. In particular, G is uniquely determined by its order and being non-commutative. Any commutative group of order 165 will be cyclic, by CRT. We conclude that there are exactly two groups of order 165 up-to-isomorphism.

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 $\phi\colon B \rightarrow \mathrm{Aut}(N)$, $b \mapsto \phi_b$, be a homomorphism and consider the group

$$G = N \rtimes_\phi B.$$

Consider two automorphisms of groups

$$f\colon N \rightarrow N, \quad g\colon B \rightarrow B.$$

Let S be G, considered merely as a set, and consider the bijective self map h defined by

$$h : S \rightarrow S, \quad (n, b) \overset{h}{\mapsto} (f(n), g(b)).$$

We may define a new group law on S by "transport of structure"; that is, let

$$\begin{aligned}(n_1,b_1)*(n_2,b_2) &= h\left[h^{-1}(n_1,b_1)\cdot h^{-1}(n_2,b_2)\right]\\ &= h\left[(f^{-1}(n_1),g^{-1}(b_1))\cdot(f^{-1}(n_2),g^{-1}(b_2))\right]\\ &= h\left[(f^{-1}(n_1)\cdot\phi_{g^{-1}(b_1)}(f^{-1}(n_2)),g^{-1}(b_1)\cdot g^{-1}(b_2))\right]\\ &= (n_1\cdot(f\circ\phi_{g^{-1}(b_1)}\circ f^{-1})(n_2),b_1b_2)\end{aligned}$$

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

$$\psi : B\to \mathrm{Aut}(N), \qquad \psi_b := f\circ\phi_{g^{-1}(b)}\circ f^{-1}.$$

We may view ψ as the composition

$$B \xrightarrow{g^{-1}} B \xrightarrow{\phi} \mathrm{Aut}(N) \xrightarrow{\tau_f} \mathrm{Aut}(N),$$

where τ_f is the conjugation by f automorphism of the group $\mathrm{Aut}(N)$. Thus, ψ 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* $f\in\mathrm{Aut}(N), g\in\mathrm{Aut}(B)$ *and*

$$\psi : B\to \mathrm{Aut}(N), \qquad \psi_b := f\circ\phi_{g(b)}\circ f^{-1}.$$

Then ψ *is a group homomorphism, and we have the isomorphism*

$$N\rtimes_\phi B\cong N\rtimes_\psi B.$$

To illustrate, in the case of groups of order pq we took $f = id$ and we let g vary over all possible automorphisms of $\mathbb{Z}/p\mathbb{Z}$ to see that as g varies the maps ψ 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 $pq, p \leq q$, allow us to determine the following are the only possibilities for the specified orders:

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	$\mathbb{Z}/15\mathbb{Z}$	

Groups of order 8 and 12 require additional analysis.

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 23.2.4. 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 $K = \{1, (12)(34), (13)(24), (14)(23)\}$). 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 $\mathbb{Z}/3\mathbb{Z} \rightarrow \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = \mathrm{GL}_2(\mathbb{F}_2) \cong S_3$ 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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ 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 $\mathbb{Z}/4\mathbb{Z} \rightarrow \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ is uniquely determined.

29. Free groups, generators and relations

Let X be a set. It will be called the **alphabet**. A **word** ω in the **alphabet** X is a finite string $\omega = \omega_1\omega_2 \dots \omega_n$, where each ω_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 ω, σ are **equivalent words** if one can get from one word to the other performing the following basic operations:

Replace $\omega_1 \dots \omega_i x x^{-1} \omega_{i+1} \dots \omega_n$ 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 σ to arrive at an equivalent word σ' 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 $\mathbb{Z} \cong \mathscr{F}(1)$, $\mathbb{Z}/n\mathbb{Z} \cong \langle x_1 | x_1^n \rangle$, $\mathbb{Z}^2 \cong \langle x_1, x_2 | x_1 x_2 x_1^{-1} x_2^{-1} \rangle$, $S_3 \cong \langle x_1, x_2 | x_1^2, x_2^3, (x_1x_2)^2 \rangle$, $D_{2n} \cong \langle x, y | x^n, y^2, xyxy \rangle$. 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 ω and τ 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 ω and τ. Suppose it receives another relative minimum first at σ_r (so the length of σ_{r-1} is bigger than that of σ_r and the length of σ_r is smaller than that of σ_{r+1}. We can take σ_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 α_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 σ and τ 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 σ_0 to σ_a and decreases from σ_a to $\sigma_n = \tau$. Then $\sigma = \tau$.

We view σ and τ as two reduced words obtained by cancellation only from the word σ_a. We argue by induction on the length of σ_a.

If σ_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 σ_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 σ, the other to τ) the first step is to delete the highlighted pair, then using induction for the word σ_a with the highlighted pair deleted, we may conclude that $\sigma = \tau$. If in the cancellation process leading to σ 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 τ. And so, in those cases we return to the previous case. Thus, we may assume that in either the reduction to σ, or the reduction to τ, the highlighted pair is not deleted. Say, in the reduction to σ. How then can σ 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 $\cdots \cancel{d}^{-1}\boxed{\cancel{d}d^{-1}}\cdots$ or $\cdots\boxed{d\cancel{d}^{-1}}\cancel{d}\cdots$. 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 ω 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 $r = \omega_1 \ldots \omega_n$, $\omega_i = x^{\pm 1}$ 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

$$R = \{r = \underline{\omega_1}\ldots\underline{\omega_n} : \text{in the group } G \text{ we have that the product } \omega_1 \cdots \omega_n = 1_G\}.$$

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 $x_1, \ldots, x_d$ 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. **Representations of finite groups**

In this chapter, we only consider finite groups G and finite dimensional complex vector spaces V. The theory of representations of infinite groups and infinite-dimensional representations is vast, and important, but is too advanced for this course. We should mention that even if one is interested in representations of Lie groups such as $\mathrm{GL}_n(\mathbb{C})$ or $U_n(\mathbb{C})$, which arise often in physics, the theory of representations of finite groups plays an important role.

Group representations are intimately related to understanding how groups acts on sets. In our current setting, the set is a complex vector space and the group acts through very particular symmetries – invertible linear transformations. Thus, this topic can be viewed as a natural continuation of our study of groups actions.

Group representations are a subject with many applications to other branches of mathematics, and outside mathematics, for example for computer science, physics, chemistry, and electrical engineering. We will see some of those at the end of this chapter. It is also a topic that is a beautiful marriage of linear algebra and group theory, thus connecting two courses that are usually not taken together.

30. First definitions

A **linear representation** of a (finite) group G is a homomorphism

$$\rho\colon G \to \mathrm{GL}(V) := \{T\colon V \to V : T \text{ is an invertible linear transformation}\},$$

where V is a finite dimensional complex vector space. We will usually drop the adjective "linear". We note that $\mathrm{GL}(V)$ is a group under composition of linear maps. We will denote such a representation by (ρ, V), where the group G is understood from the context. When we feel confident enough, we may just denote it ρ, or V, depending which notation seems more useful at that point.

A very important notion is when are two representations isomorphic. Given two representations (ρ_i, V_i) of G we define

$$\mathrm{Hom}_G(V_1, V_2) = \{T\colon V_1 \to V_2 \text{ linear} : T \circ \rho_1(g) = \rho_2(g) \circ T, \forall g \in G\}.$$

We note that there is no assumption that T is invertible, or even that $\dim(V_1) = \dim(V_2)$; in particular, we always have that the zero map is an element of $\mathrm{Hom}_G(V_1, V_2)$. Further, under addition of linear maps and multiplication by a scalar, $\mathrm{Hom}_G(V_1, V_2)$ is a complex vector space. We shall refer to elements of it as **homomorphisms of representations**, or ***G*-homomorphisms**.

Having made this definition, the notion of an **isomorphism** $(\rho_1, V_1) \cong (\rho_2, V_2)$ is clear: these are linear maps $T \in \mathrm{Hom}_G(V_1, V_2)$ that are invertible. In that case, the inverse map always satisfies $T^{-1} \in \mathrm{Hom}_G(V_2, V_1)$.

Main Goal: Classify representations of G up to isomorphism

(We will make this more precise later on).

Given a representation (ρ, V), *choose* an isomorphism $T\colon V \to \mathbb{C}^n$ ($n = \dim(V)$) and let

$$\tau\colon G \to \mathrm{GL}(\mathbb{C}^n), \quad \tau(g) = T \circ \rho(g) \circ T^{-1}.$$

It is easily verified that

$$(\rho, V) \cong (\tau, \mathbb{C}^n),$$

where the isomorphism is the map T itself. Therefore, every isomorphism class of representations is represented by some $(\tau, \mathbb{C}^n)$.

How unique is τ? It is unique up to conjugation by elements of $\mathrm{GL}(\mathbb{C}^n)$: for any $T_1 \in \mathrm{GL}(\mathbb{C}^n)$ we have

$$\tau \cong \tau_1,$$

where

$$\tau_1(g) = T_1 \circ \tau(g) \circ T_1^{-1}.$$

(this reflects the fact that we had to choose an isomorphism $T\colon V \to \mathbb{C}^n$ and the freedom in this choice is precisely modifying T to $T_1 \circ T$).

It follows that we can make everything more concrete by using the natural identification

$$\mathrm{GL}(\mathbb{C}^n) = \mathrm{GL}_n(\mathbb{C}),$$

obtained by representing any linear transformation T by its matrix $[T]$ relative to the usual basis of $\mathbb{C}^n$. Thus, *we may think about a representation also as a homomorphism*

$$\tau\colon G \to \mathrm{GL}_n(\mathbb{C}).$$

The homomorphism rule is $\tau(xy) = \tau(x)\tau(y)$, where on the right we find matrix multiplication.

When do two such homomorphisms define isomorphic representations? For any invertible matrix $M \in \mathrm{GL}_n(\mathbb{C})$, we have

$$\tau \cong \rho, \qquad \rho(g) = M\tau(g)M^{-1}, \forall g \in G,$$

and conversely. This may be a confusing point, so let's repeat it: we are allowed to choose any matrix $M \in \mathrm{GL}_n(\mathbb{C})$ but, once we made the choice, the relation $\rho(g) = M\tau(g)M^{-1}$ should hold for all $g \in G$, *with the same* M.

Although we have finally arrived at a rather concrete model for representations, the general point of view $\rho\colon G \to \mathrm{GL}(V)$ is very useful as often the vector space V doesn't have a natural basis.

We now come to one of the key notions of this whole subject: the **character of a representation**. Given a representation

$$\rho\colon G \to \mathrm{GL}(V),$$

we define its **character** χ_ρ as follows:

$$\boxed{\chi_\rho\colon G \to \mathbb{C}, \quad \chi_\rho(g) = \mathrm{Tr}(\rho(g)).}$$

It is important to note that χ_ρ is simply a function; it associate to each element g the trace of the linear operator $\rho(g)$. Usually it will not have any multiplicative properties.

The notion of a character will turn out to be central for the whole theory and we will study many properties of characters. For now, we only give a few basic facts.

Lemma 30.0.1. *(1) χ_ρ only depends on the isomorphism class of ρ.*
(2) χ_ρ is constant on conjugacy classes in G.
(3) $\chi(1) = \dim(V)$.

Proof. To calculate the trace of an operator $\rho(g)$ one needs to choose a basis B for V and represent $\rho(g)$ by a matrix $[\rho(g)]_B$. If we choose another basis, say C, then the matrices of $\rho(g)$ in the two bases are related by

$$[\rho(g)]_C = M[\rho(g)]_B M^{-1},$$

where M is the change of basis matrix. Note that if we pass from ρ to an isomorphic representation, say (τ, W),

$$\tau(g) = T\rho(g)T^{-1}$$

then once more

$$[\tau(g)]_C = M[\rho(g)]_B M^{-1},$$

where now C is a basis of W and M is the matrix representing T relative to the two bases B, C. Thus, in both cases, we have to show that

$$\mathrm{Tr}(M[\rho(g)]_B M^{-1}) = \mathrm{Tr}([\rho(g)]_B).$$

This is well known (it follows from the formula $\mathrm{Tr}(MN) = \mathrm{Tr}(NM)$ that one proves by writing down the product of the matrices explicitly and calculating the trace).

The proof that χ_ρ is constant on conjugacy classes is very similar. Relative to some basis B we have

$$\mathrm{Tr}([\rho(hgh^{-1})]_B) = \mathrm{Tr}([\rho(h)\rho(g)\rho(h)^{-1}]_B) = \mathrm{Tr}([\rho(h)]_B[\rho(g)]_B[\rho(h)^{-1}]_B) = \mathrm{Tr}([\rho(g)]_B).$$

Finally, we have $\chi_\rho(1_G) = \mathrm{Tr}(\mathrm{Id}_V) = \mathrm{Tr}(I_{\dim(V)}) = \dim(V)$, where we denote by Id_V the identity operator on V and by I_d the $d \times d$ identity matrix. □

31. Examples

We now discuss some relatively simple examples. Despite appearances, perhaps, they will turn out to be very important and will make frequent appearances. Study them carefully!

31.1. 1-dimensional representations.

A 1-dimensional representation of G could be thought of simply as a homomorphism

$$\rho\colon G \to \mathbb{C}^\times.$$

Indeed, $\mathrm{GL}_1(\mathbb{C}^\times) = \mathbb{C}^\times$. Note that in this case if $\rho \cong \tau$ then, since $\mathbb{C}^\times$ is commutative, we actually have $\rho = \tau$. Also, since the trace of a 1×1 matrix is (α) is just α it follows that

$$\chi_\rho = \rho.$$

For these reasons, 1-dimensional representations are also called **1-dimensional characters**, or **multiplicative characters** .

Let

$$G^* = \mathrm{Hom}(G, \mathbb{C}^\times).$$

We make two observations: First, G^* is a group under the rule

$$(\rho \cdot \tau)(g) = \rho(g) \cdot \tau(g).$$

Second, if we let $S^1 = \{z \in \mathbb{C}^\times : |z| = 1\}$ denote the unit circle in $\mathbb{C}$ then

$$G^* = \mathrm{Hom}(G, S^1).$$

Indeed, if $g \in G$ is of order d, $\rho \in G^*$, then $\rho(g)^d = \rho(1_G) = 1$ which implies that $\rho(g)$ is necessarily a root of unity. The group G^* is called the **character group** of G.

Lemma 31.1.1. *There is a natural isomorphism*

$$G^* \cong (G^{ab})^*,$$

where, as usual, $G^{ab} = G/G'$ is the abelianization of G.

Proof. We have seen that any homomorphism $G \to A$, where A is an abelian group, factors uniquely through G^{ab} (see 8.1.10). In particular, given any homomorphism $f\colon G \to \mathbb{C}^\times$ there is a unique homomorphism $F\colon G^{ab} \to \mathbb{C}^\times$ such that the following diagram commutes (π being the natural map $G \to G/G'$):

$$\begin{tikzcd}
G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & \mathbb{C}^\times , \\
& G^{ab} \arrow[ur, "F"'] &
\end{tikzcd}$$

and conversely. □

We will revisit this example later on. We will rely on Exercise 117 that you are encouraged to do at this point.

Example 31.1.2. The alternating groups A_n for $n \geq 5$ have only one 1-dimensional representation, which is the trivial representation $\mathbb{1}$. For any group G the **trivial representation** $\mathbb{1}$ is the 1-dimensional representation

$$G \to \mathbb{C}^\times, \quad g \mapsto 1, \forall g \in G.$$

Its character, also denoted $\mathbb{1}$, is the constant function 1.

The symmetric groups S_n, for $n \geq 5$, have only two 1-dimensional characters, $\mathbb{1}$ and sgn. Indeed, the only non-trivial normal subgroup of S_n, for $n \geq 5$, is A_n and, as $S_n/A_n \cong \{\pm 1\}$ is abelian, it must be that $S_n^{ab} \cong \{\pm 1\}$. The group $\{\pm 1\}$ has precisely two homomorphisms to $\mathbb{C}^\times$, the trivial one and the inclusion.

Example 31.1.3. The commutator subgroup of D_4 is $\{1, x^2\}$. Indeed, $[x,y] = x^2$ and so the commutator subgroup contains $\langle x^2 \rangle$. On the other hand, x^2 commutes with x and y and is therefore a central element and thus $\langle x^2 \rangle$ is a normal subgroup. As $D_4/\langle x^2 \rangle$ has order 2^2 it is abelian and it follows that $\langle x^2 \rangle \supseteq D_4'$ and we get equality: $D_4' = \langle x^2 \rangle$. We think about the abelianization as

$$D_4^{ab} = \{1, \bar{x}, \bar{y}, \overline{xy}\}$$

with $\bar{x}\bar{y} = \bar{y}\bar{x}$ and the square of every element is 1; it is a group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. As every element has order 2, every multiplicative character of D_4^{ab} takes values in $\{\pm 1\}$. It is not hard to show that there are 4 possibilities as described in the following table.

	1	$\bar{x}$	$\bar{y}$	$\overline{xy}$
$\rho_1 = \mathbb{1}$	1	1	1	1
ρ_2	1	-1	1	-1
ρ_3	1	1	-1	-1
ρ_4	1	-1	-1	1

31.2. **The regular representation ρ^{reg}.** Let G be a group. We define a vector space V with a basis $\{e_g : g \in G\}$. Often V is called the **group ring** of G and denoted $\mathbb{C}[G]$. A vector in V is a sum

$$\sum_{g \in G} a_g \cdot e_g,$$

with a_g complex numbers. We can also think about V as the collection of formal sums

$$\{\sum_{g \in G} a_g \cdot [g] : a_g \in \mathbb{C}\}.$$

The two notations are equivalent – the symbol $[g]$ corresponds to the notation e_g. In the second notation, we can see that $\mathbb{C}[G]$ has a ring structure, where

$$(\sum_{g\in G} a_g \cdot [g]) + (\sum_{g\in G} b_g \cdot [g]) = \sum_{g\in G}(a_g + b_g)\cdot [g],$$

and

$$(\sum_{g\in G} a_g \cdot [g])(\sum_{g\in G} b_g \cdot [g]) = \sum_{g\in G}(\sum_{s\in G} a_{gs^{-1}}b_s)\cdot [g].$$

However, the ring structure will not be important until much later.

The group G acts on this vector space and this representation is called the **regular representation** and denoted ρ^{reg}. We have

$$\rho^{reg}\colon G \to \mathrm{GL}(V), \qquad \rho^{reg}(g)(e_s) = e_{gs}, \;\; \forall g,s \in G.$$

In the other notation,

$$\rho^{reg}(g)(\sum_{s\in G} a_s[s]) = [g](\sum_{s\in G} a_s[s]) = \sum_{s\in G} a_s[gs].$$

The character χ^{reg} of ρ^{reg} is very simple:

$$\chi^{reg}(g) = \begin{cases} \sharp G, & g = 1_g; \\ 0, & else. \end{cases} \tag{4}$$

The proof is not hard: if $\{e_1, \dots, e_n\}$ is a basis for a vector space W, and $T\colon W \to W$ is a linear transformation, write

$$T(e_i) = \sum_{a=1}^{n} b_a e_a, \;\; b_a \in \mathbb{C}.$$

Then the contribution to $\mathrm{Tr}(T)$ from the vector e_i is b_i. Now, to calculate $\mathrm{Tr}(\rho^{reg}(g))$ we see that the contribution from the vector e_s is the coefficient of e_s in $\rho^{reg}(g)(e_s)$. As $\rho^{reg}(g)(e_s) = e_{gs}$, this contribution is 0 from *every* s if $g \neq 1$, and is 1 from *every* s if $g = 1$.

31.3. **Direct sum.** Let $(\rho_1, V_1), (\rho_2, V_2)$ be two representations of the group G. We define the **direct sum** of the representations: the vector space is $V_1 \oplus V_2$ and the representation $\rho_1 \oplus \rho_2$ is as follows:

$$\rho_1 \oplus \rho_2\colon G \to \mathrm{GL}(V_1 \oplus V_2), \quad (\rho_1 \oplus \rho_2)(g)(v_1, v_2) := (\rho_1(g)(v_1), \rho_2(g)(v_2)).$$

If we represent ρ_i as homomorphisms,

$$\rho_i\colon G \to \mathrm{GL}_{n_i}(\mathbb{C}) \quad (n_i = \dim(V_i)),$$

then

$$\rho_1 \oplus \rho_2\colon G \to \mathrm{GL}_{n_1+n_2}(\mathbb{C}), \quad (\rho_1 \oplus \rho_2)(g) = \begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix}.$$

This is a block diagonal matrix with the matrices $\rho_1(g), \rho_2(g)$ on the diagonal. It is then clear that

$$\chi_{\rho_1 \oplus \rho_2}(g) = \chi_{\rho_1}(g) + \chi_{\rho_2}(g).$$

32. Subrepresentations and irreducible representations

32.1. **Subrepresentions.** Let (ρ, V) be a representation of G. Let $U \subseteq V$ be a subspace such that

$$\rho(g)(u) \in U, \quad \forall g \in G, \forall u \in U.$$

That is, U is invariant under all the linear maps $\{\rho(g) : g \in G\}$. Then U is called a **subrepresentation** of V; we have

$$\rho|_U \colon G \to \mathrm{GL}(U), \quad \rho|_U(g) := \rho(g)|_U.$$

Example 32.1.1. $\{0\}$ and V are always sub-representations. We refer to them as **trivial subrepresentations.**

Example 32.1.2. The **standard representation** ρ^{std} of S_n.

Let $n \geq 2$. We consider S_n as contained in $\mathrm{GL}_n(\mathbb{C})$ in such a way that

$$\sigma(e_i) = e_{\sigma(i)}, \quad i = 1, 2, \ldots, n.$$

This is called the standard n-dimensional representation of S_n. For example, for $n = 3$,

$$(12) \leftrightarrow \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (123) \leftrightarrow \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Let χ^{std} be the character of ρ^{std}. In our example of $n = 3$ we have $\chi^{std}(12) = 1, \chi^{std}(123) = 0$.

Proposition 32.1.3. *We have*

$$\chi^{std}(\sigma) = \sharp \text{ fixed points of } \sigma. \tag{5}$$

Proof. The contribution to $\mathrm{Tr}(\rho^{std}(\sigma))$ coming from the basis vector e_i is the coefficient of e_i in $\rho^{std}(\sigma)(e_i) = e_{\sigma(i)}$, which is 1 if $\sigma(i) = i$ and 0 if $\sigma(i) \neq i$. Summing over all i, we find the statement in the proposition. □

Consider now the subspaces

$$U_1 := \{(a, \ldots, a) : a \in \mathbb{C}\},$$

and

$$U_0 := \{(x_1, \ldots, x_n) : \sum_{i=1}^{n} x_i = 0, x_i \in \mathbb{C}\}.$$

The space U_1 is just the trivial representation $\mathbb{1}$ of S_n, and U_0 is also a representation of S_n that we denote $\rho^{std,0}$. As $\dim(U_1) + \dim(U_0) = n$ and $U_1 \cap U_0 = \{0\}$, we find:

$$\rho^{std} = \mathbb{1} \oplus \rho^{std,0}. \tag{6}$$

32.2. **Irreducible representations and Maschke's Theorem.** A representation (ρ, V) of G is called **irreducible** if its only subrepresentations are $\{0\}$ and V, and $V \neq 0$.

Proposition 32.2.1. *The representations $\mathbb{1}$ and $\rho^{std,0}$ are irreducible representations of S_n. Thus, we have a decomposition of ρ^{std} as a sum of irreducible representations.*

Proof. Clearly $\mathbb{1}$ is irreducible for dimension reasons – there aren't any non-trivial subspaces; this is true for any group G and any 1-dimensional representation of it.

The proof for U_0 is slightly involved; we will give another proof later, much more elegant, as an application of character theory.

We assume that $n > 2$. 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'. 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). □

Theorem 32.2.2 (Maschke)**.** *Every non-zero representation (ρ, V) decomposes as a direct sum of irreducible representations.*

Remark 32.2.3. We will later prove that such a direct sum decomposition is unique, up to isomorphism and re-ordering of the summands. We can now make our goal in this chapter more precise:

Main Goal: Classify the irreducible representations of a group G. Find effective methods to determine the decomposition of a representation into irreducible representations.

Proof. (Maschke's Theorem) We begin with a lemma that shows that we can always define an inner product of V relative to which $\rho(g)$ is a unitary matrix for any $g \in G$.

Lemma 32.2.4. *There is an inner product*

$$\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C},$$

such that

$$\langle gv, gu \rangle = \langle v, u \rangle, \quad \forall g \in G, \forall u, v \in V.$$

(To simplify notation we write gv for $\rho(g)(v)$.)

Proof. (Lemma) Let $(\cdot, \cdot)$ be *any* inner product on V. Define,

$$\langle v, u \rangle = \frac{1}{\sharp G} \sum_{g \in G} (gv, gu).$$

The verification that this is an inner product is straightforward and we omit it. To check that ρ is a unitary representation relative to this inner product we calculate:

$$\begin{aligned}\langle gv, gu\rangle &= \frac{1}{\sharp G}\sum_{h\in G}(hgv, hgu)\\ &= \frac{1}{\sharp G}\sum_{h\in G}(hv, hu)\\ &= \langle v, u\rangle,\end{aligned}$$

where we used that when h runs over G so does hg. □

We now get to the proof of the theorem. We prove it by induction on $\dim(V)$.

If $\dim(V) = 1$ then V is irreducible and there is nothing to prove. In general, if V is irreducible there is nothing to prove. Otherwise, V has a subrepresentation $0 \neq U \neq V$. Let $\langle v, u\rangle$ be a G-invariant inner product on V, as in the Lemma. Then

$$V = U \oplus U^\perp.$$

We only need to show that

$$U^\perp := \{v \in V : \langle v, u\rangle = 0, \forall u \in U\}$$

is a subrepresentation. Let $g \in G$ and $v \in U^\perp$. For any $u \in U$ we have

$$\langle gv, u\rangle = \langle v, g^{-1}u\rangle = 0,$$

because $g^{-1}u \in U$ as U is a subrepresentation. It follows that $gv \in U^\perp$.

By induction,

$$U = W_1 \oplus \cdots \oplus W_a, \quad U^\perp = W_{a+1} \oplus \cdots \oplus W_b,$$

for some irreducible representations W_i of G. Then,

$$V = U \oplus U^\perp = W_1 \oplus \cdots \oplus W_b$$

is a sum of irreducible representations too. □

32.3. **The projection on V^G.** Let (ρ, V) be a representation of G. Let

$$V^G = \{v \in V : \rho(g)(v) = v, \forall g \in G\}.$$

Then V^G is a subrepresentation on which G acts trivially. It's the space of **invariant vectors**.

Lemma 32.3.1. *Let*

$$\pi(v) = \frac{1}{\sharp G}\sum_{g\in G}\rho(g)(v). \tag{7}$$

Then $\pi \in \mathrm{Hom}_G(V, V^G)$ and is a projection on the subspace V^G.

Proof. As π is a sum of linear maps it is certainly a linear map from V to V. We first show that $\mathrm{Im}(\pi) \subseteq V^G$. We need to show that all $h \in G, v \in V$ we have $\rho(h)(\pi(v)) = \pi(v)$. Indeed, $\rho(h)(\pi(v)) = \frac{1}{\sharp G}\sum_g(\rho(h)\circ\rho(g))(v) = \frac{1}{\sharp G}\sum_g \rho(hg)(v) = \frac{1}{\sharp G}\sum_g \rho(g)(v) = \pi(v)$.

To show π is a projection, we need to verify that π is the identity on V^G. But, for $v \in V^G$ we have $\pi(v) = \frac{1}{\sharp G}\sum_g \rho(g)(v) = \frac{1}{\sharp G}\sum_g v = v$.

Finally, we check that π is a homomorphism of representations. As G acts trivially on V^G this boils down to verifying that $\pi(\rho(h)v) = \pi(v)$. We calculate: $\pi(\rho(h)(v)) = \frac{1}{\sharp G}\sum_g \rho(g)(\rho(h)v) = \frac{1}{\sharp G}\sum_g \rho(gh)(v) = \frac{1}{\sharp G}\sum_g \rho(g)(v) = \pi(v)$. □

The following corollary will be used several times in the sequel:

Corollary 32.3.2 (Projection Formula)**.** *We have*

$$\dim(V^G) = \frac{1}{\sharp G}\sum_g \chi_\rho(g). \tag{8}$$

In words, the dimension of the subspace of invariant vectors is the average value of the character χ_ρ.

Proof. We have a decomposition,

$$V = V^G \oplus \mathrm{Ker}(\pi).$$

In this decomposition we can write

$$\pi = \mathrm{Id}_{V^G} \oplus 0.$$

Thus, $\mathrm{Tr}(\pi) = \dim(V^G)$. But on the other hand,

$$\mathrm{Tr}(\pi) = \frac{1}{\sharp G}\sum_g \mathrm{Tr}(\rho(g)) = \frac{1}{\sharp G}\sum_g \chi_\rho(g).$$

□

Example 32.3.3. The action of S_3 on itself by multiplication from the left, as in Cayley's Theorem 15.0.1, provides us with an embedding $S_3 \hookrightarrow S_6$. Composing with the standard representation of S_6 we get a 6-dimensional representation ρ of S_3. Does this representation have fixed vectors? what is the dimension of the space of fixed vectors??

If we enumerate the elements of S_3 as $\{1, (12), (13), (132), (23), (123)\} = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$, then

$$\rho((12)) = \begin{pmatrix} 0&1&0&0&0&0\\ 1&0&0&0&0&0\\ 0&0&0&1&0&0\\ 0&0&1&0&0&0\\ 0&0&0&0&0&1\\ 0&0&0&0&1&0 \end{pmatrix}, \qquad \rho((123)) = \begin{pmatrix} 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&1&0&0&0&0\\ 0&0&0&0&0&1\\ 0&0&1&0&0&0\\ 1&0&0&0&0&0 \end{pmatrix}.$$

(For example, $(12) \in S_3$ takes to σ_1 to σ_2, σ_2 to σ_1, σ_3 to σ_4, etc. and so corresponds to the permutation $(12)(34)(56) \in S_6$.)

If χ denotes the character of ρ, then by calculating χ on $1, (12)$ and (123) we would know its value on any $\sigma \in S_3$, because a character has a fixed value on each congruence class. We find

$$\chi(1) = 6, \quad \chi((ij)) = 0, \quad \chi((ijk)) = 0.$$

It follows from Corollary 32.3.2 that the dimension of the space of invariant vectors is 1.

Finally, note that we could have found the values of χ without writing down the matrices. Just by observation we could say that any non-identity element of S_3 is mapped to a permutation in S_6 that has no fixed points (that would be true for any group!). As for $\sigma \in S_6$, the value of $\chi^{std}(\sigma) = \sharp(\text{fixed points of } \sigma)$, it follows that $\chi(\tau) = 0$ for any $\tau \in S_3$.

Example 32.3.4. Let $(\rho, V) = (\rho^{std}, \mathbb{C}^n)$ be the standard representation. Then

$$\pi = \frac{1}{n!}\sum_{\sigma\in S_n} \rho^{std}(\sigma).$$

One checks that $V^G = U_1$ and $\mathrm{Ker}(\pi) = U_0$ (for the latter, it is easier to show $\mathrm{Ker}(\pi) \supseteq U_0$ and deduce equality by comparing dimensions). We find again the decomposition (6):

$$\rho^{std} = \mathbb{1} \oplus \rho^{std,0}.$$

Moreover, we find that

$$1 = \dim(U_1) = \dim(V^G) = \frac{1}{n!}\sum_{\sigma\in S_n} \sharp \text{ fixed points of } \sigma,$$

a formula one can also derive from the Cauchy-Frobenius formula.

33. Schur's lemma and orthogonality of characters

33.1. **The dual representation and the two Homs.** Let (ρ, V) be a representation of G. For any linear operator $\rho(g)\colon V \to V$ we have the dual operator $\rho(g)^t\colon V^* \to V^*$, where $V^* = \mathrm{Hom}(V, \mathbb{C})$ is the dual vector space to V. Recall that $\rho(g)^t$ is defined by

$$\rho(g)^t(\phi) = \phi \circ \rho(g), \quad \phi \in V^*.$$

Further, if $\{e_1, \dots, e_n\}$ are a basis for V and $\{\phi_1, \dots, \phi_n\}$ is the dual basis for V (the basis that satisfies $\phi_i(e_j) = \delta_{ij}$) then in terms of matrices we have

$$[\rho(g)^t]_{\{\phi_i\}} = ([\rho(g)]_{\{e_i\}})^t.$$

Define the **dual representation** ρ^*

$$\rho^*\colon G \to \mathrm{GL}(V^*), \quad \rho^*(g) = (\rho(g^{-1}))^t.$$

Proposition 33.1.1. *ρ^* is a representation of G and its character satisfies $\chi_{\rho^*} = \bar{\chi}_\rho$. That is,*

$$\chi_{\rho^*}(g) = \overline{\chi}_\rho(g) := \overline{\chi_\rho(g)}, \ \forall g \in G.$$

Proof. The proof is easy, but reveals two properties that are very important, and general, and so we record them here as a lemma.

Lemma 33.1.2. *Let (ρ, V) be a representation of G. Then:*

(1) Every $\rho(g)$ is diagonalizable.

(2) Every eigenvalue of $\rho(g)$ is a root of unity of order dividing d, where d is the order of g in G.

Proof. Let d be the order of g. As ρ is a homomorphism $\rho(g)^d = \rho(g^d) = \rho(1_G) = \mathrm{Id}_V$. It follows that $\rho(g)$ solves the polynomial $x^d - 1$, which is a separable polynomial (i.e., it has distinct roots over $\mathbb{C}$). Therefore, also the minimal polynomial of $\rho(g)$ is a separable polynomial and, consequently, $\rho(g)$ is diagonalizable. Let's write

$$\rho(g) \sim \mathrm{diag}(\alpha_1, \dots, \alpha_n),$$

where $n = \dim(V)$ and α_i are d-th roots of unity. □

Note that in general the basis in which $\rho(g)$ is diagonal depends on g; we cannot, in general, diagonalize all $\rho(g)$ simultaneously. However, $\rho(g^{-1}) = \rho(g)^{-1}$ is given in the same basis by

$$\mathrm{diag}(\alpha_1^{-1}, \dots, \alpha_n^{-1}) = \mathrm{diag}(\overline{\alpha_1}, \dots, \overline{\alpha_n}),$$

because the α_i are roots of unity. Thus,

$$\chi_\rho(g^{-1}) = \sum_i \overline{\alpha_i} = \overline{\chi_\rho(g)}. \tag{9}$$

To finish the proof of the Proposition it only remains to check that ρ^* is a representation. We have:

$$\rho^*(gh) = (\rho(gh)^{-1})^t = (\rho(h^{-1})\rho(g^{-1}))^t = (\rho(g^{-1}))^t \cdot (\rho(h^{-1}))^t = \rho^*(g) \cdot \rho^*(h).$$

□

We now discuss "the two Homs" and engage in a very technical calculation. However, the results will be absolutely essential to proving one of the most important theorems concerning representations: orthogonality of characters.

Let $(\rho, V), (\tau, W)$ be two representations of the group G. We have already defined (all maps appearing below are understood to be linear)

$$\mathrm{Hom}_G(V, W) = \{T\colon V \to W : T \circ \rho(g) = \tau(g) \circ T, \forall g \in G\}.$$

We also have the more naive

$$\mathrm{Hom}(V, W) = \{T : V \to W\}.$$

Proposition 33.1.3. $\mathrm{Hom}(V, W)$ *is a linear representation* σ *of* G*, where*

$$\sigma(g)(T) = \tau(g) \circ T \circ \rho(g)^{-1}, \quad T \in \mathrm{Hom}(V, W).$$

Remark 33.1.4. Note the following:

(1) $\dim(\mathrm{Hom}(V, W)) = \dim(V) \cdot \dim(W)$. This can be seen by choosing bases for the two vector spaces and representing the linear maps as matrices. See also the proof for the character formula below.

(2) We have the following relationship between the two Homs:
$$\mathrm{Hom}_G(V, W) = \mathrm{Hom}(V, W)^G.$$

(3) Consider the special case where $(\tau, W) = (\mathbb{1}, \mathbb{C})$. In this case
$$\mathrm{Hom}(V, W) = V^*,$$
and the new representation σ we have now defined on it is:
$$\sigma(g)(\phi) = \tau(g) \circ \phi \circ \rho(g^{-1}) = \phi \circ \rho(g^{-1}) = \rho(g^{-1})^t(\phi) = \rho^*(\phi).$$
Namely, we just get the dual representation again.

Proof. 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 from the vector space $\mathrm{Hom}(V, W)$ to itself.
- 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 $\sigma(g) \circ \sigma(g^{-1}) = \sigma(1) = \mathrm{Id}$, etc.). Thus, it follows that we get a homomorphism
$$\sigma : G \to \mathrm{GL}(\mathrm{Hom}(V, W)).$$

□

Theorem 33.1.5. *The character* χ_σ *of the representation* $(\sigma, \mathrm{Hom}(V, W))$ *is given by the formula*

$$\chi_\sigma = \chi_\tau \cdot \bar{\chi}_\rho.$$

Proof. We first find a convenient basis for $\mathrm{Hom}(V, W)$. Let

$$\mathscr{B} = \{e_1, \dots, e_n\}, \quad \mathscr{C} = \{f_1, \dots, f_m\},$$

be bases for V and W, respectively. Let

$$\mathscr{B}^* = \{e_1^*, \dots, e_n^*\},$$

be the dual basis for V^*. So, $e_i^*(e_j) = \delta_{ij}$ (Kronecker's delta).

We introduce the following notation: for $\phi \in V^*$ and $w \in W$, we let the symbol[15]

$$\phi \otimes w$$

[15] The choice of notation is not accidental. There is a theory of tensor products that operates in the background, but we will not discuss it in this course.

denote the element of $\mathrm{Hom}(V, W)$ given by

$$v \mapsto \phi(v) \cdot w.$$

We quickly check that it is indeed a linear map: We have $(\phi \otimes w)(\alpha_1 v_1 + \alpha_2 v_2) = \phi(\alpha_1 v_1 + \alpha_2 v_2) \cdot w = (\alpha_1 \phi(v_1) + \alpha_2 \phi(v_2)) \cdot w = \alpha_1 \phi(v_1) \cdot w + \alpha_2 \phi(v_2) \cdot w = \alpha_1 \cdot (\phi \otimes w)(v_1) + \alpha_2 \cdot (\phi \otimes w)(v_2)$.

In particular, we have the maps $e_i^* \otimes f_j$. It turns out that these maps have very simple representation as matrices. Using the bases $\mathscr{B}, \mathscr{C}$, we have an identification

$$\mathrm{Hom}(V, W) \cong M_{m\times n}(\mathbb{C}),$$

by sending any linear transformation to its matrix representation relative to these bases. Since we have $(e_i^* \otimes f_j)(e_\ell) = \delta_{i\ell} f_j$, it follows that $e_i^* \otimes f_j$ is represented by the elementary matrix E_{ij} that has all entries equal to zero, except for the ij entry that is equal to 1:

$$e_i^* \otimes f_j \leftrightarrow E_{ij}.$$

As every matrix $(m_{ij}) \in M_{m\times n}(\mathbb{C}) \cong \mathrm{Hom}(V, W)$ is equal to $\sum_{ij} m_{ij} E_{ij}$, we find:

<u>Conclusion:</u> $\{e_i^* \otimes f_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis for $\mathrm{Hom}(V, W)$.

We can calculate $\mathrm{Tr}(\sigma(g))$ by finding the action of $\sigma(g)$ on this basis. Let us introduce notation:

$$\tau(g) = (h_{ij})_{i,j=1}^m, \quad \rho(g^{-1}) = (g_{ij})_{i,j=1}^n.$$

Then,

$$\sigma(g)(e_j^* \otimes f_i) = (h_{ij})E_{ij}(g_{ij}) = \begin{pmatrix} h_{11} & \dots & h_{1m} \\ \dots & \dots & \dots \\ h_{m1} & \dots & h_{mm} \end{pmatrix} \begin{pmatrix} 0 & \dots & 0 \\ g_{j1} & \dots & g_{jn} \\ 0 & \dots & 0 \end{pmatrix} = (r_{ab}).$$

The matrix on the right has all entries equal to zero except for its i-th row, which is equal to $(g_{j1}, g_{j2}, \dots, g_{jn})$. The result is a matrix (r_{ab}) whose ab entry is

$$r_{ab} = h_{ai} g_{jb}.$$

In particular,

$$r_{ij} = h_{ii} g_{jj}.$$

Namely, we have

$$\sigma(g)(E_{ij}) = \sum_{a,b} h_{ai} g_{jb} E_{ab}.$$

The contribution to the trace of $\sigma(g)$ coming from the basis vector $e_j^* \otimes f_i = E_{ij}$ is $h_{ii} g_{jj}$. Thus,

$$\mathrm{Tr}(\sigma(g)) = \sum_{i,j} h_{ii} g_{jj} = (\sum_i h_{ii})(\sum_j g_{jj}) = \mathrm{Tr}(\tau(g)) \cdot \mathrm{Tr}(\rho(g^{-1})).$$

But, we have seen that $\mathrm{Tr}(\rho(g^{-1})) = \chi_\rho(g^{-1}) = \overline{\chi_\rho}(g)$. Therefore, we conclude that

$$\chi_\sigma = \chi_\tau \cdot \bar{\chi}_\rho.$$

□

33.2. **Schur's Lemma.** Before proving Schur's lemma, we establish some general properties of homomorphisms of representations.

Lemma 33.2.1. *For any two representations $(\rho, V), (\tau, W)$ of G and any $T \in \mathrm{Hom}_G(V, W)$ we have that $\mathrm{Ker}(T)$ is a subrepresentation of V, and $\mathrm{Im}(T)$ is a subrepresentation of W.*

Proof. Let $v \in \mathrm{Ker}(T)$ and $g \in G$. We have

$$T(\rho(g)(v)) = \tau(g)(T(v)) = \tau(g)(0) = 0.$$

It follows that $\mathrm{Ker}(T)$ is a subrepresentation of V.

Let $w \in \mathrm{Im}(T)$ and choose $v \in V$ such that $T(v) = w$. Then:

$$\tau(g)(w) = \tau(g)(T(v)) = T(\rho(g)(v)) \in \mathrm{Im}(T).$$

It follows that $\mathrm{Im}(T)$ is a subrepresentation of W. □

Lemma 33.2.2 (Schur)**.** *Let $(\rho, V), (\tau, W)$ be two irreducible representations of G. Then*

$$\mathrm{Hom}_G(V, W) \cong \begin{cases} \mathbb{C}, & (\rho, V) \cong (\tau, W); \\ 0, & \textit{else}. \end{cases} \tag{10}$$

Proof. Let $T \in \mathrm{Hom}_G(V, W)$ and suppose $T \neq 0$. Then $\mathrm{Ker}(T) \neq V$. However, $\mathrm{Ker}(T)$ is a subrepresentation of V and V is irreducible. It follows that $\mathrm{Ker}(T) = 0$ and so that T is injective. Since V is not zero (by definition), $\mathrm{Im}(T) \neq 0$ and since W is irreducible, and $\mathrm{Im}(T)$ is a subrepresentation, $\mathrm{Im}(T) = W$. Thus, T is surjective. It follows that T is an isomorphism. Therefore, if $\mathrm{Hom}_G(V, W) \neq 0$ (and V, W are irreducible) we have $(\rho, V) \cong (\tau, W)$.

It remains to show that if $(\rho, V) \cong (\tau, W)$ then $\mathrm{Hom}_G(V, W)$ is a 1-dimensional vector space. Choose, any non-zero $T \in \mathrm{Hom}_G(V, W)$. We saw that T is then an isomorphism. We get an isomorphism

$$\mathrm{Hom}_G(V, W) \cong \mathrm{End}_G(V), \quad S \mapsto T^{-1} \circ S,$$

and thus it is enough to prove that

$$\mathrm{End}_G(V) \cong \mathbb{C}.$$

Let then $R \in \mathrm{End}_G(V)$ and let λ be an eigenvalue of R. As $\lambda \cdot \mathrm{Id} \in \mathrm{End}_G(V)$, it follows that $R - \lambda \cdot \mathrm{Id} \in \mathrm{End}_G(V)$ and it follows that $\mathrm{Ker}(R - \lambda \cdot \mathrm{Id})$ is a subrepresentation of V. Since every eigenvalue has at least one non-zero eigenvector, we have that $\mathrm{Ker}(R - \lambda \cdot \mathrm{Id}) \neq 0$ and, as V is irreducible, we must have

$$\mathrm{Ker}(R - \lambda \cdot \mathrm{Id}) = V.$$

This means that $R = \lambda \cdot \mathrm{Id}$. Conversely, $\lambda \cdot \mathrm{Id}$ always belongs to $\mathrm{End}_G(V)$ (for any representation (ρ, V) whatsoever). This provides the isomorphism $\mathrm{End}_G(V) \cong \mathbb{C}$. □

Remark 33.2.3. Note that the final isomorphism $\mathrm{End}_G(V) \cong \mathbb{C}$ can be given by

$$R \mapsto \frac{1}{\dim(V)} \cdot \mathrm{Tr}(R). \tag{11}$$

33.3. **The space of class functions.** Let G be a finite group and denote by $h(G)$ the class number of G. It appeared before in §20. By definition, $h(G)$ is the number of conjugacy classes in G.

Example 33.3.1.
- If G is abelian, $h(G) = \sharp G$.
- If $G = S_n$, $h(G) = p(n)$ (the partition function of n).

A function $f \colon G \to \mathbb{C}$ is called a **class function** if

$$f(hgh^{-1}) = f(g), \quad \forall g, h \in G.$$

Namely, if f is constant on each conjugacy class. We let $\mathrm{Class}(G)$ denote the space of class functions. It is a complex vector space of dimension $h(G)$. If $\phi \in \mathrm{Class}(G)$, define a function $\bar{\phi} \in \mathrm{Class}(G)$ by

$$\bar{\phi}(g) := \overline{\phi(g)}$$

(where on the right we are simply taking the complex conjugate of the complex number $\phi(g)$).

We make $\mathrm{Class}(G)$ into a hermitian space by defining an inner product on it:

$$\langle \phi, \psi \rangle := \frac{1}{\sharp G} \sum_{g \in G} \phi(g) \cdot \bar{\psi}(g).$$

It is easy to verify that this is an inner product; we leave that as an exercise. We also define $\|\phi\|$ to be the non-negative real number satisfying $\|\phi\|^2 := \langle \phi, \phi \rangle$. Our main motivation is the following key example.

Example 33.3.2. For any representation (ρ, V) of G, its character $\chi_\rho \in \mathrm{Class}(G)$.

Example 33.3.3. Let $1 \leq r \leq n$ be integers. Define $\phi_r \colon S_n \to \mathbb{C}$ by $\phi(\sigma)$ equal to the number of cycles of length r appearing in the decomposition of σ as a product of disjoint cycles. The function ϕ_r is a class function.

While $\phi_1(\sigma)$ is the number of fixed points and so $\phi_1 = \chi^{std}$, for $r > 1$ the function ϕ_r does not arise as a character of a representation. Indeed, $\phi_r(1) = 0$ for $r > 1$ so such a representation would have to be 0-dimensional, but for $r \leq n$ the function ϕ_r is not zero: $\phi_r((12 \cdots r)) = 1$.

33.4. **Orthogonality of characters.** We now come to the theorem making characters into a very powerful tool in the study of representations.

Theorem 33.4.1 (Orthogonality of characters)**.** *Let $(\rho, V), (\tau, W)$ be two irreducible representations of G. Then:*

(1) If $\rho \ncong \tau$ then $\langle \chi_\rho, \chi_\tau \rangle = 0$.
(2) $\|\chi_\rho\| = 1$.

Otherwise said, the characters of the irreducible representations of a group G form an orthonormal set in the space of class functions Class(G).

Remark 33.4.2. We will prove in Theorem 36.1.1 below that, in fact, the characters of irreducible representations form an orthonormal *basis* for Class(G).

Proof. Let us write $U = \mathrm{Hom}(V, W)$. We have seen that (σ, U) is a representation of G, where

$$\sigma \colon G \to \mathrm{GL}(U), \quad \sigma(g)(T) = \tau(g) \circ T \circ \rho(g^{-1}),$$

and, by Theorem 33.1.5,

$$\chi_\sigma = \chi_\tau \cdot \bar{\chi}_\rho.$$

By Schur's Lemma,

$$\dim(U^G) = \dim(\mathrm{Hom}_G(V, W)) = \begin{cases} 1, & \rho \cong \tau; \\ 0, & \rho \ncong \tau. \end{cases}$$

On the other hand, by the Projection Formula (Corollary 32.3.2), we have

$$\dim(U^G) = \frac{1}{\sharp G} \sum_{g \in G} \chi_\sigma(g) = \frac{1}{\sharp G} \sum_{g \in G} \chi_\tau(g) \cdot \bar{\chi}_\rho(g) = \langle \chi_\rho, \chi_\tau \rangle.$$

The theorem follows. □

Corollary 33.4.3. *Let h be the number of irreducible characters of G, up to isomorphism. We have*

$$h \leq h(G).$$

In words, the number of irreducible representations of G is at most its class number. (We will see later that $h = h(G)$.)

The following notation will be used repeatedly. Let

$$\rho_1, \dots, \rho_h,$$

be representatives to the isomorphism classes of irreducible representations of G. More precisely, we should say, let $\{(\rho_i, V_i) : i = 1, \dots, h\}$ be representatives to the isomorphism classes of irreducible representations of G, but this is heavier notation that we will usually avoid. In the same vain, given a representation (ρ, V) instead of saying that

$$(\rho, V) \cong (\rho_1, V_1)^{\oplus a_1} \oplus \cdots \oplus (\rho_h, V_h)^{\oplus a_h},$$

we will simply write

$$\rho \cong \rho_1^{a_1} \oplus \cdots \oplus \rho_h^{a_h}.$$

(Here the a_i are non-negative integers and the notation $(\rho_1, V_1)^{\oplus a_1}$ means the direct sum of (ρ_1, V_1) with itself a_1 times, which is declared to be the zero vector space 0 if $a_1 = 0$.) We will also use the notation

$$d_i = \dim(\rho_i), \quad \chi_i = \chi_{\rho_i}.$$

Finally, whenever we view ρ_i as homomorphisms

$$\rho_i \colon G \to \mathrm{GL}_{d_i}(\mathbb{C}),$$

we will assume, when convenient, that $\{\rho_i(g) : g \in G\}$ are *unitary* matrices, which can always be arranged, as we have seen while proving Maschke's theorem.

33.5. **Unique decomposition.** We now prove that the decomposition provided by Maschke's theorem is unique.

Theorem 33.5.1. *Let ρ be a representation of G. Then there are unique non-negative integers m_i such that*

$$\rho \cong \rho_1^{m_1} \oplus \cdots \oplus \rho_h^{m_h}.$$

Proof. By Maschke's theorem, such m_i always exist. Then, by using the formula for the character of a direct sum (§31.3), we have

$$\chi_\rho = \sum_{i=1}^{h} m_i \cdot \chi_i.$$

On the other hand, we can use this formula to deduce by orthogonality of characters that

$$\langle \chi_\rho, \chi_j \rangle = \langle \sum_{i=1}^{h} m_i \cdot \chi_i, \chi_j \rangle = m_j.$$

That shows that the multiplicities m_i are determined uniquely by ρ. □

We will refer to the m_i as the **multiplicity** of the irreducible representation ρ_i in ρ.

Corollary 33.5.2. *We have an isomorphism $(\rho, V) \cong (\tau, W)$ if and only if $\chi_\rho = \chi_\tau$. In words, the isomorphism class of a representation is completely determined by its character.*

Proof. One of the first properties of characters we proved was that the character depends only on the isomorphism class. So, the "only if" is clear. Suppose now that $\chi_\rho = \chi_\tau$, then for every χ_j we have $\langle \chi_\rho, \chi_j \rangle = \langle \chi_\tau, \chi_j \rangle =: m_j$. We have seen that then both representations are isomorphic to $\rho_1^{m_1} \oplus \cdots \oplus \rho_h^{m_h}$, hence to each other. □

34. Some further theorems and examples

Before proving some additional "big theorems", we study some examples and prove some easier results that will give us a better sense of the whole subject.

34.1. **Decomposition of the regular representation.** Recall from § 31.2 the regular representation ρ^{reg} of a group G. It is the representation on the vector space $\mathbb{C}[G]$ that has basis $\{e_g : g \in G\}$, and

$$\rho^{reg}(h)(e_g) = e_{hg}, \quad \forall g, h \in G.$$

We have calculated there that

$$\chi^{reg}(g) = \begin{cases} \sharp G, & g = 1_G; \\ 0, & \text{else.} \end{cases}$$

Let us now find the decomposition of the regular representation into irreducible representations. As we have seen, the multiplicity m_i of χ_i is given by

$$m_i = \langle \chi^{reg}, \chi_i \rangle.$$

This is easy to calculate:

$$\langle \chi^{reg}, \chi_i \rangle = \frac{1}{\sharp G} \sum_g \chi^{reg}(g) \cdot \bar{\chi}_i(g) = \frac{1}{\sharp G} \chi^{reg}(1_g) \cdot \bar{\chi}_i(1_g) = d_i,$$

where $d_i = \dim(V_i)$, as per our conventions. We conclude the following proposition.

Proposition 34.1.1. *We have*

$$\rho^{reg} = \oplus_{i=1}^h \rho_i^{d_i}, \quad \chi^{reg} = \sum_{i=1}^h d_i \chi_i. \tag{12}$$

Namely, every irreducible representation appears in the regular representation with multiplicity equal to its dimension.

By calculating the dimensions of both sides in the isomorphism (12), we conclude:

Corollary 34.1.2. *We have*

$$\sharp G = \sum_{i=1}^h d_i^2. \tag{13}$$

34.2. **Criterion for being irreducible.** An easy consequence of orthogonality of characters is the following useful result.

Corollary 34.2.1. *A representation* (ρ, V) *is irreducible if and only if*

$$\|\chi_\rho\| = 1.$$

Proof. Let us write

$$\chi_\rho = \sum_i m_i \cdot \chi_i,$$

for non-negative integers m_i. By orthogonality of characters (Pythagoras), we have

$$\|\chi_\rho\|^2 = \sum_i m_i^2.$$

Thus, $\|\chi_\rho\| = 1$ if and only if there exists a unique i_0 such that $m_{i_0} = 1$ and all the rest of 0. But this is exactly the cases where ρ is irreducible. □

Remark 34.2.2. A very similar argument gives that $\|\chi_\rho\|^2 = 2$ if and only if ρ is a sum of two distinct irreducible representations, and that $\|\chi_\rho\|^2 = 3$ if and only if ρ is a sum of three distinct irreducible representations. However, when $\|\chi_\rho\|^2 = 4$ the pattern breaks down, and ρ could be either the sum of four distinct irreducible representations, or isomorphic to two copies of a single irreducible representation.

34.3. **Another look at the standard representation of S_n.** We take another look here at the standard representation of S_n, $n \geq 2$, introduced in Example 32.1.2. Recall that this is an n-dimensional representation ρ^{std} of S_n whose character χ^{std} satisfies

$$\chi^{std}(\sigma) = I(\sigma) = \sharp \text{ fixed points of } \sigma.$$

It is clear that the space of invariant vectors is $(\mathbb{C}^n)^{S_n} = U_1$ in the notation of that example and, in particular, $\dim((\mathbb{C}^n)^{S_n}) = 1$. The projection formula gives another way to calculate this dimension (see Example 32.3.4) and we get

$$\frac{1}{n!}\sum_{\sigma \in S_n} \chi^{std}(\sigma) = \frac{1}{n!}\sum_{\sigma \in S_n} I(\sigma) = 1.$$

(Note that the latter formula can also be deduced by applying CFF.) This has the pleasant interpretation that *the expected number of fixed points for a randomly chosen permutation is* 1.

Let us use the notation $T = \{1, 2, \dots, n\}$. Then, from the very definition of the inner product, we can say that

$$\|\chi^{std}\|^2 = \frac{1}{n!}\sum_{\sigma \in S_n} (\sharp \text{ fixed points of } \sigma \text{ on } T)^2.$$

Lemma 34.3.1. $\|\chi^{std}\|^2 = 2$.

Proof. Consider the action of S_n on $T \times T$ given by

$$\sigma(i, j) = (\sigma(i), \sigma(j)).$$

It is clear that S_n has two orbits on $T \times T$. Namely, $\{(i, i) : i \in T\}$ and $\{(i, j) : i \neq j \in T\}$. On the other hand, σ fixes (i, j) if and only if $\sigma(i) = i$ and $\sigma(j) = j$. Thus,

$$\sharp \text{ fixed points of } \sigma \text{ on } T \times T = (\sharp \text{ fixed points of } \sigma \text{ on } T)^2.$$

We apply the CFF to the action of S_n on $T \times T$ to conclude that

$$2 = \frac{1}{n!}\sum_\sigma \sharp \text{ fixed points of } \sigma \text{ on } T \times T = \frac{1}{n!}\sum_\sigma (\sharp \text{ fixed points of } \sigma \text{ on } T)^2 = \|\chi^{std}\|^2.$$

□

As we have seen, this implies that ρ^{std} is a sum of two distinct irreducible representations (Remark 34.2.2). But, we also know that

$$\rho^{std} = \mathbb{1} \oplus \rho^{std,0}.$$

Therefore, we conclude that $\rho^{std,0}$ is irreducible. This argument is much more elegant, I think, than the proof we previously gave.

34.4. **The character group G^* and twisting.** Recall from §31.1 the set

$$G^* = \mathrm{Hom}(G, \mathbb{C}^\times),$$

which is group under

$$(\phi_1 \cdot \phi_2)(g) = \phi_1(g) \cdot \phi_2(g).$$

For a 1-dimensional representation there is no difference between the representation and its character. The following properties are not hard to prove and the details are left as an exercise:

(1) We have a canonical isomorphism

$$(G_1 \times \cdots \times G_a)^* = G_1^* \times \cdots \times G_a^*.$$

It is given by

$$f \mapsto (f|_{G_1}, \dots, f|_{G_a}),$$

where we identify G_i with $\{1\} \times \cdots \times G_i \times \cdots \times \{1\}$. The inverse isomorphism is given by

$$(f_1, \dots, f_a) \mapsto f_1 \times \cdots \times f_a,$$

where

$$(f_1 \times \cdots \times f_a)(g_1, \dots, g_a) = f_1(g_1)f_2(g_2)\cdots f_a(g_a).$$

(2) We have a canonical isomorphism $G^* \cong (G^{ab})^*$.

(3) We have a canonical isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^* \cong \mu_n,$$

where $\mu_n = \{e^{j\cdot 2\pi i/n} : j = 0, 1, \dots, n-1\}$ is the multiplicative group of n-th roots of unity in $\mathbb{C}$. (Don't confuse $(\mathbb{Z}/n\mathbb{Z})^*$ with $(\mathbb{Z}/n\mathbb{Z})^\times$.) The isomorphism is given by

$$f \mapsto f(1) \in \mu_n,$$

and

$$\zeta \mapsto f \in (\mathbb{Z}/n\mathbb{Z})^*, \qquad f(a) := \zeta^a.$$

As every finite abelian group is isomorphic to a product of groups of the form $\mathbb{Z}/n\mathbb{Z}$, we have a method to determine G^* for any finite group G:

- Calculate G^{ab}. Any $f\colon G^{ab} \to \mathbb{C}^\times$ induces an element of G^*, i.e., $f \circ \pi$, where $\pi\colon G \to G^{ab}$ is the canonical homomorphism. All multiplicative characters of G arise this way.
- Write $G^{ab} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_a\mathbb{Z}$. Use the isomorphism $(\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_a\mathbb{Z})^* \cong (\mathbb{Z}/n_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/n_a\mathbb{Z})^*$.
- Use the identification $(\mathbb{Z}/n\mathbb{Z})^* \cong \mu_n$ to fined the multiplicative characters of $\mathbb{Z}/n\mathbb{Z}$.

In particular, we conclude that if G is a finite abelian group then

$$\sharp G = \sharp G^* = h(G).$$

Even better, we can conclude the following corollary of unique decomposition for representations. (For another proof, see the exercises).

Corollary 34.4.1. *Every irreducible representation of an abelian group G is 1-dimensional and there are $\sharp G$ of them. Every n-dimensional representation of G is isomorphic to a representation of the form*

$$\rho\colon G \to \mathrm{GL}_n(\mathbb{C}), \qquad g \mapsto \begin{pmatrix} \alpha_1(g) & & \\ & \ddots & \\ & & \alpha_n(g) \end{pmatrix},$$

for some $\alpha_i \in G^*$.

34.5. **Twisting.** Let (ρ, V) be a representation of G and let $\alpha\colon G \to \mathbb{C}^\times$ be a 1-dimensional representation of G. Then $\mathrm{Hom}((\alpha, \mathbb{C}), (\rho, V))$ is a representation of G of the same dimension and its character, by Theorem 33.1.5, is just

$$\chi_\rho \cdot \bar{\alpha}.$$

As $\bar{\alpha}\colon G \to \mathbb{C}^\times$ is likewise a 1-dimensional representation, we conclude that also $\chi_\rho \cdot \alpha$ is a character. We call the operation $\chi_\rho \mapsto \chi_\rho \cdot \alpha$ **twisting** the representation ρ by the character α. We proved the first part of the following proposition.

Proposition 34.5.1. *For any character χ of G and any 1-dimensional character α of G, also $\chi \cdot \alpha$ is a character. Moreover, if χ is irreducible, so is $\chi \cdot \alpha$.*

Proof. It is not hard to give a direct simple proof of the second part, but let us use characters instead. We have

$$\|\chi\alpha\|^2 = \frac{1}{\sharp G}\sum_g \chi(g)\alpha(g)\bar{\alpha}(g)\bar{\chi}(g).$$

However, because α is 1-dimensional, $\alpha(g)$ is a root of unity and we find

$$\|\chi\alpha\|^2 = \frac{1}{\sharp G}\sum_g \chi(g)\bar{\chi}(g) = \|\chi\|^2 = 1.$$

Thus, by Corollary 34.2.1, χ is irreducible. □

Remark 34.5.2. It is possible that $\chi \cdot \alpha = \chi$ even if $\alpha \neq \mathbb{1}$. In fact, this happens quite often, for example in cases where G has a unique irreducible representation of a given dimension. Nevertheless, in general, twisting by 1-dimensional characters is a very useful method to get new irreducible representations from known ones.

35. Character tables

The character table of a group G is one of the best ways to get insight into the structure of G and its action on vector spaces. There are whole books written on this subject.[16] In this section we will study various properties of the character table. Our treatment is by no means complete: there are additional properties we will not even mention, and there are properties will mention but we will not prove.

The **character table** of G has rows for every irreducible representation of G, and columns for every conjugacy class of G. We reserve the first row for the character $\mathbb{1}$ and the first column for the conjugacy class of the identity (often we will write a representative element for each conjugacy class, and indicate below the conjugacy class how many elements it contains). The

[16] For example: I. Martin Isaacs, *"Character Theory of Finite Groups"*, Dover 1994.

table entry corresponding to a character χ and a conjugacy class c is just $\chi(c)$. By that we mean $\chi(x)$ for any $x \in c$; the choice of x doesn't influence the value $\chi(x)$. So, for example, the character table of S_3 is the following:

	1	(12)	(123)
	1	3	2
$\chi_1 = \mathbb{1}$	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

TABLE 2. Character table of S_3

We see the three representatives $1, (12), (123)$ of the distinct conjugacy classes of S_3 and their sizes indicated by $1, 3, 2$. We see 3 irreducible characters. The first one is the trivial character $\mathbb{1}$, the second is the sign homomorphism $\mathrm{sgn}\colon S_3 \to \mathbb{C}^\times$, and the third is the character $\chi^{std,0}$.

We will usually use the notation χ_i for the rows and c_i for the columns. We use the notation introduced before: χ_i is the character of the irreducible representation ρ_i that has dimension d_i.

35.1. First properties of the character table.

Theorem 35.1.1. *The character table of G has the following properties:*

1. *The number of rows equals to the number of columns.*
2. *The sum of the squares of the entries of the first column is the cardinality of the group.*
3. *The number of rows with 1 in the first column is equal to $\sharp G^{ab}$.*
4. *Every entry in the first column is an integer dividing $\sharp G$.*
5. *The "weighted" inner-product of distinct rows is 0. The weighted self-product of a row is equal to $\sharp G$ (here the weights are the cardinality of conjugacy classes).*
6. *The "weighted" sum of the rows is the vector $(\sharp G, 0, \dots, 0)$ (here the weights are the dimensions of the representations).*

The proof consists of references to theorems we proved, or will prove shortly.

Proof. (1) is the statement that the number of irreducible characters h is actually equal to $h(G)$. We mentioned this before and will prove it in Theorem 36.1.1 below.

(2) is Corollary 34.1.2: $\sharp G = \sum_{i=1}^h d_i^2$

(3) states the the irreducible characters of dimension 1 are 1-dimensional characters $G \to \mathbb{C}^\times$, and $\sharp G^* = \sharp (G^{ab})^*$ (Lemma 31.1.1).

(4) is a theorem we will not prove because it requires some notions from algebraic number theory, but it is useful to know.

(5) is just orthogonality of characters (Theorem 33.4.1). If we use the fact that characters are class functions, we may write

$$\langle \chi_i, \chi_j \rangle = \frac{1}{\sharp G} \sum_{g \in G} \chi_i(g) \bar{\chi}_j(g) = \frac{1}{\sharp G} \sum_{i=1}^{h} |c_i| \cdot \chi_i(c_i) \bar{\chi}_j(c_i).$$

We find that if $i \neq j$ then the weighted inner-product of the rows, $\sum_{i=1}^h |c_i| \chi_i(c_i) \bar{\chi}_j(c_i)$, is equal to 0, and if $i = j$ it is equal to $\sharp G$.

(6) is just a restatement of the decomposition of the regular representation: $\chi^{reg} = \sum_{i=1}^h d_i \chi_i$ (Proposition 34.1.1). □

35.2. **Examples of character tables.**

35.2.1. *The character table of $\mathbb{Z}/n\mathbb{Z}$.* Recall that every irreducible representation of an abelian group is a multiplicative character and that we have

$$(\mathbb{Z}/n\mathbb{Z})^* \cong \mu_n.$$

We usually denote the corresponding characters $\rho_0, \dots, \rho_{n-1}$ in this case, because if we let $\zeta = e^{2\pi i/n}$ then we have

$$\rho_i(a) = \zeta^{ai}.$$

(This notation is slightly in odds with the usual convention of denoting the irreducible characters of a group G by $\chi_1, \dots, \chi_h$.) We find the following table

	0	1	2		$n-1$
$\rho_0 = \mathbb{1}$	1	1	1	$\dots$	1
ρ_1	1	ζ	ζ^2	$\dots$	ζ^{n-1}
ρ_2	1	ζ^2	ζ^4	$\dots$	$\zeta^{2(n-1)}$
$\vdots$				$\vdots$	
ρ_{n-1}	1	ζ^{n-1}	$\zeta^{2(n-1)}$	$\dots$	$\zeta^{(n-1)^2}$

TABLE 3. Character table of $\mathbb{Z}/n\mathbb{Z}$

Note that property (6) in Theorem 35.1.1 gives us the very useful fact in complex analysis: For a root of unity ζ of order n, we have $\sum_{i=0}^{n-1} \zeta^{ai} = 0$ for every $a \not\equiv 0(n)$.

35.2.2. *The character tables of $(\mathbb{Z}/2\mathbb{Z})^2$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ and $(\mathbb{Z}/3\mathbb{Z})^2$.* "Multiplying" two copies of the character table of $\mathbb{Z}/2\mathbb{Z}$ we find

	0	1
$\mathbb{1}$	1	1
ρ_1	1	-1

×

	0	1
$\mathbb{1}$	1	1
ρ_1	1	-1

=

	(0,0)	(1,0)	(0, 1)	(1,1)
$\mathbb{1} \times \mathbb{1}$	1	1	1	1
$\mathbb{1} \times \rho_1$	1	1	-1	-1
$\rho_1 \times \mathbb{1}$	1	-1	1	-1
$\rho_1 \times \rho_1$	1	-1	-1	1

TABLE 4. Character table of $(\mathbb{Z}/2\mathbb{Z})^2$

Similarly, for any abelian group $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_a\mathbb{Z}$ we can "multiply" the character tables for each $\mathbb{Z}/n_i\mathbb{Z}$ to find the character table of G. This rests on our results

$$G^* \cong (\mathbb{Z}/n_1\mathbb{Z})^* \times \dots \times (\mathbb{Z}/n_a\mathbb{Z})^* \cong \mu_{n_1} \times \dots \times \mu_{n_a},$$

and the concrete description of the character table of $\mathbb{Z}/n\mathbb{Z}$.

It is not efficient to use this method for $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ because by CRT we have $G \cong \mathbb{Z}/15\mathbb{Z}$ which is a cyclic group for which we already have a nice description. But, for example, for the case $G = (\mathbb{Z}/3\mathbb{Z})^2$ it is useful, and we find the following 9×9 table ($\omega = e^{2\pi i/3}$):

	0	1	2
$\mathbb{1}$	1	1	1
ρ_1	1	ω	ω^2
ρ_2	1	ω^2	ω

$\times$

	0	1	2
$\mathbb{1}$	1	1	1
ρ_1	1	ω	ω^2
ρ_2	1	ω^2	ω

$=$

	(0,0)	$\dots$	$(1,2)$	$\dots$	(a,b)
$\mathbb{1}\times\mathbb{1}$	1		1		1
$\vdots$					
$\rho_1\times\rho_2$	1		ω^2		ω^{a+2b}
$\vdots$		$\vdots$		$\vdots$	
$\rho_i\times\rho_j$	1		ω^{i+2j}		ω^{ai+bj}
$\vdots$		$\vdots$		$\vdots$	

TABLE 5. Character table of $(\mathbb{Z}/3\mathbb{Z})^2$

35.2.3. *The character table of* S_3. We have $h(S_3) = p(3) = 3$ and so there are 3 conjugacy classes and we take as representatives $1, (12), (123)$. Their sizes are $1, 3, 2$, respectively. We have

$$S_3^{ab} = S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z},$$

and, in fact, we know two 1-dimensional characters: $\mathbb{1}$ and sgn. As we must have

$$\sharp S_3 = 6 = 1^1 + 1^1 + x^2,$$

we conclude that the remaining irreducible representation of S_3 is 2-dimensional. We happen to know such a representation, namely, $\rho^{std,0}$ and its character $\chi^{std,0}$ whose value on a permutation σ is the number of fixed points of σ minus 1. We therefore find the following table:

	1	(12)	(123)
	1	3	2
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

TABLE 6. Character table of S_3

Remark though that we didn't really need to use our "lucky break" of knowing before-hand an irreducible 2-dimensional representation. We could have *solved* for the remaining character:

$$\chi_3 = \frac{1}{2}(\chi^{reg} - \chi_1 - \chi_2)$$

(Theorem 35.1.1).

35.2.4. *The character table of* D_4. It requires some calculations but one find that

$$D_4' = \{1, x^2\}, \quad D_4^{ab} = \{1, \bar{x}, \bar{y}, \bar{x}y\},$$

and that every element of D_4^{ab} has order 2. Thus,

$$D_4^{ab} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \qquad \bar{x} \mapsto (1,0), \bar{y} \mapsto (0,1).$$

We also calculate "by hand" the conjugacy classes and find that they are given by

$$c_1 = \{1\},\ c_2 = \{x, x^{-1}\},\ c_3 = \{x^2\},\ c_4 = \{y, yx^2\},\ c_5 = \{yx, yx^{-1}\}.$$

There isn't a really quick way to do that, but one can note that since $\langle x \rangle$ is a normal subgroup, conjugacy classes are either contained in it, or disjoint from it. At any rate, we now know that D_4 has four 1-dimensional representations, "lifted" from $(\mathbb{Z}/2\mathbb{Z})^2$. That is, if χ is an irreducible character of $(\mathbb{Z}/2\mathbb{Z})^2$ and f is the composition $D_4 \rightarrow D_4^{ab} \rightarrow (\mathbb{Z}/2\mathbb{Z})^2$ then $\chi \circ f$ is an 1-dimensional character of D_4.

In addition, D_4 has one more irreducible representation and its dimension x satisfies

$$8 = \sharp D_4 = 1^2 + 1^2 + 1^2 + 1^2 + x^2.$$

It follows that we are missing a 2-dimensional representation. Note that we can solve for the missing character, say χ, using the result on the sum of the rows of the character table, but it is also natural to wonder whether the missing representation is provided by the action of D_4 on the plane (the action inducing the action of D_4 on the square). In this representation ρ^{pl}, the action of the representatives for conjugacy classes is given as follows:

$$1 = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix},\ \ x = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix},\ \ y = \begin{pmatrix} -1 & \\ & 1 \end{pmatrix},\ \ x^2 = \begin{pmatrix} -1 & \\ & -1 \end{pmatrix},\ \ yx = \begin{pmatrix} & -1 \\ -1 & \end{pmatrix}.$$

We can now write the character table of D_4. The last row is $\chi^{pl} = \chi_{\rho^{pl}}$, which is indeed irreducible because $\|\chi^{pl}\| = 1$.

	1	x	y	xy	x^2
	1	2	2	2	1
$\mathbb{1}$	1	1	1	1	1
$\rho_1 \times \mathbb{1}$	1	-1	1	-1	1
$\mathbb{1} \times \rho_1$	1	1	-1	-1	1
$\rho_1 \times \rho_1$	1	-1	-1	1	1
χ^{pl}	2	0	0	0	-2

TABLE 7. Character table of D_4

Here is an application. The composition ρ defined by

$$\begin{tikzcd} D_4 \arrow[r] & S_4 \arrow[r, "\rho^{std}"] & \mathrm{GL}_4(\mathbb{C}) \end{tikzcd},$$

(where the first arrow is the natural inclusion of D_4 into S_4, $x \mapsto (1234), y \mapsto (24)$) is a 4-dimensional representation of D_4. It is a bit hard to understand this action. Indeed, in terms of matrices

$$x = \begin{pmatrix} 0&0&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \end{pmatrix},\ \ y = \begin{pmatrix} 1&0&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \\ 0&1&0&0 \end{pmatrix},$$

and it is not easy to understand what is the overall action of elements of the group. However, we can decompose ρ into irreducible representations. A calculation gives

$$\langle \chi_\rho, \mathbb{1} \rangle = 1 \quad, \langle \chi_\rho, \rho_1 \times \mathbb{1} \rangle = 1, \quad \langle \chi_\rho, \chi^{pl} \rangle = 1.$$

This tells us that

$$\rho \cong \mathbb{1} \oplus (\rho_1 \times \mathbb{1}) \oplus \rho^{pl}.$$

That means that there is another basis for $\mathbb{C}^4$ in which the representation has the form

$$x = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

And a general element g of D_4 will act by a matrix of the form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \pm 1 & 0 \\ 0 & 0 & \rho^{pl}(g) \end{pmatrix}.$$

It is now much easier to understand the action of D_4.

35.2.5. *The character table of S_4.*

Here is a general principle. Let $f \colon A \to B$ be a homomorphism of groups. Let $\rho \colon B \to \mathrm{GL}(V)$ be a representation of B. Then $\rho \circ f$ is a representation of A and its character is simply

$$\chi_{\rho\circ f} = \chi_\rho \circ f \colon A \to \mathbb{C}.$$

In fact, we have used it several times before in the situation $G \to G^{ab} \to \mathbb{C}^\times$ to lift 1-dimensional characters of G^{ab} to G.

Now, if f is *surjective* and ρ is irreducible then also $\rho \circ f$ is irreducible. Indeed, suppose that $U \subseteq V$ is a subrepresentation of $\rho \circ f$. That is, for all $a \in A$ we have $\rho(f(a))(U) \subseteq U$. Then, as f is surjective, it follows that for all $b \in B$ we have $\rho(b)(U) \subseteq U$. It follows that U is a subrepresentation of ρ and so $U = 0$ or V.

Let us use this for the surjective homomorphism $f \colon S_4 \to S_3$, whose kernel is K, the Kline group. We have studied this homomorphism before. Using it, we can lift the characters of S_3 to S_4, and so we easily find the first 3 rows of the character table of S_4. (The conjugacy classes of S_n correspond to the cycle type of permutations and that gives us the columns' labels.) As there are 5 conjugacy classes, there are two additional irreducible representations. We know one of them, $\rho^{std,0}$, and we get the last row as the twist $\rho^{std,0} \cdot \mathrm{sgn}$ (or by solving the equation where the sum of the rows with multiplicities is equal to the vector $(24, 0, 0, 0, 0)$). We find the following table.

	1	(12)	(123)	(1234)	(12)(34)
	1	6	8	6	3
$\mathbb{1}$	1	1	1	1	1
sgn	1	-1	1	-1	1
$\chi_3 \circ f$	2	0	-1	0	2
$\chi^{std,0}$	3	1	0	-1	-1
$\chi^{std,0} \cdot \mathrm{sgn}$	3	-1	0	1	-1

TABLE 8. Character table of S_4

35.2.6. *Character table of A_4.* The representatives for the conjugacy classes of A_4 are given by $1, (12)(34), (123), (132)$. There are therefore 4 irreducible representations. As A_4/K is of order 3, it follows that $A_4/K \cong \mathbb{Z}/3\mathbb{Z}$ and that $K \supseteq A_4'$. As A_4 is not abelian, $A_4' \neq \{1\}$ and so contains some element of cycle type $(2,2)$. But those form a single conjugacy class and A_4' is normal. It follows that $A_4' = K$.

We conclude that there are 4 irreducible representations, of which 3 are 1-dimensional, and the last is 3-dimensional (as $\sharp A_4 = 1^2 + 1^2 + 1^2 + x^2$ only allows $x = 3$). Using the result about the sum of rows we find the following character table:

	1	(123)	(132)	$(12)(34)$
	1	4	4	3
$\mathbb{1}$	1	1	1	1
χ_1	1	ω	ω^2	1
χ_2	1	ω^2	ω	1
χ	3	0	0	-1

TABLE 9. Character table of A_4

It turns out that the last character is just $\chi^{std,0}|_{A_4}$. This is no coincidence. One can prove that for $n \geq 4$ the representation $\rho^{std,0}|_{A_n}$ is an irreducible representation of A_n (Exercise 128).

35.3. **Orthogonality of columns.** In this subsection we show that the columns of the character table enjoy an orthogonality property. We begin with some renormalization device to make the argument more transparent, hopefully.

For every character χ of G we define a vector $v_\chi \in \mathbb{C}^h$, where $h = h(G)$ is the number of conjugacy classes of G. Let $c_1, \dots, c_h$ be the conjugacy classes of G, and let

$$v_\chi = (\sqrt{\frac{\sharp c_1}{\sharp G}} \cdot \chi(c_1), \dots, \sqrt{\frac{\sharp c_h}{\sharp G}} \cdot \chi(c_h))$$

The point of this construction is that for every two characters χ, ψ (or even any two class functions) we have

$$\langle \chi, \psi \rangle = \langle v_\chi, v_\psi \rangle,$$

where the inner-product on the left is the inner product of class-functions, and the inner-product on the right is the usual inner-product in $\mathbb{C}^h$. In fact, we have already noticed something very similar – see the proof of part (5) of Theorem 35.1.1.

Let $\chi_1, \dots, \chi_h$ denote the irreducible characters of G. It follows that the rows of the following matrix are orthonormal:

$$\begin{pmatrix} v_{\chi_1} \\ \hline v_{\chi_2} \\ \hline \vdots \\ \hline v_{\chi_h} \end{pmatrix}.$$

But this implies that the columns of the same matrix are an orthonormal set too. Namely, for any two conjugacy classses c_a, c_b we get that

$$\sum_{i=1}^{h} \sqrt{\frac{\sharp c_a}{\sharp G}} \sqrt{\frac{\sharp c_b}{\sharp G}} \cdot \chi_i(c_a)\bar{\chi}_i(c_b) = \delta_{ab}.$$

Note that $\sharp(G)/\sharp(c_a) = \sharp Cent(x)$ for any $x \in C_a$. Therefore, we conclude the following.

Proposition 35.3.1 (Orthogonality of columns). *We have the following orthogonality properties of the columns of the character table.*

(1) *If $c_a \neq c_b$ are conjugacy classes then the product of the c_a column with the c_b column is* 0*. To be precise:*

$$\sum_{i=1}^{h} \chi_i(c_a)\bar{\chi}_i(c_b) = 0.$$

(2) *For every conjugacy class c_a the norm of the c_a column is the cardinality of its centralizer. That is,*

$$\sum_{i=1}^{h} |\chi_i(c_a)|^2 = \sharp Cent(x), \quad x \in c_a.$$

It follows that we can use the entries of the character table, more specifically we can use the second part of the proposition, to figure out the size of conjugacy classes. We record it as a corollary.

Corollary 35.3.2. *The character table determines the size of the conjugacy classes.*

36. The irreducible characters form a basis for Class(G)

In this section we fill a gap and prove that the irreducible characters of a group G form a basis for Class(G). Nothing prevented us from proving it sooner; it just seemed more useful to see some examples before developing the theory further.

36.1. **Irreducible characters form a basis.**

Theorem 36.1.1. *Let G be a group and let $\chi_1, \dots, \chi_h$ be its irreducible characters. Then*

$$\{\chi_1, \dots, \chi_h\}$$

is an orthonormal basis for Class(G).

Proof. We begin with a lemma that constructs endomorphisms of representations.

Lemma 36.1.2. *Let (ρ, V) be a representation of G and let α a class function. Then the linear operator*

$$T = T_\rho = \sum_{g \in G} \alpha(g)\rho(g) \in \mathrm{End}_G(V).$$

Proof. The fact that T is a linear operator is clear, because $\alpha(g)$ are scalars and T is the sum of the linear operators $\alpha(g)\rho(g)$. The point is that it commutes with ρ. We have

$$\rho(h) \circ T \circ \rho(h)^{-1} = \sum_{g \in G} \alpha(g)\rho(hgh^{-1}) = \sum_{g \in G} \alpha(hgh^{-1})\rho(hgh^{-1}).$$

The last equality is true because α is a class function. Now, $g \mapsto hgh^{-1}$ is a bijection of G (even an automorphism) and hence

$$\rho(h) \circ T \circ \rho(h)^{-1} = \sum_{g \in G} \alpha(hgh^{-1})\rho(hgh^{-1}) = \sum_{g \in G} \alpha(g)\rho(g) = T.$$

□

We know already that $\{\chi_1, \dots, \chi_h\}$ are an orthonormal set. To prove they form a basis we need only show for $\beta \in \mathrm{Class}(G)$,

$$\langle \chi_i, \beta \rangle = 0, \forall i \implies \beta \equiv 0.$$

Let $\alpha = \bar{\beta}$. It will of course be enough to prove $\alpha \equiv 0$.

Let (ρ, V) be an irreducible representation. We claim the the operator

$$T_\rho := \sum_{g \in G} \alpha(g)\rho(g) \in \mathrm{End}_G((\rho, V))$$

is actually the zero operator. By Schur's Lemma, we have $\mathrm{End}_G((\rho, V)) \cong \mathbb{C}$ under the map $T \mapsto \frac{1}{\dim(V)}\mathrm{Tr}(T)$ (Equation (11)). Now,

$$\mathrm{Tr}(T_\rho) = \sum_{g \in G} \alpha(g)\mathrm{Tr}(\rho(g)) = \sum_{g \in G} \chi_\rho(g)\bar{\beta}(g) = \sharp G \langle \chi_\rho, \beta \rangle = 0.$$

And therefore $T_\rho = \frac{1}{\dim(V)}\mathrm{Tr}(T_\rho) \cdot Id_V = 0$.

Note that the construction

$$\rho \mapsto T_\rho = \sum_{g \in G} \alpha(g)\rho(g)$$

commutes with direct sums. Thus, we may conclude that for *any* representation (ρ, V) of G we have $T_\rho = 0$. In particular this holds of the regular representation. That is, we conclude that $\sum_{g \in G} \alpha(g)\rho^{reg}(g)$ is the zero operator on $\mathbb{C}[G]$. In this case, we must have

$$\sum_{g \in G} \alpha(g)\rho^{reg}(g)(e_1) = 0,$$

where $e_1 \in \{e_g : g \in G\}$ is the basis vector indexed by the identity element of G. However,

$$\sum_{g \in G} \alpha(g)\rho^{reg}(g)(e_1) = \sum_{g \in G} \alpha(g)e_g.$$

As $\{e_g\}$ is a basis, it follows that $\alpha(g) = 0$ for all $g \in G$, as we wanted to show. □

36.2. **Even more properties of the character table.** We organize together all the properties of the character table we have seen, implicitly or explicitly.

Theorem 36.2.1. *Let G be a group with class number h. Let $\{\chi_i : i = 1, \dots, h\}$ be its irreducible characters, $d_i = \dim(\chi_i) = \chi_i(1)$, and let $\{c_a : a = 1, \dots, h\}$ be the conjugacy classes of G. We assume always that $\chi_1 = \mathbb{1}$ and $c_1 = \{1_g\}$.*

The character table of G has the following properties:

1. *The number of rows equals to the number of columns.*
2. *The sum of the squares of the entries of the first column is the cardinality of the group.*
3. *The number of rows with 1 in the first column is equal to $\sharp G^{ab}$.*
4. *Every entry in the first column is an integer dividing $\sharp G$.*
5. *The "weighted" inner-product of distinct rows is 0. The weighted self-product of a row is equal to $\sharp G$ (here the weights are the cardinality of conjugacy classes).*
6. *The "weighted" sum of the rows is the vector $(\sharp G, 0, \dots, 0)$ (here the weights are the dimensions of the representations).*

(7) *For any two columns c_a, c_b we have*

$$\sum_{i=1}^{h} \chi_i(c_a)\bar{\chi}_i(c_b) = 0, \quad a \neq b,$$

and

$$\sum_{i=1}^{h} |\chi_i(c_a)|^2 = |Cent(x)|, \; x \in c_a.$$

(8) *If $\chi_i(c_a) = \alpha$ then $\chi_i(c_a^{-1}) = \bar{\alpha}$ where c_a^{-1} is the conjugacy class $\{x^{-1} : x \in c_a\}$. In particular, the set of entries of the character table is closed under complex conjugation.*

(9) *If χ_i is 1-dimensional and χ_j is any other irreducible character, then $\chi_i \cdot \chi_j = \chi_k$ for some irreducible character χ_k (possibly equal to χ_j).*

(10) *$|\chi_i(g)| \leq \chi_i(1)$, with equality if and only if $\rho_i(g) = \alpha \cdot Id$ for some root of unity α.*

(11) *If $c_a \neq c_b$ then there is some character χ_i such that $\chi_i(c_a) \neq \chi_i(c_b)$.*

(12) *The weighted sum of the columns, where the i-th column is given weight $|c_i|$, is the vector ${}^t(\sharp G, 0, \dots, 0)$.*

Proof. We have already proved properties (1) - (6) in Theorem 35.1.1 (only that now we have really proved (1)). Property (7) is the orthogonality of columns proven in Proposition 35.3.1.

Property (8) was also mentioned before: we have seen that $\chi_i(x^{-1}) = \overline{\chi_i(x)}$ (Equation 9). Property (9) is of course the twisting operation we have studied in § 34.5. Property (10) follows from the fact that $\chi_i(g)$ is a sum of d_i roots of unity and the absolute value is equal to d_i if and only if they all point in the same direction.

Property (11) follows from the fact that the $\{\chi_i\}$ form a basis for the class functions and so for any given $c_a \neq c_b$ a suitable linear combination of them should have value 1 on c_a and value 0 on c_b. This is only possible if for some i, $\chi_i(c_a) \neq \chi_i(c_b)$.

Property (12) is essentially he orthogonality of χ_1 and χ_i for $i \neq 1$. Indeed, the i-th entry of this sum of columns is

$$\sum_{j=1}^{h} |c_j|\chi_i(c_j) = \sharp G \cdot \langle \chi_i, \chi_1 \rangle = \sharp G \cdot \delta_{i,1}.$$

□

Character tables have even more properties. We mention an additional one, which is a theorem of Burnside, just because it is so easy to state (we will not use it in this course)

Theorem 36.2.2 (Burnside)**.** *If $d_i > 1$ then χ_i takes the value 0 for some conjugacy class.*

37. Using the character table to find normal subgroups

We will now see a beautiful application of character tables for the calculation of all normal subgroups of a group G.

37.1. **Normal subgroups and character kernels.** Let (ρ, V) be any representation of G with character $\chi = \chi_\rho$. Define

$$\text{Ker}(\chi_\rho) := \{g \in G : \chi_\rho(g) = \chi(1)\} = \{g \in G : \chi_\rho(g) = \dim(V)\}.$$

Lemma 37.1.1. *We have*

$$\text{Ker}(\chi_\rho) = \text{Ker}(\rho),$$

and so $\text{Ker}(\chi_\rho)$ *is a normal subgroup of* G*.*

Proof. Let $g \in \mathrm{Ker}(\rho)$ then $\rho(g) = \mathrm{Id}_V$. Then, $\chi(g) = \mathrm{Tr}(\mathrm{Id}_V) = \dim(V)$ and thus $g \in \mathrm{Ker}(\chi)$.

Conversely, let $g \in \mathrm{Ker}(\chi)$ and $d = \dim(V)$. As $\chi(g)$ is a sum of d roots of unity (which are the eigenvalues, with multiplicity, of $\rho(g)$), the only way this sum can be equal to to d if all these roots of unity are 1. This implies $\rho(g) = \mathrm{Id}_V$. □

In particular, if $\chi_1, \dots, \chi_h$ denote the irreducible characters of G, as per our usual notation, we have the normal subgroups

$$\mathrm{Ker}(\chi_i), \quad i = 1, 2, \dots, h.$$

Note that these subgroups can be written as a union of conjugacy classes, given the character table of G.

Lemma 37.1.2. *Let χ be a character of a representation (ρ, V) of G. Suppose that*

$$\chi = \sum_{i \in I} a_i \chi_i,$$

for a subset $I \subseteq \{1, 2, \dots, h\}$ and positive integers a_i. Then,

$$\mathrm{Ker}(\chi) = \cap_{i \in I} \mathrm{Ker}(\chi_i).$$

Once more, note that this can be calculated effectively from the character table of G.

Proof. We have

$$\chi(1) = \sum_{i \in I} a_i \chi_i(1).$$

If $g \in \mathrm{Ker}(\chi_i)$ for every i, then

$$\chi(g) = \sum_{i \in I} a_i \chi_i(g) = \sum_{i \in I} a_i \chi_i(1) = \chi(1),$$

and so $g \in \ker(\chi)$.

Conversely, if $g \in \ker(\chi)$ we have

$$\chi(1) = \chi(g) = \sum_{i \in I} a_i \chi_i(g) = \sum_{i \in I} a_i \chi_i(1).$$

Since the a_i are positive integers and $|\chi_i(g)| \leq \chi_i(1)$, the only way the last equality can hold is if $\chi_i(g) = \chi_i(1)$ for every $i \in I$. Namely, if $g \in \mathrm{Ker}(\chi_i)$, for all $i \in I$. □

Lemma 37.1.3. *Any normal subgroup $N \lhd G$ is of the form $\mathrm{Ker}(\chi)$ for some character χ.*

Proof. Let $H = G/N$ and consider the composition

$$G \xrightarrow{\pi} G/N = H \xrightarrow{\rho_H^{reg}} \mathrm{GL}(\mathbb{C}[H]).$$

Let $\rho = \rho_H^{reg} \circ \pi$. Since the regular representation ρ_H^{reg} of H is injective, we have $\mathrm{Ker}(\rho) = \mathrm{Ker}(\pi) = N$. Therefore,

$$N = \mathrm{Ker}(\chi_\rho).$$

□

We summarize our discussion in the following theorem.

Theorem 37.1.4. *Let $\chi_1, \dots, \chi_h$, $h = h(G)$, be the irreducible characters of G. Let*

$$N_i = \mathrm{Ker}(\chi_i).$$

Any normal subgroup N of G is of the form

$$N = \cap_{i \in I} \mathrm{Ker}(\chi_i),$$

for a suitable subset $I \subseteq \{1, 2, \dots, h\}$. And, conversely, any such intersection is a normal subgroup of G.

Remark 37.1.5. The whole point is, of course, that we have a practical easy method to find all the normal subgroups of a group G from the character table. Note, also, that the theorem implies that any proper maximal normal subgroup of G is of the form $\mathrm{Ker}(\chi_i)$ for some i (although, the converse is not true; $\mathrm{Ker}(\chi_i)$ is often not a maximal normal subgroup).

Example 37.1.6. We illustrate the theorem using the character table of A_4. Recall that it is given by the following table, where in the last column we indicated the kernel of the character.

	1	(123)	(132)	$(12)(34)$	Ker
	1	4	4	3	
$\mathbb{1}$	1	1	1	1	A_4
χ_1	1	ω	ω^2	1	K
χ_2	1	ω^2	ω	1	K
χ	3	0	0	-1	$\{1\}$

TABLE 10. Character table of A_4

We conclude that A_4 has only one non-trivial normal subgroup, which is K.

37.2. **Recognizing the commutator subgroup.** Given a group G we have several normal subgroups canonically associated to it. For example, the commutator subgroup G' and the centre $Z(G)$. In light of Theorem 37.1.4, it makes sense to ask how to construct them from the character table. For the center, this is just the union of all conjugacy classes of size 1. For the commutator subgroup we have the following proposition.

Proposition 37.2.1. *We have*

$$G' = \bigcap_{\chi \text{ 1-dim. char.}} \operatorname{Ker}(\chi).$$

Proof. Suppose that $g \in G'$ and ρ is a 1-dimensional representation, then $\rho(G') = 1$ (and so, as we have used several times before, ρ factors through G^{ab}). Thus, $G' \subseteq \bigcap_{\chi \text{ 1-dim. char.}} \operatorname{Ker}(\chi)$.

Suppose now that $g \notin G'$ and denote $\bar{g}$ its image in G^{ab}. Then $\bar{g} \neq 0$ (the identity element of the abelian group G^{ab}). Write

$$G^{ab} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_a\mathbb{Z}.$$

Then $\bar{g} = (g_1, \dots, g_a)$ and assume without loss of generality that $g_1 \neq 0$.

Let $\zeta = e^{2\pi i/n_1}$ and ρ the multiplicative character of $\mathbb{Z}/n_1\mathbb{Z}$ given by $\rho(a) = \zeta^a$. Then, $\rho \times \mathbb{1} \times \cdots \times \mathbb{1}$ is a multiplicative character of G^{ab} and hence, through $G \to G^{ab}$, also of G. We have

$$(\rho \times \mathbb{1} \times \cdots \times \mathbb{1})(g) = (\rho \times \mathbb{1} \times \cdots \times \mathbb{1})(\bar{g}) = \rho(g_1) = \zeta^{g_1} \neq 1.$$

Thus, $g \notin \bigcap_{\chi \text{ 1-dim. char.}} \operatorname{Ker}(\chi)$, and the proof is complete. □

Remark 37.2.2. One can also characterize $Z(G)$ in terms of the characters of G. See Exercise 131.

38. MORE EXAMPLES OF REPRESENTATIONS

In this section we consider two more examples of representations, more difficult than those we considered thus far.

38.1. **The character table of the Frobenius group F_{20}.** The **Frobenius group** F_{20} is the group

$$\mathbb{Z}/5\mathbb{Z} \rtimes (\mathbb{Z}/5\mathbb{Z})^\times.$$

Recall that $(\mathbb{Z}/5\mathbb{Z})^\times = \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ and the semi-direct product is taken relative to the identity map $(\mathbb{Z}/5\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$. The group law is very simple,

$$(n_1, b_1)(n_2, b_2) = (n_1 + b_1 n_2, b_1 b_2), \qquad n_i \in N := \mathbb{Z}/5\mathbb{Z}, b_i \in B := (\mathbb{Z}/5\mathbb{Z})^\times.$$

The Frobenius group can be realized into other ways:

(1) As a group of matrices

$$\left\{ \left(\begin{smallmatrix} b & n \\ & 1 \end{smallmatrix}\right) : b \in \mathbb{Z}/5\mathbb{Z}^\times, n \in \mathbb{Z}/5\mathbb{Z} \right\},$$

with multiplication

$$\left(\begin{smallmatrix} b_1 & n_1 \\ & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} b_2 & n_2 \\ & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} b_1 b_2 & n_1 + b_1 n_2 \\ & 1 \end{smallmatrix}\right).$$

(2) As the subgroup of S_5 given by

$$\langle (12345), (2354) \rangle.$$

The isomorphism of F_{20} with the group of matrices is evident. For the realization as the subgroup of permutations, we send

$$(12345)^n \mapsto (n, 1), \qquad (2345) \mapsto (0, 2).$$

Because

$$(2354)(12345)(2354)^{-1} = (12345)^2,$$

and $(0,2)(1,1)(0,2)^{-1} = (2,1)$, it follows (with some additional arguments) that we have an isomorphism $\langle (12345), (2354) \rangle \cong F_{20}$.

Next, we calculate the conjugacy classes of F_{20}. For elements of N, conjugation by N is trivial and so by conjugating by elements of B we get the full conjugacy classes (using that $F_{20} = NB$). We have the formula

$$(0, b)(n, 1)(0, b^{-1}) = (bn, 1).$$

We find two conjugacy classes:

$$a_1 = \{(0,1)\}, \quad a_2 = \{(i,1) : i = 1,2,3,4\}.$$

Likewise, conjugating elements of B by B is trivial and so we will get the full conjugacy classes of elements of B by conjugating them by elements of N. We have the relation

$$(n,1)(0,b)(-n,1) = ((1-b)n, b).$$

For $b = 2, 3, 4$, we get the conjugacy classes

$$c_2 = \{(i,2) : 0 \le i \le 4\}, \quad c_3 = \{(i,3) : 0 \le i \le 4\}, \quad c_4 = \{(i,4) : 0 \le i \le 4\}.$$

We see that we already accounted for all the elements of the group. Therefore, F_{20} has 5 conjugacy classes (of sizes $1, 4, 5, 5, 5$).

Note that $F_{20}/N \cong B \cong (\mathbb{Z}/5\mathbb{Z})^\times$, $(n, b) \mapsto b$. As F_{20} is not abelian, and N has no non-trivial subgroups, it follows that $N = F_{20}'$ and $F_{20}^{ab} \cong (\mathbb{Z}/5\mathbb{Z})^\times$, which is cyclic group of order 4 with generator 2.Thus, F_{20} has precisely 5 irreducible representations, 4 of which are 1-dimensional. Therefore, as the size of the group is the sum of the squares of the dimensions of the irreducible representations, the remaining irreducible representation is 4-dimensional. We can find its character χ_4 by using that the weighted sum of the rows of the character table is the regular representation. (The notation is chosen so that the first 4 characters have notation that agrees with the notation we used for cyclic groups.)

It is not hard to check that under the realization of F_{20} as a subgroup of S_5 in fact $\chi_4 = \chi^{std,0}|_{F_{20}}$.

	a_1	a_2	c_2	c_3	c_4
	1	4	5	5	5
	$(0,1)$	$(1,1)$	(0,2)	$(0,3)$	$(0,4)$
$\chi_0 = \mathbb{1}$	1	1	1	1	1
χ_1	1	1	i	$-i$	-1
χ_2	1	1	-1	-1	1
χ_3	1	1	$-i$	i	-1
χ_4	4	-1	0	0	0

TABLE 11. Character table of F_{20}

38.2. **Monomial representations.** Consider a finite group G acting on a non-empty set S. Construct a vector space V with basis $\{e_s : s \in S\}$; we have $\dim(V) = \sharp S$. There is a natural representation

$$\rho\colon G \to \mathrm{GL}(V), \quad \rho(g)(e_s) = e_{g*s}.$$

Such representations are called **monomial**.

In fact, we have already seen at least two instances of this construction. When $S = G$, and G acts by left multiplication, we get $V = \mathbb{C}[G]$ and $\rho = \rho^{reg}$. When $G = S_n$, and $S = \{1, 2, \dots, n\}$, we get $V = \mathbb{C}^n$ and $\rho = \rho^{std}$. As in these cases, it is easy to check that

$$\chi_\rho(g) = I(g) = \sharp \text{ fixed points of } g \text{ in } S.$$

Applying CFF and the projection formula, we get

$$\frac{1}{\sharp G} \sum_{g \in G} \chi_\rho(g) = \sharp \text{ orbits of } G \text{ in } S = \dim(V^G). \tag{14}$$

One way one may get such actions, is by choosing a subgroup $B < G$ and letting $S = G/B$, the set of left cosets of B in G (in fact, any set S on which G acts is a union of such examples). The representation is called the **coset representation**, which explains the name we have been using for the action of G on S throughout the course.

To make the situation even more specific, assume that

$$G = N \rtimes_\phi B.$$

Therefore, $G = NB, N \cap B = \{1\}$. Then,

$$G/B = \{nB : n \in N\}.$$

We check that $gnB = nB \Leftrightarrow g \in nBn^{-1}$. But,

$$nBn^{-1} = \{(n,1)(1,b)(n^{-1},1) : b \in B\} = \{(n\phi_b(n)^{-1}, b) : b \in B\}.$$

If $g = (n_1, b) \in nBn^{-1}$ it means that g necessarily equals to $(n\phi_b(n)^{-1}, b)$ for some n. We conclude that

$$\chi((n_1,b)) = I((n_1,b)) = \sharp\{n \in N : n_1 = n\phi_b(n)^{-1}\}.$$

Continuing with a general analysis will require making more assumptions on ϕ. Instead, let us take the case of $F_{20} = \mathbb{Z}/5\mathbb{Z} \rtimes_{id} (\mathbb{Z}/5\mathbb{Z})^\times$. Here, $n_1 = n\phi_b(n)^{-1}$ is written in additive notation and the condition is $n_1 = (1-b)n$. Now,

- if $b \neq 1$ there is a unique solution to the equation $n_1 = (1-b)n$.
- if $b = 1$ and $n_1 = 0$ there are 5 solutions to the equation $n_1 = (1-b)n$.

- if $b = 1$ and $n_1 \neq 0$ there are no solutions to the equation $n_1 = (1-b)n$.

We conclude that the character χ has the values $\chi(a_1) = 5, \chi(a_2) = 0, \chi(c_2) = \chi(c_3) = \chi(c_4) = 1$. Therefore,

$$\chi = \chi_4 + \chi_0,$$

and that tells us how the representation decomposes. Incidentally, note that the action of F_{20} on the 5 cosets of B gives us the inclusion $F_{20} \subset S_5$ we used before.

38.3. **A combinatorial application.** Let G be a finite group acting transitively on a finite non-empty set S. Let

$$G_0 = \{g \in G : g \text{ has no fixed point in } S\}.$$

G_0 is a subset of G, not a subgroup. We proved before (Proposition 17.1.3) that if $\sharp X \geq 2$ then

$$\sharp G_0 \geq 1.$$

Theorem 38.3.1 (Cameron-Cohen)**.**

$$\sharp G_0 \geq \frac{\sharp G}{\sharp X}.$$

Proof. Let $I(g) = \chi(g)$ be the number of fixed points of g in S, where χ is the character of the monomial representation of G coming from S.

Compare the proof of the following lemma to the proof of Lemma 34.3.1. It is really the same.

Lemma 38.3.2. *We have*

$$\frac{1}{\sharp G}\sum_{g\in G}\chi^2(g) \geq 2.$$

Proof. Consider the action of G on the set $S \times S$, $g(a,b) = (g(a), g(b))$. The class function χ^2 is the character of this representation and the dimension of the space of invariant vectors is $\frac{1}{\sharp G}\sum_{g\in G}\chi^2(g)$, which is equal to the number of orbits of G in $S \times S$ by Equation (14). To prove the lemma we only need to show that there is more than 1 orbit. And, indeed, one orbit is the diagonal $\{(s,s) : s \in S\}$ and, since $\|S\| \geq 2$, there must be at least one more orbit. □

Let $n = \sharp S$. Note that for $g \notin G_0$ we have $1 \leq \chi(g) \leq n$ and therefore

$$\frac{1}{\sharp G}\sum_{g\in G-G_0}(\chi(g)-1)(\chi(g)-n) \leq 0.$$

Therefore,

$$\frac{1}{\sharp G}\sum_{g\in G}(\chi(g)-1)(\chi(g)-n) \leq \frac{1}{\sharp G}\sum_{g\in G_0}(\chi(g)-1)(\chi(g)-n) = n\cdot\frac{\sharp G_0}{\sharp G}.$$

On the other hand,

$$\begin{aligned}\frac{1}{\sharp G}\sum_{g\in G}(\chi(g)-1)(\chi(g)-n) &= \frac{1}{\sharp G}\sum_{g\in G}\chi^2(g) - (n+1)\frac{1}{\sharp G}\sum_{g\in G}\chi(g) + \frac{1}{\sharp G}\sum_{g\in G} n \\ &\geq 2-(n+1)+n = 1.\end{aligned}$$

Combining the two inequalities, the theorem follows. □

J.-P. Serre used this in proving the following theorem in number theory.

Theorem 38.3.3. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial of degree n. The density of prime numbers p (in the set of all primes) such that f has no root modulo p is at least $1/n$.*

Example 38.3.4. If we take the most simple non-trivial situation $f(x) = x^2 + 1$, the theorem states that for at least $1/2$ the primes f has no zero modulo p.

On the other hand, f has a zero modulo p if and only if -1 is a square modulo p. As -1 has order 2 modulo p (if $p > 2$), this happens if and only if there are elements of order 4 in $\mathbb{Z}/p\mathbb{Z}^\times$. Using that $\mathbb{Z}/p\mathbb{Z}^\times$ is a cyclic group of order $p-1$ we see that this is the case if and only if $p \equiv 1 \pmod 4$. Thus, we conclude that the density of primes of the form $4k+3$ is at least $\frac{1}{2}$ (in fact, it is known to be precisely $1/2$).

39. Introduction to Fourier analysis on finite groups.

In this section we are following the fantastic book by P. Diaconis, *"Group representations in probability and statistics"* and if you find the following sections interesting, I very much recommend reading it; you should have essentially all the prerequisite knowledge for reading much of the book. Before commencing, let us mention that the theory of Fourier transform for groups has many applications to other branches of science (computer science, chemistry, physics, electrical engineering), and even within mathematics to many branches besides probability and statistics.

39.1. **Convolution.**

Let G be a finite group. Let

$$C(G,\mathbb{C}) = \{f\colon G \to \mathbb{C}\},$$

be the vector space of complex-valued functions on G. It is of course just the vector space $\mathbb{C}[G]$ we used many times before. A function f defines an element $\sum_g f(g)[g]$ of $\mathbb{C}[G]$, and conversely. It has dimension $\sharp G$.

For $g \in G$ define the **delta function** $\delta_g\colon G \to \mathbb{C}$ by

$$\delta_g(x) = \begin{cases} 1, & g = x; \\ 0, & \text{else.} \end{cases}$$

This function corresponds to $[g] \in \mathbb{C}[G]$. The collection $\{\delta_g : g \in G\}$ is a basis for $C(G,\mathbb{C})$.

We define the **convolution** of two functions $f, g \in C(G,\mathbb{C})$ as

$$(f * g)(x) = \sum_{s\in G} f(xs^{-1})g(s).$$

Note that for a non-abelian group in general $f * g \neq g * f$. In fact, convolution is just the product in the ring $\mathbb{C}[G]$; if we write an element of $\mathbb{C}[G]$ as $\sum_g a_g[g]$, where $a_g \in \mathbb{C}$, then

$$(\sum_g a_g[g]) + (\sum_g b_g[g]) = \sum_g (a_g + b_g)[g], \qquad (\sum_g a_g[g])(\sum_g b_g[g]) = \sum_g (\sum_s a_{gs^{-1}} b_s)[g].$$

And so, it is clear that $C(G,\mathbb{C})$ is a ring under addition of functions and convolution, with identity element δ_1. For the same reason, the following two properties are evident, nonetheless we prove the first in the language of convolutions.

- $\delta_g * \delta_h = \delta_{gh}$.
- $f = \sum_g f(g)\delta_g$.

Indeed, $(\delta_g * \delta_h)(x) = \sum_{s\in G} \delta_g(xs^{-1})\delta_h(s) = \delta_g(xh^{-1})$, which is a function that is everywhere zero except at $x = gh$ where it is 1. Thus, $\delta_g * \delta_h = \delta_{gh}$.

39.2. **The Fourier transform.** The **Fourier transform** $\hat{f}$ of a function $f \in C(G, \mathbb{C})$ is a function on representations (ρ, V) of G. It associate to a representation ρ the element

$$\hat{f}(\rho) = \sum_{s \in G} f(s)\rho(s) \in \mathrm{End}(V).$$

In this part of the course, we will always assume that the representations are unitary, which we can always achieve by a suitable inner-product (cf. the proof of Maschke's theorem, Theorem 32.2.2).

Lemma 39.2.1. *We have the following properties of the Fourier transform:*

1. $\widehat{f+g} = \hat{f} + \hat{g}$, *and* $\widehat{\alpha f} = \alpha \hat{f}$, $\alpha \in \mathbb{C}$.
2. $\hat{\delta}_g(\rho) = \rho(g)$.
3. $\widehat{f * g} = \hat{f} \cdot \hat{g}$.
4. *Let U be the* **uniform distribution** *on G, $U(g) = \frac{1}{|G|}, \forall g \in G$. Let (ρ, V) be a representation of G. Then $\hat{U}(\rho)$ is the projection operator on the sub-representation V^G. Thus, if ρ is irreducible and $\rho \not\cong \mathbb{1}$ then $\hat{U}(\rho) = 0$, while $\hat{U}(\rho)(\mathbb{1}) = Id$.*

Proof. The first two properties are immediate from the definition. For the third, let (ρ, V) be a representation of G. Then,

$$\begin{aligned}\widehat{f * g}(\rho) &= \sum_{s \in G} (\sum_{t \in G} f(st^{-1}) g(t)) \cdot \rho(s) \\ &= (\sum_{x \in G} f(x)\rho(x))(\sum_{t \in G} g(t)\rho(t)) \\ &= \hat{f}(\rho) \cdot \hat{g}(\rho).\end{aligned}$$

(The last product means product in the ring $\mathrm{End}(V)$).

The fourth property is just the definition of the projection operator and the fact that V^G is a subrepresentation of V. □

39.3. **Fourier Inversion and Plancherel's formula.** The following theorem is very much reminiscent of Fourier analysis over $\mathbb{R}$.

Theorem 39.3.1. *Let $\rho_1, \dots, \rho_h$ be unitary representatives for the irreducible representations of G and let $d_i = \dim(\rho_i)$, $\chi_i = \chi_{\rho_i}$.*

1. *(Fourier Inversion). For any function $f \in C(G, \mathbb{C})$,*

$$f(s) = \frac{1}{|G|} \sum_{i=1}^{h} d_i \cdot \mathrm{Tr}(\rho_i(s^{-1})\hat{f}(\rho_i)). \tag{15}$$

2. *(Plancherel's formula) For any two functions $f, h \in C(G, \mathbb{C})$,*

$$\sum_{s \in G} f(s^{-1})h(s) = \frac{1}{|G|} \sum_{i=1}^{h} d_i \mathrm{Tr}(\hat{f}(\rho_i)\hat{h}(\rho_i)). \tag{16}$$

Proof. The proof is surprisingly simple for such scary looking formulas. First note that by linearity and bilinearity, it is enough to prove Fourier inversion for the functions δ_g, and the Plancherel formula for the functions δ_g, δ_h. We first verify Fourier inversion for δ_g. In this case, the right hand side of (15) evaluated at s is:

$$\begin{aligned}\frac{1}{|G|}\sum_{i=1}^{h} d_i \cdot \mathrm{Tr}(\rho_i(s^{-1})\hat{\delta}_g(\rho_i)) &= \frac{1}{|G|}\sum_{i=1}^{h} d_i \cdot \mathrm{Tr}(\rho_i(s^{-1})\rho_i(g)) \\ &= \frac{1}{|G|}\sum_{i=1}^{h} d_i \cdot \mathrm{Tr}(\rho_i(s^{-1}g)) \\ &= \frac{1}{|G|}\sum_{i=1}^{h} d_i\chi_i(s^{-1}g) \\ &= \frac{1}{|G|}\rho^{reg}(s^{-1}g).\end{aligned}$$

This is a function that vanished everywhere, except at $s = g$, where it receives the value 1. Namely, this is just the function $\delta_g(s)$, as required.

The right-hand side of Plancherel's formula (16) is equal to

$$\begin{aligned}\frac{1}{|G|}\sum_{i=1}^{h} d_i\mathrm{Tr}(\hat{\delta}_g(\rho_i)\hat{\delta}_h(\rho_i)) &= \frac{1}{|G|}\sum_{i=1}^{h} d_i\mathrm{Tr}(\rho_i(g)\rho_i(h)) \\ &= \frac{1}{|G|}\sum_{i=1}^{h} d_i\mathrm{Tr}(\rho_i(gh)) \\ &= \frac{1}{|G|}\sum_{i=1}^{h} d_i\chi_i(gh) \\ &= \frac{1}{|G|}\rho^{reg}(gh).\end{aligned}$$

This expression is equal to 1 if $g = h^{-1}$, and is equal to 0 otherwise. The sum

$$\sum_{s\in G}\delta_g(s^{-1})\delta_h(s)$$

has exactly the same property, and we get the equality we were after. □

We now derive a variant of Plancherel's formula that is very useful for applications. Recall the (potentially confusing, but customary) notation for a complex matrix M: $M^* = \bar{M}^t$.

Corollary 39.3.2. *Let f be a real-valued function then*

$$\sum_{s\in G} f(s)h(s) = \frac{1}{|G|}\sum_{i=1}^{h} d_i \cdot \mathrm{Tr}((\hat{f}(\rho_i))^* \cdot \hat{h}(\rho_i)). \tag{17}$$

Proof. Let g be the function $g(s) = f(s^{-1})$. Then $\sum_{s\in G} f(s)h(s) = \sum_{s\in G} g(s^{-1})h(s)$ and we can apply Plancherel's formula to this sum. It only remains to note that for $\rho = \rho_i$ for some i,

$$\hat{g}(\rho) = \sum_s f(s^{-1})\rho(s) = \sum_s f(s)\rho(s^{-1}) = \sum_s f(s)\rho(s)^* = (\sum_s f(s)\rho(s))^* = \hat{f}(\rho)^*,$$

where we used that ρ_i is unitary and f is real-valued. □

39.4. **Random walks on cyclic groups.** Let p be a positive integer and consider the integers modulo p, $\mathbb{Z}/p\mathbb{Z}$. For various applications in cryptography, statistics, computer science and more, it is of interest to randomly choose a congruence class modulo p, or to emulate a random walk on $\mathbb{Z}/p\mathbb{Z}$. True randomness is hard; it's hard to generate and hard to "excavate" from nature. For that reason, one tries to expand, or stretch, a small amount of randomness to create a process that is pseudo-random; it is not completely random, but for all practical purposes, it is.

Consider then the following process

$$x_{k+1} = a_k x_k + b_k, \quad k = 1, 2, \dots.$$

At each iteration a_k and b_k can be chosen among the classes $(\mathbb{Z}/p\mathbb{Z})^\times$ and $\mathbb{Z}/p\mathbb{Z}$, respectively, according to some agreed upon distribution. (This process is related to pseudo-random number generators, but we will now get into that here.) The simplest situation that is not completely deterministic is

$$a_k = 1, \forall k, \quad b_k \text{ chosen from } \{\pm 1\} \text{ with equal probability.}$$

This process just requires a fair coin-toss at every step.

Let us denote functions on $\mathbb{Z}/p\mathbb{Z}$ by vectors $(a_0, \dots, a_{p-1})$. And let us suppose that the initial seed is $x_0 = 0$, namely, it is the vector $(1, 0, \dots, 0)$ with probability 1. Then, the distribution after one iteration is $P = (0, 1/2, \dots, 1/2)$, and after n-steps it is given by $P^{*n} := P * P * \cdots * P$ (convolution n-times). For example, applying the random walk twice, it is clear that we can only end at $0, 2$ of $-2 = n - 2$, and the probability we end at 0 can be found as

$$P(b_1 = 1) \cdot P(b_2 = -1) + P(b_1 = -1) \cdot P(b_2 = 1) = \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2}.$$

Similarly the probability for ending at 2 is $P(b_1 = 1) \cdot P(b_2 = 1) = 1/4$, and so on. We recognize that we are just calculating $P * P$. For example, $P * P(0) = \sum_{j=0}^{p-1} P(j)P(-j) = P(1)P(p-1) + P(p-1)P(1) = 1/2$.

Let us switch for a moment to multiplicative notation (which will hopefully be less confusing), and write $\mathbb{Z}/p\mathbb{Z} = \langle t \rangle$ where $t^p = 1$. Using the group-ring presentation, we can say that

$$P = \frac{1}{2}(t + \frac{1}{t}),$$

and so

$$P^{*n} = \frac{1}{2^n}(t + \frac{1}{t})^n = \frac{1}{2^n} \sum_{j=0}^{n} a_j(n) t^j,$$

where

$$a_j(n) = \sum_{i \in \{0, \dots, n\}, 2i - n \equiv j(p)} \binom{n}{i}.$$

The limiting distribution is thus

$$\lim_{n \to \infty} P^{*n} = \lim_{n \to \infty} (a_0(n), a_1(n), \dots, a_{p-1}(n)).$$

Our main interest is to know whether $\lim_{n \to \infty} P^{*n}$ approaches the uniform distribution U, and, if so, how fast? The fact that it approaches U is fairly easy (and follows from basic theory of Markov chains). The main question is how quickly it approaches U.

To gauge this we introduce the **total variation norm** $\| \cdot \|_{max}$. Let G be a finite group. For any two probability distributions $P, Q \in C(G, \mathbb{C})$ we let

$$\|P - Q\|_{max} = \max_{A \subset G} |P(A) - Q(A)| = \frac{1}{2} \sum_{g \in G} |P(g) - Q(g)|,$$

where $P(A) = \sum_{a \in A} P(a)$ is the probability of the event A.

Lemma 39.4.1 (Diaconis-Shahshahani). *Let G be a finite group with irreducible (unitary) representations $\rho_1 = \mathbb{1}, \dots, \rho_h$. and let P be a probability distribution on G. Then,*

$$\|P - U\|_{max}^2 \leq \frac{1}{4} \sum_{i=2}^{h} d_i \cdot \mathrm{Tr}(\hat{P}(\rho_i)^* \cdot \hat{P}(\rho_i)).$$

(Namely, the trivial representation $\mathbb{1}$ is the only one not appearing in this sum.)

We will prove this lemma later on. Let us first see its application for the process we are discussing. In this case, recall that the irreducible representations of $\mathbb{Z}/p\mathbb{Z}$ are the 1-dimensional representations $\{\rho_j : j = 0, 1, \ldots, p-1\}$, where

$$\rho_j(a) = \zeta^{aj} \quad (\zeta = e^{2\pi i/p}).$$

(Namely, ρ_j is the character such that $\rho_j(1)$ is the p-th root of unity $e^{j2\pi i/p}$.) Then,

$$\hat{P}(\rho_j) = \frac{1}{2}(\rho_j(1) + \rho_j(-1)) = \cos(2\pi j/p).$$

By multiplicativity of the Fourier transform,

$$\hat{P}^{*n}(\rho_j) = \cos(2\pi j/p)^n.$$

Applying the Diaconis-Shahshahani lemma we find

$$\|P^{*n} - U\|^2_{max} \leq \frac{1}{4}\sum_{j=1}^{p-1}\cos(2\pi j/p)^{2n}.$$

This last sum, though elementary in appearance, is not that easy to estimate, yet a relatively elementary argument gives a bound and one gets the following, if $p \geq 7$ and **odd**:

$$\|P^{*n} - U\|^2_{max} \leq e^{-\frac{\pi^2}{2}\cdot\frac{n}{p^2}}.$$

This can be formulated qualitatively as saying that

"for $a_k \equiv 1$, and b_k chosen uniformly from the set $\{1, -1\}$, about p^2 iterations of the process

$$x_{k+1} = a + kx_k + b_k$$

are required to achieve a distribution close to the uniform distribution."

One can perform a similar analysis for the case $a_k = 1$ and b_k chosen uniformly from $\{0, 1, -1\}$ and get a very similar result. On the other hand, in stark-contrast, one can prove the following results for p such that $\gcd(p, 6) = 1$:

"for $a_k \equiv 3$, and b_k chosen uniformly from $\{1, -1\}$, about $\log p$ iterations of the process $x_{k+1} = a_kx_k + b_k$ are required to achieve a distribution close to the uniform distribution."

One reason the estimates are so different is that we are transferring from representation theory for the group $\mathbb{Z}/p\mathbb{Z}$ to representation theory for the group $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}^\times$. The process $x_{k+1} = 3x_k + b_k$ is thought of as coming from a random walk on the group $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}^\times$ corresponding to taking powers of the random element $(b, 3)$, where $b = \{1, 0, -1\}$ with equal probability. See Exercise 39.4.2

Exercise 39.4.2. Prove that last estimate using the Diaconis-Shahshahani lemma for the group $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}^\times$. (Finding the representations is Exercise **??**.)

39.5. **Proof of the Diaconis-Shahshahani lemma.** Let us now prove the lemma. Recall the statement:

Let G be a finite group with irreducible (unitary) representations $\rho_1 = \mathbb{1}, \ldots, \rho_h$. and let P be a probability distribution on G then

$$\|P - U\|^2_{max} \leq \frac{1}{4}\sum_{i=2}^{h} d_i \mathrm{Tr}(\hat{P}(\rho_i)^* \cdot \hat{P}(\rho_i)).$$

(Namely, the trivial representation $\mathbb{1}$ is the only one not appearing in this sum.)

Proof. Applying the Cauchy-Schwarts inequality for real numbers $(\sum a_n b_n)^2 \leq (\sum a_n^2)(\sum b_n^2)$ and taking all the $b_n = 1$, we find that

$$4\|P-U\|_{max}^2 = (\sum_{s\in G} |(P(s)-U(s)|)^2 \leq \sharp G \cdot \sum_{s\in G}(P(s)-U(s))^2.$$

We view the last sum as $\sum_{s\in G} f(s)h(s)$, where $f(s) = h(s) = (P(s)-U(s))$. Apply the version of Plancherel's formula given in Corollary 39.3.2 to find

$$\sharp G \cdot \sum_{s\in G}(P(s)-U(s))^2 \leq \sum_{i=1}^{h} d_i \mathrm{Tr}(\hat{f}(\rho)^* \cdot \hat{f}(\rho))$$

Now, $\hat{f}(\rho_i) = (\hat{P}-\hat{U})(\rho_i)$ and, using Lemma 39.2.1, we see that it is equal to $\hat{P}(\rho_i)$ for $\rho_i \neq \mathbb{1}$ (i.e., for $i > 1$), while $\hat{f}(\mathbb{1}) = (\hat{P}-\hat{U})(\mathbb{1}) = 1-1 = 0$. Therefore, we find

$$\sum_{i=1}^{h} d_i \mathrm{Tr}(\hat{f}(\rho)^* \cdot \hat{f}(\rho)) = \sum_{i=2}^{h} d_i \mathrm{Tr}(\hat{P}(\rho)^* \cdot \hat{P}(\rho)),$$

and the proof is complete. □

39.6. **Riffle shuffles.** This is a famous problem that one can attack by similar techniques. The actual estimates are very difficult though and, in any case, not accessible to us because they require full and detailed knowledge of the representation theory of the symmetric group. It is interesting, nonetheless, to see how the problem is set up and the first steps of the analysis.

A deck of cards, consisting of N cards ($N = 52$ in a usual deck) is split into two piles, one with k cards and the other with $N-k$ cards, with probability $\frac{1}{2^N}\binom{N}{k}$. Say, the left pile and the right pile. Then the cards from the two piles are interleaved randomly, where a card is chosen from the left pile with probability k/N and from the right pile with probability $(N-k)/N$. In the new pile the cards appear in a new order that is a permutation $\pi \in S_N$. Such a permutation is called, naturally enough, a **shuffle**, and the process of shuffling cards this way is called **riffle shuffle** or **dovetail shuffle**. It has the following form for some k

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & \dots & \dots & N-2 & N-1 & N \\ k+1 & 1 & 2 & k+2 & 3 & k+4 & \dots & k-2 & \dots & k-1 & N & k \end{pmatrix}$$

Experiments show that this is a good model for real-life card shuffles.

After n shuffles we get a certain probability distribution on S_N. If P is the original distribution, the distribution after n shuffles is P^{*n}. It is easy to understand the distribution P. We have $P(\pi) = 0$ if π is not a k-shuffle for any k, and $P(\pi) = 2^{-N}$ if π is a k-shuffle. But it is complicated to describe P^{*n} (and you can convince yourself of that by considering the case $n = 2$); more sophisticated methods are needed.

Similarly to the case of random walks on $\mathbb{Z}/p\mathbb{Z}$, routine arguments with Markov chains show that $P^{*n} \to U$ relative to the total variation norm. The question is how fast? Once more the main idea is to use the Diaconis-Shahshahani Lemma to get an estimate of the form

$$\|P^{*n}-U\|_{max}^2 \leq \frac{1}{4} \sum_{\rho\neq\mathbb{1},\ \text{irred.}} \dim(\rho) \cdot \mathrm{Tr}((\hat{P}(\rho)^*)^n \cdot (\hat{P}(\rho))^n),$$

where now ρ runs over all irreducible representations of S_n and that, on the other hand, even 5 shuffle will exhibit significant bias towards particular permuations.

The following table (their Q is our P) is taken from a paper of Bayer and Diaconis. It shows that 7 shuffles suffice to shuffle reasonably-well a deck of 52 cards.

Total variation distance for m shuffles of 52 cards

m	1	2	3	4	5	6	7	8	9	10
$\|Q^m - U\|$	1.000	1.000	1.000	1.000	0.924	0.614	0.334	0.167	0.085	0.043

39.7. **Rubik's cube.** We have discussed Rubik's cube in §17.3. in particular, we introduced the notation U, D, F, B, L, R and the Cayley graph relative to the generators $U^i, D^i, F^i, B^i, L^i, R^i$, $i = 1, 2, 3$. There is a rational for using these redundant set of generators; in practice, the moves $U^2, U^3 = U^{-1}$, for example, take almost the same time as U.

In cube solving competitions, cube scramblers are used. These are computer programs that produce a position of the cube and a set of instructions of how to get to it that judges use to create the cube positions to be solved. Naturally, we wish to have all cube positions given to the participants "equally hard", and also "hard enough" so that undeserving achievements will not be recorded as world-records. One needs to find a method that produces such positions. The scramblers are choosing randomly generators to provide directions for creating the cube positions. However, we would like to guarantee that (with high probability) such sets of directions lead to equally hard positions that are also among the hardest possible.

The question of which position requires the most moves to solve was open for a long time and was finally settled by Rokicki et al. that determined this number to be 20. (This number is known as "God's number"; I don't personally like this terminology.) The following table is taken from a paper of Rokicki; the first column indicates the minimal number of moves required to solve a position and the last column indicates the number of cube positions requiring this number. We ignore the middle column; it relates to the method of analysis used in their paper.

d	Canonical sequences	Positions
0	1	1
1	18	18
2	243	243
3	3,240	3,240
4	43,254	43,239
5	577,368	574,908
6	7,706,988	7,618,438
7	102,876,480	100,803,036
8	1,373,243,544	1,332,343,288
9	18,330,699,168	17,596,479,795
10	244,686,773,808	232,248,063,316
11	3,266,193,870,720	3,063,288,809,012
12	43,598,688,377,184	40,374,425,656,248
13	581,975,750,199,168	531,653,418,284,628
14	7,768,485,393,179,328	6,989,320,578,825,358
15	103,697,388,221,736,960	91,365,146,187,124,313
16	1,384,201,395,738,071,424	≈1,100,000,000,000,000,000
17	18,476,969,736,848,122,368	≈12,000,000,000,000,000,000
18	246,639,261,965,462,754,048	≈29,000,000,000,000,000,000
19	3,292,256,598,848,819,251,200	≈1,500,000,000,000,000,000
20	43,946,585,901,564,160,587,264	≈300,000,000

We see that the bulk of the cube positions require 18 moves. It is thus natural to perform the random process P and hope that P^{*n} is very closed to a distribution Q that has values, say, $Q(17) \approx Q(19) \approx 0.05$, $Q(18) \approx 0.90$ and otherwise $Q(i) \approx 0$. But, is it possible?? More precisely, what is

$$\min_n \|P^{*n} - Q\|_{max}.$$

I don't know the answer to that. (A careful analysis might require understanding the representations of the Cube group.) In real-life, the *Tnoodle scrambler program* is used by the World Cube Association to generate positions and the quality bar seems pretty low. At some point in time, they were OK with producing cube positions only guaranteed to require 11 moves or more, which seems rather bad. By simply running the program for say 1,000 times for each $n = 15 - 25$ and using fast cube-solvers, one could get a very reliable statistics on this question. The whole project shouldn't take more than a week to run a desktop computer.

40. 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 did not discuss at all (such as the theory of modules and algebraic integers).

Finally, but still within the realm 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 to 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.

(5) In number theory, representations of groups play a central role. The subject of automorphic forms is really about the representations theory of certain infinite groups. At a more accessible level, group representations play an important role in the study of L-functions, and in the study of equations over finite fields (for example, Gauss sums can be viewed as Fourier transforms). For a concrete example, in a different direction, we might mention Roth's theorem.

A subset A of the natural numbers is said to have positive **upper density** if

$$\limsup_{n\to\infty} \frac{|A \cap \{1,2,3,\dots,n\}|}{n} > 0.$$

Roth's theorem on arithmetic progressions states that a subset of the natural numbers with positive upper density contains a 3-term arithmetic progression; namely, there are positive integers x, d such that $x, x+d, x+2d$ belong to A. This is a surprisingly difficult theorem, and many people have worked on various generalizations of it. This is a subject of ongoing research. Roth's proof, as well as current day developments, use heavily the Fourier analysis on the group $\mathbb{Z}/n\mathbb{Z}$.

41. 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 its 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 (i) tensor products of representations and their decomposition; some study of (ii) the representations of symmetric group and their connections to Young tableaux, hook lengths and other mysterious terminology; (iii) 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; (iv) 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) Consider the symmetric group S_7.
   (a) Calculate the order of the following element of S_7: $(2\ 3\ 5)(7\ 1)(4\ 2)(3\ 4\ 5\ 1)(6\ 5)$.
   (b) Find an element of order 12 in S_7.
   (c) Prove that S_7 doesn't have an element of order 15.

(6) Let $n \geq 3$, an integer. Consider the dihedral group D_n with $2n$ elements. It has generators x, y that satisfy $x^n = y^2 = 1$ and $yxy = x^{-1}$. Show that $yx^a y = x^{-a}$ for any integer $a > 0$. Show algebraically that every element of D_n that is not a power of x has order 2.

(7) Let $n \geq 3$, an integer. Find two elements of order 2 of D_n that together generate it.

(8) Let G be a group and let x, y be elements of G that commute: $xy = yx$. Let n be the order of x and m the order of y. Assume that $\gcd(n, m) = 1$. Show the following.
   - $\langle x \rangle \cap \langle y \rangle = \{1_G\}$.
   - The order of the element xy is mn.
   - Show that the assumption that x and y commute is necessary. (One can find a counter-example already in S_3.)

(9) 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.

(10) 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.

(11) Identify S_3 as a subgroup of S_4 by thinking about elements of S_3 as permutations that fix the element 4. Prove that a subgroup of S_4 that contains S_3 is either equal to S_3 or to S_4.

(12) Let $\alpha \in \mathbb{R}^n$, $n \geq 2$, be a non-zero vector. We define a reflection in the hyperplane perpendicular to α 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 σ_α is indeed a linear map that fixes the hyperplane orthogonal to α and sends α to $-\alpha$. Given α, β 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 $n = 2$.)

(13) Let T be a non-empty set (possibly infinite) and define Σ_T as the set of all functions $f \colon T \to T$ that are bijective. Show that Σ_T is a group under composition of functions (if $T = \{1, 2, \dots, n\}$ we can identify Σ_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.

(14) Let G be a finite group and $H_1 \subset H_2$ be subgroups of G such that $[H_2 : H_1] = p$, a prime number. Prove that if J is a subgroup of G such that $H_1 \subseteq J \subseteq H_2$ then either $H_1 = J$ of $H_2 = J$.

(15) Let G be a group and let $H_1 \subset H_2$ be subgroups of G. Prove that the index is multiplicative:
$$[G : H_1] = [G : H_2][H_2 : H_1].$$
If you know how to work well with infinite sets, prove this assertion as equalities of cardinalities. If not, assume that $[G : H_1]$ is a finite integer, and prove the assertion as an equality of integers. (In particular, using this claim, there is no need to assume in Exercise (14) that G is a finite group.)

(16) 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?).

(17) The Euler function φ,
$$\varphi : \mathbb{Z}_{>0} \to \mathbb{Z},$$
defined by
$$\varphi(n) = \sharp\{0 < a \leq n : \gcd(a, n) = 1\}.$$
Prove that it has the following properties:
- If n and m are relatively prime then $\varphi(nm) = \varphi(n)\varphi(m)$.
- If p is a prime $\varphi(p^a) = p^a - p^{a-1}$.
- $\varphi(n) = n\prod_{p|n}(1 - 1/p)$ (the product taken over the prime divisors p of n).

(18) Let $\mathbb{F}$ be a finite field with q elements.
(a) Let $n \geq 1$ be an integer. How many solutions does the equation
$$x^n - 1 = 0$$
has in $\mathbb{F}$?
(b) Find the solutions for $x^n - 1 = 0$ in $\mathbb{F} = \mathbb{Z}/11\mathbb{Z}$ for $n = 2, 3, 4, 5$. (You may use that 2 generates the cyclic group $(\mathbb{Z}/11\mathbb{Z})^\times$.)

(19) Let $\mathbb{F} \subset \mathbb{L}$ be finite fields, $\sharp\ \mathbb{F} = q$.
(a) Prove that $\sharp\ \mathbb{L} = q^n$ for some integer $n \geq 1$.
(b) Prove that for every $a \in \mathbb{F}$ we have $a^q = a$ and that every $a \in \mathbb{L}$ that satisfies $a^q = a$ is actually in $\mathbb{F}$. (Hint: what do we know about $\mathbb{F}^\times$?)
(c) Prove that the map $x \mapsto x^{(q^n-1)/(q-1)}$ defines a surjective homomorphism $\mathbb{L}^\times \to \mathbb{F}^\times$.

(20) 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 $B = \{a \in \mathbb{Z}/p^n\mathbb{Z} : a \equiv 1 \pmod{p}\}$.

(21) 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.

(22) (**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. [17]

(23) Use group theory to prove Wilson's theorem: For every prime p, $(p-1)! \equiv -1 \pmod{p}$.

[17] 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 primes are known. In particular, $2^{2^5} + 1 = 4294967297$ was famously factored by L. Euler as 641×6700417, and it is 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.

(24) 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.

(25) 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 $G_1 \ncong G_2$.

(26) Give an example of groups $A \lhd B \lhd C$ such that A is not normal in C.

(27) Let $\sigma \in S_n$ be a permutation. Find a formula (in terms of the factorization of σ into disjoint cycles) for the cardinality of $\mathrm{Cent}_{S_n}(\sigma)$. Fix n; for which permutations σ the minimum is obtained?

(28) Give an example of a group G and a subgroup $H \neq \{1\}$ of G for which $H \cap \mathrm{Cent}_G(H) = \{1\}$ and $\mathrm{Cent}_G(H) \neq \{1\}$.

(29) Prove that if $N < G$ and $[G : N] = 2$ then $N \lhd G$. (This can be done without using group actions.)

(30) Let $m < n$ be positive integers. Calculate $N_{S_n}(S_m)$. In particular, find when $N_{S_n}(S_m) = S_m$.

(31) Find two subgroups A, B of the symmetric group S_4 that have the following properties: (1) they are both isomorphic to the group S_3; (2) they generate S_4: $\langle A, B\rangle = S_4$.

(32) Prove that the alternating group A_4 is generated by $\{x, y\}$, for any choice of $x \in A_4$ an element of order 3, and for any choice of $y \in A_4$ as an element of order 2.

(33) Prove that S_4 is generated by $\{x, y\}$, for a suitable choice of an element x of order 3 and for a suitable choice of an element y of order 2.

(34) 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.

(35) *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. Prove also that the commutator subgroup G' is a characteristic subgroup.
  (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.

(36) If G, H are finite groups such that $(|G|, |H|) = 1$ prove that every group homomorphism $f : G \to H$ is trivial ($f(G) = \{1\}$).

(37) 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).

(38) Find the centralizer in $\mathrm{GL}_3(\mathbb{R})$ of each of the following matrices

$$\begin{pmatrix} 1 & & \\ & 2 & \\ & & 3 \end{pmatrix}, \quad \begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & \end{pmatrix}, \quad \begin{pmatrix} 1 & & \\ & -1 & \\ & & 1 \end{pmatrix}.$$

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 is 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.

(39) 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.

(40) Let G be a finite group with a unique maximal subgroup. Prove that G is cyclic of prime power order.

(41) Prove that $\mathbb{Q}$, considered as an abelian group relative to addition, has no maximal subgroups.

(42) Let A, B be normal subgroups of a group G and suppose that $G = AB$. Prove that

$$G/(A \cap B) \cong G/A \times G/B.$$

(43) Let G be a group. Let $\text{Aut}(G)$ be the collection of automorphisms of G (isomorphisms from the group onto itself). Show that $\text{Aut}(G)$ 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 $\tau_g \in \text{Aut}(G)$ and that the map $G \to \text{Aut}(G), g \mapsto \tau_g$, 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 $\text{Inn}(G)$. Prove that $\text{Inn}(G)$ is a normal subgroup of $\text{Aut}(G)$. The quotient group $\text{Aut}(G)/\text{Inn}(G)$ is called the **outer automorphism group** of G and is denoted $\text{Out}(G)$.

(44) Prove that $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. More generally, prove that

$$\text{Aut}((\mathbb{Z}/n\mathbb{Z})^N) \cong \text{GL}_N(\mathbb{Z}/n\mathbb{Z}) := \{M = (m_{i,j})_{i,j=1}^N : m_{i,j} \in \mathbb{Z}/n\mathbb{Z}, \det(M) \in (\mathbb{Z}/n\mathbb{Z})^\times\}.$$

(45) In this exercise we shall prove that $\text{Aut}(S_n) = S_n$ 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 $\sharp\text{Aut}(S_n) \leq n!$.

(d) Show that for $n > 6$ there is an isomorphism $S_n \cong \text{Aut}(S_n)$.

(46) Let $T = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and consider the following permutations on the set T:

$$\sigma(x, y) = (y, x), \quad \alpha(x, y) = (x + 1, y + 2).$$

Let $H = \langle \sigma, \alpha \rangle$ be the subgroup of the permutation group of T generated by σ and α.

(a) Prove that H is not commutative by calculating $[\alpha, \sigma]$.

(b) Determine the number of orbits of H in T and the size of every orbit. (Hint: it is useful to consider the function $(x, y) \mapsto x + y \pmod 3$).

(c) Prove that H has more than 12 elements.

(47) **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.

(48) 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.)

(49) Let H, K be subgroups of a group G. Prove that

$$[G : H \cap K] \leq [G : H] \cdot [G : K].$$

(50) Find the number of necklaces with 16 beads, 8 of them blue, 4 red and 4 white, up to symmetries by D_{16}.

(51) Find the number of necklaces with 12 beads, 2 red, 4 green, 3 blue and 3 yellow, up to symmetries by D_{12}.

(52) 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.)

(53) 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).

(54) 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?

(55) 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.)

(56) 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 $G/(K\ \mathrm{Stab}_G(s))$.

(57) 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 Γ of rigid transformation of the cube was isomorphic to S_4. We can deduce that Γ 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.

(58) Show that the symmetric group S_5 can be made to act transitively on a set of size 6 or 10, but that it cannot act transitively on a set of size 8.

(59) 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 colour.)

(60) The German artist Gerhard Richter created the art installation "4900 Colours: Version II", exhibited in the Serpentine Gallery in London in 2008. The installation is created by combining glass panels, where each panel is composed of 5×5 squares, coloured in one of 25 possible colours. If you are interesting in learning more about this, see the beautiful article by David Spiegelhalter,

https://plus.maths.org/content/understanding-uncertainty-pure-randomness-art

(but this is not required for solving the question). If we wanted to count the number of such distinct 5×5 panels, we can rotate them, but as glass panels are transparent we can also flip them over.

(a) Suppose we only used 3 colours (instead of Richter's 25 colours).[18] How many such distinct glass panels can be created then, up to such symmetries? (To clarify, we do not pose any constrains on the panels, so we also allow monochromatic panels and so on...)

(b) What is the probability that a 3-coloured glass panel thus created randomly actually has only 2 colours?

(61) Prove that the free group on 2 elements, $\mathscr{F}_2$ has a subgroup of index n for every positive integer n.

(62) (Flags and Parabolic subgroups) Let $n \geq 1$ be an integer, $\mathbb{F}$ a field and $G = \mathrm{GL}_n(\mathbb{F})$. Then G acts on $\mathbb{F}^n$ by $(M, v) \mapsto Mv$.

(a) Prove that there are precisely two orbits: $\{0\}$ and $\mathbb{F}^n - \{0\}$.

(b) Let $1 \leq d_1 < d_1 < \cdots < d_r < n$ be integers ($r \geq 1$) that we fix from now on. A **flag** $V^\bullet$ of type $(d_1, d_2, \dots, d_r)$ in $\mathbb{F}^n$ is a collection of sub vector spaces

$$V^\bullet : \{0\} \subsetneqq V_1 \subsetneqq V_2 \subsetneqq \cdots \subsetneqq V_r \subsetneqq \mathbb{F}^n, \qquad d_i = \dim(V_i).$$

For example, for e_i the usual basis of $\mathbb{F}^n$, we have the standard flag $V^\bullet_{st}$, where

$$V_i = \mathrm{Span}(e_1, \dots, e_{d_i}).$$

Let $\mathscr{F}_{(d_1,d_2,\dots,d_r)}$ be the set of all flags of type $(d_1, d_2, \dots, d_r)$ in $\mathbb{F}^n$. Prove that $\mathrm{GL}_n(\mathbb{F})$ are transitively on $\mathscr{F}_{(d_1,d_2,\dots,d_r)}$ and calculate $\mathrm{Stab}(V^\bullet_{st})$.[19]

(c) Assume now that $\mathbb{F}$ is a finite field with q elements. Give a formula for the cardinality of $\mathscr{F}_{(d_1,d_2,\dots,d_r)}$, $\mathrm{Stab}(V^\bullet_{st})$, and $[\mathrm{GL}_n(\mathbb{F}) : \mathrm{Stab}(V^\bullet_{st})]$.
Here is an example: let $n = 4$, $(d_1, \dots, d_r) = (2)$. Then $\mathscr{F}_{(2)}$ is the collection of planes in $\mathbb{F}^4$. The standard flag is

$$V^\bullet_{st} : \mathrm{Span}(e_1, e_2).$$

The stabilizer is the group of matrices of the form:

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix},$$

[18] If I had asked you about Richter's original choice of 25 possible colours, the answer would have been on the order of magnitude of 10^{34}, a number too big to be interesting.

[19] This subgroup is an example of a parabolic subgroup of $\mathrm{GL}_n(\mathbb{F})$ and all parabolic subgroups are those conjugate to $\mathrm{Stab}(V^\bullet_{st})$ of some $(d_1, d_2, \dots, d_r)$.

where $A, D \in \mathrm{GL}_2(\mathbb{F}), B \in M_2(\mathbb{F})$.
If we take $(d_1, d_2, \dots, d_r) = (1, 2)$, the standard flag is $\mathrm{Span}(e_1) \subset \mathrm{Span}(e_1, e_2)$ and the stabliizer are the matrices of the form

$$\begin{pmatrix} a & \star & \star & \star \\ 0 & b & \star & \star \\ 0 & 0 & c & d \\ 0 & 0 & e & f \end{pmatrix},$$

where a, b are non-zero elements of $\mathbb{F}$, the $\star$ are (any) elements of $\mathbb{F}$, and $\left(\begin{smallmatrix} c & d \\ e & f \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F})$.

(63) Let $\mathbb{F}_q$ be a finite field with q elements. The group $\mathrm{GL}_2(\mathbb{F}_q)$ acts transitively on $\mathbb{F}_q^2 - \{0\}$ (cf. Exercise 62). Consider the following 3 subgroups of $\mathrm{GL}_2(\mathbb{F}_q)$ and their induced action on $\mathbb{F}_q^2 - \{0\}$,

$$B = \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) : a, b, d \in \mathbb{F}_q, ad \neq 0\}, \quad C = \{\left(\begin{smallmatrix} 1 & b \\ 0 & d \end{smallmatrix}\right) : b, d \in \mathbb{F}_q, d \neq 0\},$$
$$D = \{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) : a, b \in \mathbb{F}_q, a \neq 0\}.$$

How many orbits they have? (Although this can be done using just linear algebra, it's better if you use also the Cauchy-Frobenius formula.)

(64) Prove that for $n \geq 5$, A_n is the unique non-trivial normal subgroup of S_n.

(65) 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.

(66) For which n, if any, is there an injective homomorphism $S_n \to A_{n+1}$?

(67) Prove that for $n \geq 5$ the commutator subgroup of S_n is A_n.

(68) 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.

(69) 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.

(70) 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).

(71) Write the conjugacy classes of A_6. Devise a direct proof that A_6 is simple.

(72) 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.

(73) 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.

(74) 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.

(75) Let G be a finite non-trivial p-group. Prove that G' (the commutator subgroup of G) is a proper subgroup of G.

(76) Let G be a finite p-group and $H \lhd G$ a non-trivial normal subgroup. Prove that $H \cap Z(G) \neq \{1\}$.

(77) 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.)

(78) Let $p > 2$ be a prime, $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$. Let G be the subgroup of 3×3 matrices of the form

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

where a, b, c are in $\mathbb{F}$. Thus, G is a group with p^3 elements.
  (a) Calculate the commutator subgroup G' and prove that $G^{ab} = G/G' \cong \mathbb{F} \times \mathbb{F}$ (where the right hand side is a group under component-wise addition).
  (b) Prove that $Z(G) = G'$.
  (c) Prove that if A is a subgroup of G with p^2 elements then $A \supset Z(G)$. (One way to prove that is to show that, *if not*, then necessarily A is an abelian group, $G = A\ Z(G)$ and that also G is abelian.)
  (d) Prove that G has precisely $p + 1$ subgroups of order p^2.

(79) 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.

(80) 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.

(81) 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 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.

(82) 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 the Frattini subgroup $\Phi(G)$ 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.

(83) 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.

(84) In Exercise 79 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 48). 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.

(85) **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, $N_G(N_G(P)) = N_G(P)$.

(86) Let $G_1 \subset G_2$ be two finite groups and p a prime dividing $\sharp G_1$. Prove that if H_1 is a p-Sylow subgroup of G_1 there is a p-Sylow subgroup H_2 of G_2 such that $H_2 \cap G_1 = H_1$.

(87) 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.

(88) How many elements of order 5 could there be in a group of order 20?

(89) Prove that in a group of order 20 the number of elements of order 4 must be either 0, 2 or 10. Show by providing an example that the cases 0 and 2 do occur. (The case 10 also occurs. See exercise 109.)

(90) Let G be a group of order 30.
- Prove that either the 3-Sylow subgroup of G is normal, or the 5-Sylow of G is normal (or both).
- Prove that G has a subgroup H of order 15.
- Prove that every 5-Sylow subgroup of G is contained in H.
- Prove that G has precisely 4 elements of order 5.

(91) Let p be an odd prime. Find the order and generators for a p-Sylow subgroup of S_p and S_{2p}.

(92) Find all Sylow subgroups, up to conjugation, for the group S_5 and determine for each prime p how many p-Sylow subgroups there are.

(93) Find all Sylow subgroups, up to conjugation, for the group $\mathrm{GL}_3(\mathbb{F}_2)$.

(94) 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 44.)

(95) 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.

(96) Find a subgroup of the symmetric group S_7 of order 21.

(97) Let G be a group of order $3^2 \cdot 7 \cdot 23$.
(a) Prove that G is solvable.
(b) Assuming that G is non-abelian, what are the possibilities for the order of $Z(G)$?

(98) Let G be a solvable group. Prove that $G \neq G'$.

(99) 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.)

(100) Find a composition series for A_4 and find the composition factors. Prove that A_4 does not 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.

(101) 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 $i = 1, 2, \dots, n$.

(102) Let A, B be solvable subgroups of a group G. Suppose that $B \subseteq N_G(A)$ (and so AB is a group). Prove that AB is also solvable.

(103) Prove that a group of order pqr is solvable, where $p < q < r$ are distinct primes.

(104) 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.

(105) Let $G = N \rtimes_\phi B$. Prove that G is abelian if and only if both N and B are abelian and $\phi : B \to \operatorname{Aut}(N)$ is the trivial homomorphism.

(106) Construct a non-abelian group of order 75 as a semi-direct product. (Hint: at some point you may wish to use the matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$.)

(107) Construct a group of order 600 containing S_5 as a normal subgroup but which is not a direct product of the form $A \times S_5$.

(108) (a) Construct two non-isomorphic abelian groups of order 18.
(b) Using semi-direct products construct a non-abelian group of order 18, which is non-isomorphic to the Dihedral group D_9.

(109) (a) Let p be a prime and choose an isomorphism $\phi\colon \mathbb{Z}/(p-1)\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}^\times$. Use it to construct a non-trivial semi-direct product

$$\mathbb{Z}/p\mathbb{Z} \rtimes_\phi \mathbb{Z}/(p-1)\mathbb{Z}.$$

You may assume in the sequel that the isomorphism type of this group does not depend on the choice of the isomorphism ϕ.
(b) For $p = 5$ the group gotten this way is denoted F_{20} (it's an example of a Frobenius group). Show that F_{20} is isomorphic to the following subgroup of S_5:

$$\langle (12345), (2354) \rangle.$$

(c) Calculate the number of elements of order 4 in F_{20}.
(d) Prove that any two distinct 2-Sylow subgroups of F_{20} intersect only at the identity. (Hint: prove that a non-trivial permutation belonging to such an intersection will

have at least 2 fixed points, but also has cycle structure $2, 2, 1$, which is impossible in S_5.)

(110) Prove that the group $\mathrm{PSL}_2(\mathbb{F}_3)$, which is the quotient of $\mathrm{SL}_2(\mathbb{F}_3)$ by the scalar matrices $\{\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\}$, has order 12. We have constructed 5 groups of order 12, 2 abelian and 3 non-abelian, and proved that they are the complete list of groups of order 12 up to isomorphism. Determine to which of these is $\mathrm{PSL}_2(\mathbb{F}_3)$ isomorphic.

(111) 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.)

(112) Let $n \geq 3$. Show that $\langle x, y | x^n, y^2, xyxy\rangle$ is a presentation of the dihedral group D_n.

(113) Find a presentation for the group Q of quaternions of order 8.

(114) Prove that $\langle x, y | x^2, y^2\rangle$ is an infinite group.

(115) 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 $n = 10800$.

(116) Let (ρ, V) be a representation of a group G. Let $v \in V$. Prove that $\mathrm{Span}\{\rho(g)v : g \in G\}$ is always a subrepresentation of V. Give an example for which it is a reducible.

(117) 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) $(A \times B)^* \cong A^* \times B^*$.

(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 $\alpha_i \in G^*$.

(118) (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 χ for this action and calculate $\|\chi\|^2$.

(c) Write the character table of Q.

(119) Let (ρ, V) be a representation of a group G, where V is a vector space of dimension n. Suppose that its character, χ_ρ, is the constant function n:

$$\chi_\rho(g) = n, \quad \forall g \in G.$$

Prove that ρ is a trivial representation. Namely, that $\rho(g) = \mathrm{Id}_V$ for all $g \in G$.

(120) Let (ρ, 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 $\rho(g), g \in Q$.

(121) Let (ρ, V) be a representation of G, where $\sharp G = n$ and $\dim(V) > n$. Prove that V is reducible.

(122) Let ρ^{reg} be the regular representation of G. Determine $\sum_{g \in G} \rho^{reg}(g)$.

(123) The group A_4 acts on $\mathbb{R}^3$ via its action on a regular tetrahedron. Write the character χ for this action and calculate $\|\chi\|^2$. (Hint: you don't have to work with the usual basis. There is another basis for $\mathbb{R}^3$ in which the computations are much easier!)

(124) 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.

(125) Let $(\alpha, V), (\tau, W)$ be two representations of a group G. Prove that (α, V) is isomorphic to a sub-representation of (τ, W) if and only if for every irreducible character ρ of G we have $\langle \chi_\alpha, \rho \rangle \leq \langle \chi_\tau, \rho \rangle$.

(126) 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.)

(127) 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 ρ of S_n on this vector space such that

$$\rho(\sigma)(v_t) = v_{\sigma(t)}.$$

Nothing to prove so far. First, give a combinatorial interpretation for the character χ of this representation, interpreting $\chi(\sigma)$ in terms of transpositions and fixed points.

Now, specialize all this to the case $n = 4$. Write the character of the representation ρ completely explicitly. Using the character table of S_4 (it appears in the course notes) decompose the 6-dimensional representation ρ into irreducible representations. You are not required to decompose the vector space itself, only to find the abstract decomposition of ρ into a sum of irreducible representations.

Now view ρ merely as representation of the Klein group. Factor it into irreducible representations (in the same sense as above).

(128) Show that for $n \geq 4$, $\rho^{st,0}$, viewed as a representation of A_n, is irreducible.

(129) 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.)

(130) Prove that two elements x, y of a group G are conjugate, if and only if $\chi(x) = \chi(y)$ for every irreducible character χ of G.

(131) Prove that

$$Z(G) = \{g \in G : |\chi(g)| = \chi(1), \ \chi \text{ irreducible character}\}.$$

(132) Let G be a finite group with n elements and k conjugacy classes. Denote by $m = [G : G']$ the index of the commutator subgroup. Prove that

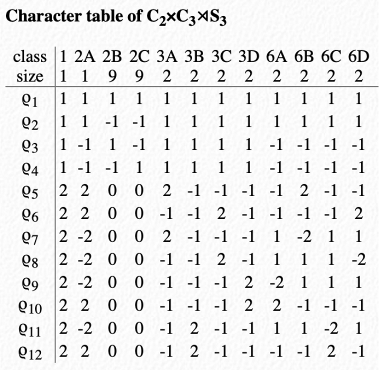
$$n + 3m \geq 4k.$$

(Hint: the solution uses group representations.)

(133) Prove that if a value α appears in the character table of a group G then also $\bar{\alpha}$ appears in the character table. Prove that if all the entries in the character group are real, then every element of the group is conjugate to its inverse. (Make use also of question 130.)

(134) Prove that for any n, the value of any character of the group S_n is a real number. (In fact, it's an integer, but this would be too hard to prove based on what we have learned in this course.)

(135) Here is the character table of the group $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \rtimes_\phi S_3$ (ϕ is a unique non-trivial homomorphism $S_3 \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$). Determine all normal subgroups of this group, their orders and their inclusion relation. Determine the commutator subgroup and the centre of the group (in the sense of writing them as a union of conjugacy classes). Is G^{ab} a cyclic group? Is G' a cyclic group?



Character table of $C_2 \times C_3 \rtimes S_3$

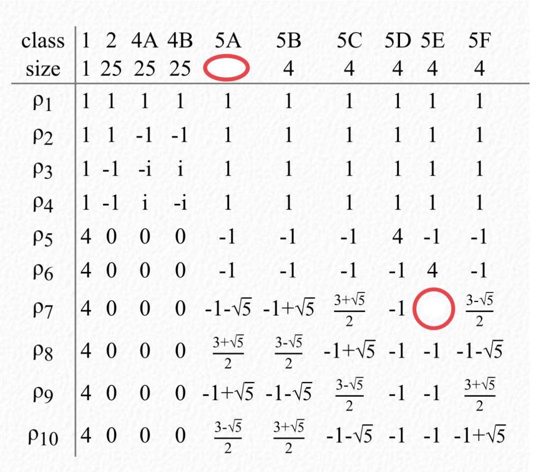
class	1	2A	2B	2C	3A	3B	3C	3D	6A	6B	6C	6D
size	1	1	9	9	2	2	2	2	2	2	2	2
ϱ_1	1	1	1	1	1	1	1	1	1	1	1	1
ϱ_2	1	1	-1	-1	1	1	1	1	1	1	1	1
ϱ_3	1	-1	1	-1	1	1	1	1	-1	-1	-1	-1
ϱ_4	1	-1	-1	1	1	1	1	1	-1	-1	-1	-1
ϱ_5	2	2	0	0	2	-1	-1	-1	-1	2	-1	-1
ϱ_6	2	2	0	0	-1	-1	2	-1	-1	-1	-1	2
ϱ_7	2	-2	0	0	2	-1	-1	-1	1	-2	1	1
ϱ_8	2	-2	0	0	-1	-1	2	-1	1	1	1	-2
ϱ_9	2	-2	0	0	-1	-1	-1	2	-2	1	1	1
ϱ_{10}	2	2	0	0	-1	-1	-1	2	2	-1	-1	-1
ϱ_{11}	2	-2	0	0	-1	2	-1	-1	1	1	-2	1
ϱ_{12}	2	2	0	0	-1	2	-1	-1	-1	-1	2	-1

(136) Let $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$, where p is a prime number. Consider the group

$$G = \{ \left(\begin{smallmatrix} b & n \\ 0 & 1 \end{smallmatrix}\right) : b, n \in \mathbb{F}, b \neq 0 \}.$$

Find the character table of G. (Start by finding the number of conjugacy classes and the number of 1-dimensional representations.)

(137) Consider a group G with the following character table.

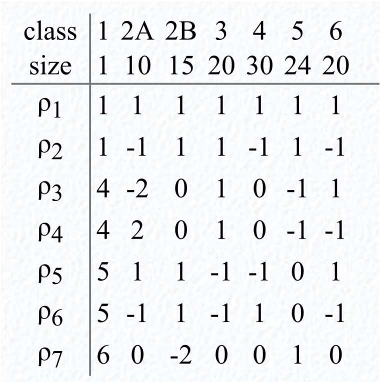


class	1	2	4A	4B	5A	5B	5C	5D	5E	5F
size	1	25	25	25	○	4	4	4	4	4
ρ_1	1	1	1	1	1	1	1	1	1	1
ρ_2	1	1	-1	-1	1	1	1	1	1	1
ρ_3	1	-1	-i	i	1	1	1	1	1	1
ρ_4	1	-1	i	-i	1	1	1	1	1	1
ρ_5	4	0	0	0	-1	-1	-1	4	-1	-1
ρ_6	4	0	0	0	-1	-1	-1	-1	4	-1
ρ_7	4	0	0	0	$-1-\sqrt{5}$	$-1+\sqrt{5}$	$\frac{3+\sqrt{5}}{2}$	-1	○	$\frac{3-\sqrt{5}}{2}$
ρ_8	4	0	0	0	$\frac{3+\sqrt{5}}{2}$	$\frac{3-\sqrt{5}}{2}$	$-1+\sqrt{5}$	-1	-1	$-1-\sqrt{5}$
ρ_9	4	0	0	0	$-1+\sqrt{5}$	$-1-\sqrt{5}$	$\frac{3-\sqrt{5}}{2}$	-1	-1	$\frac{3+\sqrt{5}}{2}$
ρ_{10}	4	0	0	0	$\frac{3-\sqrt{5}}{2}$	$\frac{3+\sqrt{5}}{2}$	$-1-\sqrt{5}$	-1	-1	$-1+\sqrt{5}$

The top row provides notation for the different conjugacy classes and the row below it indicates the number of elements in each conjugacy class (except that you will have deduce some of the entries). Answer the following questions:

(a) What is $\sharp G$? What is $\sharp G^{ab}$? What is $\sharp Z(G)$? What is the size of the conjugacy class 5A? What is the value of ρ_7 on the conjugacy class 5E? (In each case, explain what you rely on.)
(b) Determine the structure of G^{ab} up to isomorphism.
(c) Prove that $\forall x \in G', x \neq 1, \sharp Cent(x) = 25$, where $Cent(x) = \{g \in G : gx = xg\}$.
(d) Prove that besides G and $\{1\}$, G has exactly 4 normal subgroups and determine their orders and inclusion relation.

(138) The table below is the character table of the symmetric group S_5.



class	1	2A	2B	3	4	5	6
size	1	10	15	20	30	24	20
ρ_1	1	1	1	1	1	1	1
ρ_2	1	-1	1	1	-1	1	-1
ρ_3	4	-2	0	1	0	-1	1
ρ_4	4	2	0	1	0	-1	-1
ρ_5	5	1	1	-1	-1	0	1
ρ_6	5	-1	1	-1	1	0	-1
ρ_7	6	0	-2	0	0	1	0

(a) Use your knowledge of the 1-dimensional representations of S_5, and other considerations, to write a representative permutation for each conjugacy class.
(b) The group S_5 acts on the set $T = \{\{i,j\} : i,j \in \{1,2,\dots,5\}, i \neq j\}$ that has 10 elements. Show that this defines a 10-dimensional representation (ρ, V) of S_5. A basis for this vector space can be given by

$$\{v_{\{i,j\}} : 1 \leq i < j \leq 5\}.$$

Write the character χ_ρ of ρ. (Namely, provide its value on each conjugacy class in S_5.)
(c) Find the decomposition of χ_ρ as a sum of irreducible characters and, in particular, determine the dimension of the space of fixed vectors $\dim(V^{S_5})$.
(d) Consider the natural inclusion $S_3 \subset S_5$ and the subspace

$$V^{S_3} = \{v \in V : \rho(\sigma)(v) = v, \forall \sigma \in S_3\}.$$

Find a basis for V^{S_3}.

(139) Let T be the non-abelian group of order 12 that we constructed as

$$T = \mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z},$$

where we identify $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ with $(\mathbb{Z}/3\mathbb{Z})^\times = \{1,2\}$ and where ϕ is the homomorphism:

$$\phi : \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}), \quad \phi(a) = 2^a.$$

In this question we will eventually write the character table of T. Elements of T are written as (n,b), $n \in \mathbb{Z}/3\mathbb{Z}, b \in \mathbb{Z}/4\mathbb{Z}$ and multiplication is given by

$$(n_1,b_1)(n_2,b_2) = (n_1 + 2^{b_1}n_2, b_1 + b_2).$$

(a) Prove that T has 6 conjugacy classes and write each of them explicitly.[20]

(b) Prove that T has four 1-dimensional representations and deduce that the irreducible representations of T are: four 1-dimensional representations and two irreducible 2-dimensional representations.

(c) Let $\psi\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}), \psi(a) = 2^a$. Show that there is a natural homomorphism

$$f\colon T \to \mathbb{Z}/3\mathbb{Z} \rtimes_\psi \mathbb{Z}/2\mathbb{Z}.$$

(d) Prove that $\mathbb{Z}/3\mathbb{Z} \rtimes_\psi \mathbb{Z}/2\mathbb{Z} \cong S_3$ and thus has an irreducible 2-dimensional representation ρ'.

(e) Write the character of the representation $\rho := \rho' \circ f$.

(f) Write the full-character table of T.

(140) 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 $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$, 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:

(141) 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.

(142) 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.

(143) 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 $p^2 \nmid |G|$.

(144) **Coxeter groups.** A Coxeter group can be defined as a group with the presentation

$$\langle r_1, \dots, r_n | (r_i r_j)^{m_{ij}} = 1 \rangle$$

where the m_{ij} are positive integers, where we allow formally $m_{ij} = \infty$ and that means that no relation is put on $r_i r_j$. Furthermore, $m_{ii} = 1$ for all i, and for every pairi, j, we have $m_{ij} = m_{ji}$. One refers to $S = \{r_1, \dots, r_n\}$ as the generators and a Coxeter system is a pair (W, S) as above.

Thus, a Coxeter group is generated by "reflections" r_i that do not necessarily commute (as we may have $m_{ij} > 2$) and, as such, they often arise from geometry. Particular Coxeter groups are also a fundamental object in the theory of Lie groups, where they appear under the name Weyl group.

Prove the following ((b) is more challenging than (a) and (c), I believe):

(a) Prove that for $n \geq 3$, the matrix $(m_{ij}) = \left(\begin{smallmatrix} 1 & n \\ n & 1 \end{smallmatrix}\right)$ defines a Coxeter group

$$\langle r_1, r_2 : r_1^2 = r_2^2 = (r_1 r_2)^n = 1 \rangle$$

isomorphic to D_n.

[20] If you did your calculation correctly you will find that 2 are of size 1,2 are of size 2 and 2 are of size 3.

(b) Let $n \geq 2$. For $1 \leq i \leq j \leq n-1$, let $m_{ii} = 1$, $m_{i\,i+1} = 3$ and $m_{ij} = 2$ if $j - i \geq 2$ and complete the matrix (m_{ij}) by symmetry. Show that the Coxeter group

$$\langle r_1, \dots, r_{n-1} | (r_i r_j)^{m_{ij}} = 1 \rangle$$

is isomorphic to the symmetric group S_n. (So, for example, S_3 is isomorphic to the group $\langle r_1, \dots, r_2 | r_1^2 = r_2^2 = (r_1 r_2)^3 = 1 \rangle$.)

(c) Show that the Coxeter group $\langle r_1, \dots, r_2 | r_1^2 = r_2^2 = 1 \rangle$ (with corresponding matrix $(m_{ij}) = \left(\begin{smallmatrix} 1 & \infty \\ \infty & 1 \end{smallmatrix}\right)$) is an infinite group.

(145) Let (W, S) be a Coxeter system. We define the **length** $\ell(w)$ of $w \in W$ as r, where $r \geq 0$ is the minimal integer so that one can write

$$w = s_1 s_2 \cdots s_r, \quad s_i \in S.$$

Note: there may be more than one such expression of length r for w, but any such expression $w = s_1 s_2 \cdots s_r, \quad s_i \in S$ is called a **reduced decomposition** of w. Prove the following:

(a) $\ell(w) = \ell(w^{-1}$.

(b) $\ell(w_1 w_2) \leq \ell(w_1) + \ell(w_2)$.

(c) The function $d(w_1, w_2) = \ell(w_1 w_2^{-1})$ is a metric on W.

(d) For the Coxeter system $(S_n, \{(12), (23), \dots, (n-1\ n)\})$, for $n = 3, 4$, calculate the length of (13) and $(14)(23)$.

(146) (**Goursat's Lemma**) Gourstat's lemma provides a method to find all subgroups of a product $A \times B$ of two groups. We first provide motivation by providing a general method to construct such subgroups. Goursat's lemma would show that this method is the most general one; that every subdirect product of $A \times B$ is obtained this way.

To begin with, denote by $\pi_A \colon A \times B \to A$, $\pi_B \colon A \times B \to B$, the projections

$$\pi_A(a, b) = a, \quad \pi_B(a, b) = b.$$

A subgroup H of $A \times B$ is called a **subdirect product** if

$$\pi_A(H) = A \quad \text{and} \quad \pi_B(H) = B.$$

(Note that we always have that H is a subdirect product of $\pi_A(H) \times \pi_B(H)$ and so for many purposes, such as classifying all subgroups H of $A \times B$, we may reduce to the case of subdirect products.)

(a) Let $K \lhd B$ and let $f \colon A \to B/K$ be a surjective homomorphism. Let $H \subseteq A \times B$ be given by

$$H = \{(a, b) : f(a) = bK\}.$$

Prove that H is a subdirect product of $A \times B$.

(b) Let N be the kernel of f. We have then an induced isomorphism

$$F \colon A/N \to B/K.$$

Denote by $\bar{a}$ elements of A/N and by $\bar{b}$ elements of B/K. Let Γ_F be the graph of F:

$$\Gamma_F = \{(\bar{a}, F(\bar{a})) : \bar{a} \in A/N\}.$$

Prove that Γ_F is a subgroup of $A/N \times B/K$ and that H is the pre-image of Γ_F in $A \times B$ under the natural homomorphism $A \times B \to A/N \times B/K$. That is

$$H = \{(a, b) : a \in A, b \in B, F(\bar{a}) = \bar{b}\}.$$

(c) Prove Goursat's lemma, which is the converse of the above:
Let H be a subdirect product of $A \times B$. There are normal subgroups $N \lhd A, K \lhd B$ and an isomorphism $F \colon A/N \to B/K$ such that H is the pre-image of Γ_F under the natural homomorphism $A \times B \to A/N \times B/K$.

(i) Let $N = H \cap A = \mathrm{Ker}(\pi_B \colon H \to B)$ and $K = H \cap B = \mathrm{Ker}(\pi_A \colon H \to A)$.[21] Prove that N and K are normal subgroups of A and B, respectively, and that the function

$$F \colon A/N \to B/K, \quad F(\bar{a}) = \pi_B(a,b)K = bK = \bar{b},$$

defined by choosing any element (a,b) in H such that $\bar{a} = aN$, is a well-defined homomorphism.

(ii) Prove that, in fact, F is an isomorphism and that H is the pre-image of Γ_F.

(iii) Prove that $\sharp H = \sharp A \times \sharp K = \sharp B \times \sharp N$, if A and B are finite groups.

(d) Use the results above to find all subdirect products of $S_3 \times S_3$.

(147) **Shuffles.** Let $n \geq 1$ and $1 \leq d \leq n$ be integers. A **shuffle** (sometimes called a riffle shuffle) is a permutation σ of S_n such that that

$$\sigma(1) < \sigma(2) < \cdots < \sigma(d), \quad \sigma(d+1) < \sigma(d+2) < \cdots < \sigma(n).$$

This definition depends on d, but we do not indicated that in the terminology unless we must. We will then talk about a $(d, n-d)$ shuffle. The name comes from shuffling cards. Imagine a deck of n cards and a shuffle of it, where you take the top d cards and stick them in order into the other $n-d$ cards. [22]

(There is a similar notion, that for lack of better terminology we will call an inverse-shuffle. These are permutations σ that satisfy $\sigma^{-1}(1) < \cdots < \sigma^{-1}(d)$ and $\sigma^{-1}(d+1) < \cdots < \sigma^{-1}(n)$. Note that the inverse of a shuffle is an inverse-shuffle)

(a) Prove that there are $\binom{n}{d}$ permutations in S_n that are $(d, n-d)$-shuffles.

(b) Consider the group $S_d \times S_{n-d}$ as a subgroup of S_n, where we identify S_{n-d} with permutations of $\{d+1, \dots, n\}$. More formally, to a pair $(\sigma, \tau) \in S_d \times S_{n-d}$ associate the permutation $\rho \in S_n$ given by

$$\rho(i) = \begin{cases} \sigma(i) & 1 \leq i \leq d \\ \tau(i-d) + d & d+1 \leq i \leq n. \end{cases}$$

Prove that the set of $(d, n-d)$ shuffles are a complete set of representatives for the right cosets $S_n / S_d \times S_{n-d}$.

(c) Likewise, prove that the set of $(d, n-d)$ inverse shuffles are a complete set of representatives for the left cosets $S_d \times S_{n-d} \backslash S_n$.

(d) Consider now $(1, n-1)$-shuffles and the oriented Cayley graph of S_n relative to the set of $(1, n-1)$-shuffles. First draw this graph for the groups S_3 and S_4. Prove for a general n that the Cayley graph is connected (namely, that every permutation can be obtained as a product of $(1, n-1)$-shuffles) and estimate its diameter.

(148) Let $\mathbb{F}$ be a field. Prove that the subgroup U of $GL_3(\mathbb{F})$ is a non-trivial semi-direct product, where

$$U = \left\{ \left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{smallmatrix} \right) : a, b, c \in \mathbb{F} \right\}.$$

(149) Let n be a positive integer. Find the number of conjugacy classes, the centre and the commutator subgroup of the group

$$\mathbb{Z}/n\mathbb{Z} \rtimes_\phi (\mathbb{Z}/n\mathbb{Z})^\times,$$

where $\phi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ is given by $a \mapsto [a]$, where $[a]$ is the automorphism of $\mathbb{Z}/n\mathbb{Z}$ defined as

$$[a](x) = ax.$$

[21] It is more accurate to say that $N = H \cap (A \times \{1\})$, and $K = H \cap (\{1\} \times B)$, but we will identify A with $A \times \{1\}$ and B with $\{1\} \times B$.

[22] If you are interested in learning more about shuffles and their combinatorial and probabliistic uses, I recommend the paper by Aldous and Diaconis, *Shuffling cards and stopping times,* Amer. Math. Monthly 93 (1986), no. 5, 333–348, as a starting point.

INDEX