Lecture notes for MAT301

Petr Kosenko

August 12, 2022

Abstract

These are lecture notes made for the MAT301 course held in Summer 2021 in the University of Toronto. The notes are heavily inspired by J.A. Gallian's textbook "Contemporary Abstract Algebra" (9th ed.), which was used as a primary textbook in the course. However, they can be used as an independent reference as well.

If you see any typos, you can email me at `petr.kosenko@mail.utoronto.ca`.

1 Introduction: groups of symmetries

Definition 1.1. By a **planar figure** we will mean a subset of $\mathbb{R}^2$.

For example, think of a point or a square $\{0,1\} \times [0,1] \cup [0,1] \times \{0,1\} \subset \mathbb{R}^2$ as a planar figure.

Definition 1.2. An **isometry** of $\mathbb{R}^2$ is a (bijective) map $f : \mathbb{R}^2 \to \mathbb{R}^2$ which preserves distances:

$$\|f(x) - f(y)\| = \|x - y\| \quad \text{for all } x, y \in \mathbb{R}^2, \tag{1}$$

where $\|(a,b)\| := \sqrt{a^2 + b^2}$.

Remark: check that (1) implies that f is bijective, so we don't need to include this adjective as a part of the definition.

Of course, this definition can be immediately generalized to $\mathbb{R}^n$ for all $n \geq 1$:

Definition 1.3. For any $x, y \in \mathbb{R}^n$ define the **Euclidean norm** as follows:

$$||x - y|| = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}.$$

Then we define an **isometry** in $\mathbb{R}^n$ as a (bijective) map $f : \mathbb{R}^2 \to \mathbb{R}^2$ which preserves distances:

$$\|f(x) - f(y)\| = \|x - y\| \quad \text{for all } x, y \in \mathbb{R}^n,$$

For example, the identity map is always an isometry. A 90-degree rotation $(x, y) \mapsto (-y, x)$ is also an isometry.

Definition 1.4. Let $A \subset \mathbb{R}^2$ be a planar figure. Then the set of all isometries f for which $f(A) = A$ is called the **group of symmetries of A**. Elements of this set are called **symmetries** of A.

Example 1.1. Consider a square with vertices at $A = (0,0), B = (0,1), C = (1,0), D = (1,1)$ (notation differs a bit from what was used in the lectures). Let us try to describe all symmetries of a square.

Lemma 1.1. Any symmetry takes vertices to vertices.

Proof. It is easy to see that the centre point of the square, $Z = (0.5, 0.5)$, is the only point which is **equidistant** from all vertices of the square. Therefore, any symmetry f has to preserve Z. In other words, we have $f(Z) = Z$, and (1) implies

$$\|Z - f(A)\| = \|Z - A\| = (\sqrt{2})^{-1}, \quad \cdots \|Z - f(D)\| = \|Z - D\| = (\sqrt{2})^{-1}.$$

However, A, B, C, D are the only points for which their distance to Z equals $(\sqrt{2})^{-1}$. Therefore, $\{f(A), f(B), f(C), f(D)\}$ is just a permutation of $\{A, B, C, D\}$. □

And a similar argument applied to the sides yields the following:

Lemma 1.2. Any symmetry takes adjacent vertices to adjacent vertices.

Combining these two lemmas, we can see that any symmetry is defined by the images of any two adjacent vertices. For example, if $f(A)$ and $f(B)$ are defined, then $f(C)$ has to be adjacent to $f(A)$, but $f(A)$ has only two neighbours and one is already taken. Therefore, the only possible options for a symmetry are

$$\begin{aligned}
A &\mapsto A, \qquad B \mapsto B \\
A &\mapsto A, \qquad B \mapsto C \\
A &\mapsto B, \qquad B \mapsto A \\
A &\mapsto B, \qquad B \mapsto D \\
A &\mapsto C, \qquad B \mapsto A \\
A &\mapsto C, \qquad B \mapsto D \\
A &\mapsto D, \qquad B \mapsto B \\
A &\mapsto D, \qquad B \mapsto C.
\end{aligned}$$

This leaves us with 8 symmetries. Moreover, there is a nice geometric description of these symmetries. We have four clockwise rotations $\{Id, R_{90}, R_{180}, R_{270}\}$, and four reflections, which we will denote by $\{H, V, D_1, D_2\}$, where H stands for the reflection with respect to the line $y = 0.5$, V stands for the reflection with respect to $x = 0.5$, and D_1, D_2 are reflections with respect to the main diagonal and opposite diagonal respectively.

It is very important to understand that any two symmetries can be **composed** to obtain another symmetry. For example,

$$\begin{aligned}
H \circ R_{90}(A) &= H(B) = A \\
H \circ R_{90}(B) &= H(D) = C \\
H \circ R_{90}(C) &= H(A) = B \\
H \circ R_{90}(D) &= H(C) = D,
\end{aligned}$$

but this is precisely how D_2 acts on the vertices. Also, it is easy to verify that

$$R_{90} \circ R_{180} = R_{270}, \quad R_{180} \circ R_{180} = Id.$$

This also implies that

$$R_{180}^{-1} = R_{180}, R_{90}^{-1} = R_{270},$$

as **inverses of symmetries** are also symmetries. Finally, it is easy to check that, when computing compositions of several symmetries, like $H \circ D_1 \circ R_{90}$, the order does not matter:

$$H \circ (D_1 \circ R_{90}) = (H \circ D_1) \circ R_{90}$$

This property is called **associativity**.

As the last example shows, the set of symmetries has several important properties:

- Any composition of symmetries is a symmetry,
- The identity map is always a symmetry,

- Composition is associative,
- The inverse of a symmetry is a symmetry.

These four properties are what will motivate us to introduce the notion of an **abstract group**, or just a **group**.

Remark. Finally, we want to remark that we could consider any "object" X with some "structure", and thus it would make sense to look at all bijections $X \to X$ which preserve said structure. The resulting set is expected to satisfy all four listed properties as well. As a very simple illustration of this principle, we can consider a square with a fixed **orientation**. Only rotations preserve the orientation, but all four properties still hold for this four-element set of symmetries.

2 Abstract groups

Let us recall that if X, Y are sets, then we define their **direct product** $X \times Y$ as the set of all ordered pairs (x, y) for $x \in X, y \in Y$.

Definition 2.1. A **binary operation** on a set G is a function $G \times G \to G$.

Definition 2.2. A **group** is a triple $(G, e, \cdot)$, where G is a set, $\cdot : G \times G \to G$ is a binary operation, and $e \in G$, such that the following properties are satisfied:

1. (associativity) For any $x, y, z \in G$ we have $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
2. (identity) For any $a \in G$ we have $a \cdot e = e \cdot a = a$. Such $e \in G$ is called an **identity** of G.
3. (inverse) For any $a \in G$ there exists an element $b \in G$ such that $a \cdot b = b \cdot a = e$. Such an element $b \in G$ is called an **inverse** of a.

In particular, every group is a **non-empty** set, because any group has to contain the identity element.

Let us prove some basic properties of groups.

Proposition 2.1 (idenitity is unique)**.** If G is a group, then the identity is unique.

Proof. Suppose that e and e' are both identities in G. Then

$$e \cdot e' = e = e'.$$

□

Proposition 2.2 (cancellation property)**.** If $a \cdot b = a \cdot c$ for some elements $a, b, c \in G$, then $b = c$. If $b \cdot a = c \cdot a$ for some elements $a, b, c \in G$, then $b = c$.

Proof. If $a \cdot b = a \cdot c$, then we can find such an element d, that $d \cdot a = a \cdot d = e$. Therefore, we can multiply both sides of the first equality by d from the left:

$$d \cdot (a \cdot b) = d \cdot (a \cdot c) \Rightarrow (d \cdot a) \cdot b = (d \cdot a) \cdot c \Rightarrow b = c.$$

If $b \cdot a = c \cdot a$, then we can multiply both sides of the first equality by d from the right:

$$(b \cdot a) \cdot d = (c \cdot a) \cdot d \Rightarrow b = c.$$

□

This proposition allows us to prove that the inverses are also unique:

Corollary 2.1. If G is a group, then for $a \in G$ there is only one inverse $b \in G$ of a.

Proof. If b' is another inverse, then we would have

$$a \cdot b' = a \cdot b = b \cdot a = b' \cdot a = e.$$

The cancellation property immediately implies that $b = b'$. □

Remark. This allows us to denote the inverse of a by a^{-1}. The above corollary proves that the function $(\cdot)^{-1} : G \to G$ is a well-defined map.

Proposition 2.3. For any $a, b \in G$ we have $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Proof.

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot a^{-1} = e.$$
$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot (a^{-1} \cdot a) \cdot b = b^{-1} \cdot b = e.$$

□

Remark. However, as inverses are unique, $ab = e$ automatically implies $a = b^{-1}$ (compare to Q6 in Assignment 1). Nevertheless, you will have to deal with invertible objects in other mathematical structures, and if you want to check that an object A is inverse to B with respect to an operation $\cdot$, then you absolutely need to check both equalities: $A \cdot B = B \cdot A = e$. As a simple example, consider two maps $L, R : \mathbb{N} \to \mathbb{N}$, where

$$L(k) = \max\{k - 1, 1\}, \quad R(k) = k + 1,$$

and the binary operation is the functional composition. Then

$$L(R(k)) = k \text{ for all } k \in \mathbb{N},$$

but

$$R(L(1)) = 2.$$

Therefore, L and R are not inverse to each other, even if one composition **is** the identity map.

Remark. Also, later in this course we will start dropping the operation $\cdot$ from our computations, thus replacing $a \cdot b$ with ab.

Definition 2.3. The order of a group $(G, e, \cdot)$ is the number of elements in G, and it is denoted by $|G|$. If $|G| < \infty$, then we will call G a **finite group**.

Remark. If for any $a, b \in G$ we have $a \cdot b = b \cdot a$, then G is called an **abelian group**. The ultimate goal of MAT301 is classifying all **finite abelian** groups. Classifying all **finite** groups is unimaginably harder, though – the proof of the classification spans hundreds of mathematical papers!

Let us, finally, provide some examples of groups:

Example 2.1. As always, we start with the simplest object possible. Let $G = \{e\}$, $e \cdot e = e$. This is a group, which is often called a **trivial group**.

Example 2.2. If A is a planar figure, then its group of symmetries $(Sym_A, Id, \circ)$ is a group with respect to the composition. This was, essentially, proven in the introductory lecture.

2.1 Integers mod n

Example 2.3. Here we provide a brief review of modular arithmetic. First of all, we need to introduce some notation:

Definition 2.4. Let X be a set. A subset $R \subset X \times X$ is called a **relation** on X. We will denote $(a, b) \in R \Leftrightarrow a \sim_R b$.

A relation R on X is called an **equivalence relation** if it satisfies the following properties:

- (reflexivity) For any $a \in X$ we have $a \sim_R a$

- (symmetry) If $a \sim_R b$, then $b \sim_R a$
- (transitivity) If $a \sim_R b$ and $b \sim_R c$ then $a \sim_R c$.

Let us denote by $\mathbb{Z}$ the set of all integers, and by $\mathbb{N}$ the set of natural numbers (positive integers). Let $n \in \mathbb{N}$. Then we want to define an equivalence relation on $\mathbb{Z}$ like this:

$$a \equiv_n b \Leftrightarrow n|a-b \Leftrightarrow \exists k \in \mathbb{Z} : a - b = nk.$$

We will also use the notation $a \equiv b (\text{mod } n)$ – this is the standard notation. If $a \equiv b (\text{mod } n)$, then we say that a is **congruent** to b modulo n.

Let us prove that $\equiv_n$ is an equivalence relation.

- For any a we have
$$a \equiv a (\text{mod } n) \Leftrightarrow n|a-a \Leftrightarrow n|0,$$
but every non-zero number divides zero!
- For any a, b we have
$$a \equiv b (\text{mod } n) \Leftrightarrow n|a-b \Leftrightarrow a-b = kn \Leftrightarrow b-a = (-k)n \Leftrightarrow b \equiv a (\text{mod } n).$$
- Suppose that $a \equiv b (\text{mod } n)$ and $b \equiv c (\text{mod } n)$. Then there exist $k, l \in \mathbb{Z}$ such that $a - b = kn$ and $c - b = ln$. Adding these two equalities, we get
$$c - a = (k+l)n,$$
but this implies $a \equiv c (\text{mod } n)$.

Notation. If $n \in \mathbb{N}$, for any $a \in \mathbb{Z}$ we will denote $[a]_n = \{b \in \mathbb{Z} : a \equiv b (\text{mod } n)\}$. These are subsets of $\mathbb{Z}$ which are called **equivalence classes** of a with respect to $\equiv_n$.

For example,

$$[0]_3 = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}.$$

The following propositions easily follow from the definition of congruency mod n.

Proposition 2.4. For any $a \in \mathbb{Z}$ we have

$$[a]_n = \{a + kn \,|\, k \in \mathbb{Z}\}.$$

Proposition 2.5. For any $n \in \mathbb{N}$ the sets $[0]_n, \dots [n-1]_n$ define a partition of $\mathbb{Z}$. In other words,

$$[a]_n \cap [b]_n = \begin{cases} [a]_n, & \text{if } a \equiv b \,(\text{mod } n) \\ \emptyset, & \text{otherwise.} \end{cases}$$

Definition 2.5. For any $n \in \mathbb{N}$ let us define

$$\mathbb{Z}/n\mathbb{Z} := \{[0]_n, [1]_n, \dots [n-1]_n\}.$$

For example, $\mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$.

Theorem 2.1.

- $(\mathbb{Z}, 0, +)$ is an infinite group.
- For any $n \in \mathbb{N}$ the triple $(\mathbb{Z}/n\mathbb{Z}, [0]_n, +)$ is a group, where we define
$$[a]_n + [b]_n = [a+b]_n.$$

It is worth noting that $(\mathbb{Z}, 1, \times)$ is not group – you can't take a multiplicative inverse of 2, for example. Let us play the same game with $(\mathbb{Z}/n\mathbb{Z}, [1]_n, \times)$. It is not a group (why?), but if we define the **multiplicative group of integers mod** n

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n | \gcd(a, n) = 1\},$$

then $\left((\mathbb{Z}/n\mathbb{N})^\times, [1]_n, \times\right)$ is a well-defined group.

Remark. Later in this course, we will tend to drop the square brackets when working with $\mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^\times$ if it does not cause any confusion.

2.2 Dihedral groups

Example 2.4. Recall that a regular polygon is a vertex-transitive polygon: we require that all sides have the same lengths and all internal angles are equal as well.

Definition 2.6. Let $n \geq 3$. Let P_n denote a regular n-gon. Then its group of symmetries is denoted by D_n, and called the **dihedral group**.

Let us try to describe the group structure of D_n.

Proposition 2.6.

1. Every symmetry in D_n preserves vertices. In particular, adjacent vertices map to adjacent vertices.
2. The order of D_n equals $2n$.

The idea of the proof is the same as for the square. The center of P_n has to be fixed, but vertices are the points which maximize the distance to the center, so any isometry has to preserve them.

All symmetries of P_n can be classified as follows: we have n rotations: $\{Id, R_{2\pi/n}, \dots, R_{2\pi(n-1)/n}\}$, and we have n reflections. When n is odd, then every for every reflection its axis passes through a vertex and the midpoint of the opposite side. If n is even, we have $n/2$ reflections with axis passing through two opposite vertices, and we have $n/2$ reflections passing through the midpoints of the opposite sides.

Let us denote $R_{2\pi/n} = r$, and let is fix a random reflection s.

Proposition 2.7.

1. Let $1 \leq k \leq n$. Then $\underbrace{r \cdot r \cdot \dots \cdot r}_{k \text{ times}} = r^k = R_{2\pi k/n}$. Also, $ss = Id$.
2. $srs^{-1} = r^{-1} = r^{n-1}$. As a consequence, $sr^k s = r^{-k}$.
3. Every element of D_n can be written as r^k or $r^l s$ for some $0 \leq k < n$ or $0 \leq l < n$.

Let us consider an example of a computation in a dihedral group. Let $n = 10$. Then

$$r^6 s^3 r^{21} r^5 s^{100} = r^6 s^3 r^{26} (s^2)^{50} = r^6 s^3 r^{26} = r^6 s r^{26}.$$

Then we use one of the relations to prove that $r^6 s = s r^{-6}$, so

$$r^6 s r^{26} = s r^{20} = s.$$

3 Subgroups

First of all, we want to highlight two kinds of notations which are used when working with various groups.

If a group is endowed with a **multiplicative operation**, so we have a triple $(G, e, \cdot)$, then we will denote

$$\underbrace{a \cdot \dots \cdot a}_{n \text{ times}} = a^n, \quad \underbrace{a^{-1} \cdot \dots \cdot a^{-1}}_{k \text{ times}} = a^{-k}.$$

This is the default notation when working with abstract groups.

If a group is endowed with an **additive operation**, so that we have $(G, 0, +)$, then we denote

$$\underbrace{a + \dots + a}_{n \text{ times}} = na, \quad \underbrace{-a \cdot \dots \cdot -a}_{k \text{ times}} = -ka.$$

This notation is preferred when working with integers modulo n or vector spaces.

3.1 Order of an element in a group

Recall that the order of a group is the number of elements in the respective underlying set.

Definition 3.1. Let G be a group and let us consider $a \in G$. The **order** of a is the smallest positive integer n such that $a^n = e$ (in the additive notation $na = 0$). The order will be denoted by $|a|$ or $\mathrm{ord}(a)$. If it does not exist, we will denote $\mathrm{ord}(a) = \infty$.

Example 3.1. Let $G = \mathbb{Z}/6\mathbb{Z}$. What is the order of $[2]$? Well, observe that

$$[2] + [2] = [4], \quad [2] + [2] + [2] = [6] = [0].$$

Therefore, $\mathrm{ord}([2]) = 3$.

Example 3.2. Consider $G = (\mathbb{Z}/15\mathbb{Z})^\times$. Then

$$(\mathbb{Z}/15\mathbb{Z})^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

This is a group with respect to multiplication modulo 15. Let us find the order of 7. We have

$$\begin{aligned} 7^1 &\equiv 7 (\mathrm{mod}\ 15) \\ 7^2 &\equiv 4 (\mathrm{mod}\ 15) \\ 7^3 &\equiv 13 (\mathrm{mod}\ 15) \\ 7^4 &\equiv 1 (\mathrm{mod}\ 15) \end{aligned}$$

Therefore, $\mathrm{ord}(7) = 4$.

Example 3.3. Consider $G = \mathbb{Z}$, $a = 1$. Then $\mathrm{ord}(1) = \infty$. There is no such n that $n \cdot 1 = 0$. This is an element of an **infinite order**.

Lemma 3.1. Let G be a group, and let $a \in G$ be an element with the following property: $a^k = e$ and $a^n = e$ for some positive integers $k, n \in \mathbb{N}$. Then $a^{\gcd(k,n)} = e$.

In particular, $\mathrm{ord}(a) = \gcd\{n \in \mathbb{N} : a^n = e\}$.

Proof. There are many ways to prove this, each way using a different definition of the gcd. Let use use the fact that there exist two integers $s, t \in \mathbb{Z}$ such that $ks + nt = \gcd(n, k)$. Then we have

$$a^{\gcd(k,n)} = a^{ks+nt} = a^{k^s} a^{n^t} = (a^k)^s (a^n)^t = e^s e^t = e.$$

□

3.2 Subgroups: definitions and examples

Definition 3.2. Let $(G, e, \cdot)$ be a group. A non-empty subset $H \subset G$ is called a **subgroup** of G if H is a group with respect to the binary operation on G.

What does this definition mean?

- For any $h_1, h_2 \in H$ we have $h_1 h_2 \in H$.
- For any $h \in H$ we have $h^{-1} \in H$, where the inverse is taken in G.
- The identity element e_G of G belongs to H. (this is implied by non-emptiness of H: take $a \in H$, then $a^{-1} \in H$, then $aa^{-1} = e \in H$.) In particular, this is the identity element in H, as well.

The three properties outlined above are referred to as **the second subgroup test** in the textbook.

Remark. If $H \subset G$ is a subgroup, then sometimes we will use the notation $H \leq G$, but more often than not we will just write $H \subset G$ and explicitly indicate that H is a subgroup.

Theorem 3.1 (one-step subgroup test)**.** Let G be a group and let $H \subset G$ be a subset. If for any $a \in H$ and $b \in H$ we have that $ab^{-1} \in H$, then H is a subgroup of G.

Let us use these two tests to find some subgroups!

Example 3.4. Let $G = \mathbb{Z}$. Then the subset of all even numbers $H = \{2k : k \in \mathbb{Z}\}$ is a subgroup due to the one-step test: If a and b are even, then $a - b$ is also even. We will also denote $H = 2\mathbb{Z}$.

Example 3.5. Let G be an abelian group. (for every $x, y \in G$ we have $xy = yx$) Define $H = \{x \in G : x^2 = e\}$. Then H is a subgroup due to the one-step subgroup test. Suppose that $a^2 = e$ and $b^2 = e$. Then

$$(ab^{-1})^2 = ab^{-1}ab^{-1} = aab^{-1}b^{-1} = a^2(b^2)^{-1} = e.$$

Example 3.6. Let $n \geq 3$. Consider $G = D_n$. Let $H = \{Id, r, r^2, \ldots, r^{n-1}\}$. Then H is a subgroup due to the one-step subgroup test: $r^k r^{-l} = r^{k-l} = r^{k-l(\mathrm{mod} n)} \in H$.

Example 3.7. Let $n \geq 2$. Consider

$$GL_n(\mathbb{R}) = \{\text{all invertible real-valued } n \times n \text{ matrices}\} = \{\text{all invertible linear operators } \mathbb{R}^n \to \mathbb{R}^n\}.$$

Then $(GL_n(\mathbb{R}), E, \cdot)$ is a group with respect to matrix multiplication and the identity matrix E.

Keep in mind that you need to choose the right definition to efficiently prove that the matrix multiplication is associative!

Then we define

$$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\}.$$

Then, due to the multiplicativity of det, we get that $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.

Example 3.8. Let G be a group. Define

$$Z(G) = \{x \in G : xy = yx \, \forall y \in G\}.$$

This subset is called **the centre** of G.

Proposition 3.1. The centre of G is a subgroup.

Proof. Here we will not use the one-step test, but check all axioms separately.

1. Because the identity commutes with all elements of G, we have $e \in Z(G)$.
2. Let $a, b \in Z(G)$. To check that $ab \in Z(G)$, we have to do the following computation:

$$(ab)y = a(by) = a(yb) = (ay)b = y(ab).$$

3. Let $a \in Z(G)$. To check that $a^{-1} \in Z(G)$, we write

$$a^{-1}y = (y^{-1}a)^{-1} = (ay^{-1})^{-1} = ya^{-1}.$$

□

Example 3.9. If G is an abelian group, then $Z(G) = G$.

Example 3.10. If n is even, then $Z(D_n) = \{e, R_\pi\}$. If n is odd, then $Z(D_n) = \{e\}$.

Definition 3.3. If G is a group, and $g \in G$, then we define $C(g) = \{x \in G : gx = xg\}$. This is a subset which is called the **centralizer** of g.

This is also a subgroup for any g, the proof is very similar to the argument provided above. For example, in D_4 we have $C(H) = \{Id, H, V, R_\pi\}$.

4 Cyclic subgroups

Definition 4.1. Let G be a group, $g \in G$. Then we denote $\langle g \rangle = \{g^n : n \in \mathbb{Z}\} \subset G$.

Proposition 4.1. For any element g the subset $\langle g \rangle$ is a subgroup. It is called a **cyclic subgroup generated by** g. Moreover, every element $x \in G$ satisfying $\langle x \rangle = \langle g \rangle$ is called a **generator** of the cyclic subgroup.

Proof. This is a perfect opportunity to use the one-step subgroup test: let $x, y \in \langle g \rangle$. Then $x = g^k$ and $y = g^l$ for some $k, l \in \mathbb{Z}$, and

$$xy^{-1} = a^k a^{-l} = a^{k-l} \in \langle g \rangle .$$

□

Example 4.1. If $G = \mathbb{Z}$, then $\langle 2 \rangle = 2\mathbb{Z}$ and $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$.

Example 4.2. Let $G = \mathbb{Z}/10\mathbb{Z}$. Then

$$\begin{aligned} \langle 2 \rangle &= \{0, 2, 4, 6, 8\} \\ \langle 4 \rangle &= \{0, 4, 8, 2, 6\} \\ \langle 7 \rangle &= \{0, 7, 4, 1, 8, 5, 2, 9, 6, 3\} = \mathbb{Z}/10\mathbb{Z}. \end{aligned}$$

Keep in mind that the subgroup $\{0, 2, 4, 6, 8\}$ has several generators, because $\{0, 2, 4, 6, 8\} = \langle 2 \rangle = \langle 4 \rangle$, as shown above.

Lemma 4.1. Let $H \leq G$ be a subgroup, and let $g \in G$. Then $g \in H$ is equivalent to $\langle g \rangle \subseteq H$.

Proof. Let $g \in H$. Because H is a subgroup, for every $k \in \mathbb{Z}$ the element $g^k \in H$, as well, but every element in $\langle g \rangle$ is of form g^k, so $\langle g \rangle \subseteq H$. The reverse implication is trivial, as $g \in \langle g \rangle$. □

Remark. Until we talk about **isomorphisms** (see Section 6), this remark is purely for building some informal intuition, but every cyclic group "behaves" in the same way as $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}$, because if $\operatorname{ord}(a) = n$, then $a^k \cdot a^l = a^{k+l \pmod n}$.

The next theorem somewhat justifies this intuition.

Theorem 4.1 (Theorem 4.1 in Gallian)**.** Let G be a group, and let $a \in G$.

1. If $\operatorname{ord}(a) = \infty$, then $a^i = a^j$ only if $i = j$.
2. If $\operatorname{ord}(a) = n < \infty$, then $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$, and $a^i = a^j$ if and only if $n | i - j$.

Proof.

1. If $a^i = a^j$ then $a^{i-j} = e$, but because the order of a is infinite, this can happen only for $i = j$.
2. Again, observe that $a^{i-j} = e$ and $a^n = e$. Applying the Lemma 3.1, we get that $a^{\gcd(n, i-j)} = e$. However, as n is the order of a, we have

   $$n \leq \gcd(n, i - j) \leq n \Rightarrow \gcd(n, i - j) = n.$$

   In particular, this implies $n | i - j$.

   Moreover, if $n | (i - j)$, then $(i - j) = kn$ for some $k \in \mathbb{Z}$, so

   $$a^{i-j} = a^{kn} = e^k = e.$$

   Therefore, all elements a^k for $0 \leq k \leq n - 1$ are distinct, as their difference of their powers can never be divisible by n.

□

Corollary 4.1.

1. $\operatorname{ord}(a) = |\langle a \rangle|$.
2. If G is a group, $g \in G$, $\operatorname{ord}(g) = n$, and $g^k = e$, then $n|k$.
3. If G is finite, $a, b \in G$, $ab = ba$, then $\operatorname{ord}(ab)|\operatorname{ord}(a)\operatorname{ord}(b)$.

Proof.

1. As the proof of Theorem 4.1(2) shows,
$$|\langle a \rangle| = |\{e, a, \ldots, a^{n-1}\}| = n = \operatorname{ord}(a).$$
2. Again, just replace $i - j$ with k in the proof of Theorem 4.1(2).
3. Let us denote $k = \operatorname{ord}(a), l = \operatorname{ord}(b)$. Then
$$(ab)^{kl} = \underbrace{(ab)(ab)\ldots(ab)}_{kl \text{ times}} = a^{kl}b^{kl} = e^l e^k = e.$$

□

Theorem 4.2 (Theorem 4.2 in Gallian)**.** Let $a \in G$ have $\operatorname{ord}(a) = n$, and consider $k \in \mathbb{N}$. Then

1. $\left\langle a^k \right\rangle = \left\langle a^{\gcd(n,k)} \right\rangle$
2. $\operatorname{ord}(a^k) = \dfrac{n}{\gcd(n,k)}$.

Proof.

1. First of all, we need to show that $\left\langle a^k \right\rangle \subset \left\langle a^{\gcd(n,k)} \right\rangle$. To do this, it is enough to show that $a^k \in \left\langle a^{\gcd(n,k)} \right\rangle$ due to Lemma 4.1. However, as $\gcd(n,k)|k$, we can find an integer m such that $a^k = a^{\gcd(n,k)m} \in \left\langle a^{\gcd(n,k)} \right\rangle$.

   Using the same idea, let us show now that $a^{\gcd(n,k)} \in \left\langle a^k \right\rangle$. For this we need to invoke the definition of the gcd again: consider integers s, t such that $\gcd(n,k) = ns + kt$. Then
$$a^{\gcd(n,k)} = a^{ns+kt} = (a^n)^s (a^k) = (a^k)^t \in \left\langle a^k \right\rangle.$$
   This argument proves that $\left\langle a^k \right\rangle \subseteq \left\langle a^{\gcd(n,k)} \right\rangle$ and $\left\langle a^k \right\rangle \supseteq \left\langle a^{\gcd(n,k)} \right\rangle$, so $\left\langle a^k \right\rangle = \left\langle a^{\gcd(n,k)} \right\rangle$.
2. The Corollary 4.1(1) shows that $\operatorname{ord}(a^k) = |\left\langle a^k \right\rangle| = |\left\langle a^{\gcd(n,k)} \right\rangle| = \operatorname{ord}(a^{\gcd(n,k)})$.

   Let us prove that $\operatorname{ord}(a^{\gcd(n,k)}) = \frac{n}{\gcd(n,k)}$. It is obvious that
$$(a^{\gcd(n,k)})^{\frac{n}{\gcd(n,k)}} = a^n = e,$$
   however, if $(a^{\gcd(n,k)})^m = e$, then $n|\gcd(n,k)m$ due to the Corollary 4.1(2). In particular, $\frac{n}{\gcd(k,n)}|m$. Therefore, $\frac{n}{\gcd(n,k)}$ the smallest power that works.

□

Example 4.3. Consider an element a in a group G with $\operatorname{ord}(a) = 30$. Then we have
$$\left\langle a^{26} \right\rangle = \left\langle a^{\gcd(26,30)} \right\rangle = \left\langle a^2 \right\rangle = \{e, a^2, a^4, \ldots, a^{28}\}$$
$$\left\langle a^{17} \right\rangle = \left\langle a^{\gcd(17,30)} \right\rangle = \langle a \rangle.$$
$$\left\langle a^{18} \right\rangle = \left\langle a^{\gcd(18,30)} \right\rangle = \left\langle a^6 \right\rangle = \{e, a^6, a^{12}, \ldots, a^{24}\}$$

Moreover,

$$\operatorname{ord}(a^{26}) = 30/\gcd(26,30) = 15,$$
$$\operatorname{ord}(a^{17}) = 30/\gcd(17,30) = 30,$$
$$\operatorname{ord}(a^{18}) = 30/\gcd(18,30) = 5,$$

which is compatible with the corollaries we proved before.

Corollary 4.2.

1. In every cyclic group, the order of every element divides the order of the group.
2. Let $a \in G$, $\operatorname{ord}(a) = n$. Then

   $$\left\langle a^i \right\rangle = \left\langle a^j \right\rangle \Leftrightarrow \gcd(n,i) = \gcd(n,j) \Leftrightarrow \operatorname{ord}(a^i) = \operatorname{ord}(a^j),$$

   and

   $$\langle a \rangle = \left\langle a^j \right\rangle \Leftrightarrow \ \gcd(n,j) = 1 \Leftrightarrow \operatorname{ord}(a) = |\left\langle a^j \right\rangle|$$

3. The element $k \in \mathbb{Z}/n\mathbb{Z}$ is a generator of $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(k,n) = 1$.

Proof.

1. Let $G = \langle g \rangle$. If $\operatorname{ord}(g) = n$, then for every $k \in \mathbb{Z}$ we have

   $$\operatorname{ord}(g^k) = \frac{n}{\gcd(n,k)},$$

   which divides n.

2. Again, this follows from Theorem 4.2:

   $$\left\langle a^i \right\rangle = \left\langle a^j \right\rangle \Leftrightarrow |\left\langle a^i \right\rangle| = |\left\langle a^j \right\rangle| \Leftrightarrow \frac{n}{\gcd(n,i)} = \frac{n}{\gcd(n,j)} \Leftrightarrow \operatorname{ord}(a^i) = \operatorname{ord}(a^j).$$

3. The element $k \in \mathbb{Z}/n\mathbb{Z}$ is a generator if and only if $|\langle k \rangle| = n$, but $|\langle k \rangle| = \operatorname{ord}(k) = \frac{n}{\gcd(n,k)} = n$, so $\gcd(n,k) = 1$.

□

Example 4.4. Let $G = \mathbb{Z}/30\mathbb{Z}$. Then we can verify that 6 does not generate G, but 7 or 11 do, as they are coprime with 30.

Example 4.5. Let $G = (\mathbb{Z}/50\mathbb{Z})^\times$. We can verify that $|G| = 20$, and 3 generates this group. But the corollary implies that 3^j also generates G for j which are coprime with 20.

Theorem 4.3 (Theorem 4.3 in Gallian)**.** Let $G = \langle a \rangle$. Then the following statements hold.

1. Every subgroup of G is cyclic.
2. Order of a subgroup in G divides $|G|$.
3. For each positive divisor k of n there is a unique subgroup of order k, and it is generated by $a^{n/k}$.

Example 4.6. Consider $G = \mathbb{Z}/20\mathbb{Z}$. The divisors of 20 are $1, 2, 4, 5, 10, 20$, so the respective subgroups are

$$\{0\}$$
$$\{0, 10\}$$
$$\{0, 5, 10, 15\}$$
$$\{0, 4, 8, 12, 16\}$$
$$\{0, 2, 4, \ldots 18\}$$
$$\{0, 1, 2, 3, \ldots, 19\} = G.$$

5 Permutation groups

Definition 5.1. Let A be a set. A **permutation** of A is a bijection $A \to A$. **A permutation group** of a set A is a set of permutations of A which forms a group with respect to the composition.

Remark. In our course we will always consider permutations of finite sets, with elements labeled by natural numbers, e.g. $A = \{1, 2, \dots, n\}$.

If α is a permutation on $\{1, 2, \dots, n\}$, then we can uniquely describe it via diagram

$$\begin{bmatrix} 1 & 2 & \dots & n-1 & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n-1) & \alpha(n) \end{bmatrix}.$$

Example 5.1. Let us multiply two permutations:

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}, \quad \gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix}.$$

Then

$$\sigma\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{bmatrix},$$

$$\gamma\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{bmatrix}.$$

This example shows that the multiplication of permutations is not a commutative operation. Finally, let us compute σ^{-1}:

$$\sigma^{-1} = \begin{bmatrix} 2 & 4 & 3 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{bmatrix}.$$

Example 5.2. Consider the group of **all** permutations of an n-element set $\{1, 2, \dots, n\}$. This group is usually denoted by S_n. Recall that $|S_n| = n!$ for all $n \geq 1$. For example, we can explicitly list all elements of S_3:

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}.$$

We can easily check that even S_3 is non-abelian, and this is a very small group!

Definition 5.2. Let $\{a_1, \dots, a_k\} \subset \{1, \dots, n\}$ be a subset, where all a_i are distinct. A **cycle** $\alpha = (a_1 a_2 \dots a_k)$ is a permutation, which acts as follows:

$$\alpha(a_i) = a_{i+1} \text{ for } 1 \leq i < k,$$
$$\alpha(a_k) = a_1,$$
$$\alpha(b) = b \text{ for } b \notin \{a_1, \dots, a_k\}$$

We will call the set $\{a_1, \dots, a_k\}$ **the support** of the cycle α, and k is called the **length** of α. Cycles of length k are sometimes referred to as k-cycles.

Example 5.3.

- $(1\,2\,3\,4) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$.
- $(1\,2\,6\,5\,4) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 3 & 1 & 4 & 5 \end{bmatrix}$. Notice how 3 is fixed by this cycle, as it is not in the support?
- Any cycle is preserved by a cyclic permiutation of the terms in its support, for example,

$$(1\,2\,3\,4) = (2\,3\,4\,1) = (3\,4\,1\,2) = (4\,1\,2\,3).$$

Remark. 2-cycles $(i\,j)$ are called **transpositions**.

Example 5.4.

$$(1\,2\,3)(1\,3) = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = (2\,3).$$

Finally, $Id = (1)$.

Remark. The cyclic structure of the identity permutation is not uniquely defined, as Id can be represented as (k) for any $1 \leq k \leq n$. This does not cause any contradictions, however.

So far, we have introduced two ways to encode permutations, but know we show that cycle notation is quite flexible when working with permutations.

Proposition 5.1. If $\alpha = (a_1 a_2 \dots a_k)$ and $\beta = (b_1 b_2 \dots b_l)$ have non-intersecting supports (such cycles are called **disjoint**), then $\alpha\beta = \beta\alpha$.

Proof. First of all, let us denote all the elements in $\{1, \dots, n\}$ not belonging to supports of α, β by c_i, where $1 \leq i \leq m$ for $m = n - k - l$. To check that $\alpha\beta = \beta\alpha$, we can just apply both permutations to a_i, b_i and c_i. Let us do these computations:

$$\begin{aligned} &\alpha\beta(a_i) = \alpha(a_i) = a_{i+1}, && \beta\alpha(a_i) = \alpha(a_{i+1}) = a_{i+1}, \\ &\alpha\beta(b_i) = \alpha(b_i + 1) = b_{i+1}, && \beta\alpha(b_i) = \alpha(b_i) = b_{i+1}, \\ &\alpha\beta(c_i) = \alpha(c_i) = c_i, && \beta\alpha(c_i) = \alpha(c_i) = c_i. \end{aligned}$$

Both computations agree, therefore, $\alpha\beta = \beta\alpha$. □

Theorem 5.1. Every permutation can be written as a product of disjoint cycles. Moreover, this presentation is unique up to a permutation of cycles themselves or cyclic shifts of terms inside the cycles.

Theorem 5.2. Let σ be a permutation, and let $\alpha = (a_1 a_2 \dots a_k)$ be a cycle. Then

$$\sigma\alpha\sigma^{-1} = (\sigma(a_1)\sigma(a_2), \dots, \sigma(a_k)).$$

Corollary 5.1. Let σ be a permutation, and let $\gamma = \alpha_1 \dots \alpha_m$, where α_i are disjoint cycles. Then

$$\sigma\gamma\sigma^{-1} = \sigma\alpha_1\sigma^{-1} \dots \sigma\alpha_m\sigma^{-1}.$$

Keep in mind that we can apply the previous theorem to any of $\sigma\alpha_i\sigma^{-1}$.

The above corollary shows that computing conjugates in S_n does not require to do manual permutation multiplication.

Example 5.5.

$$(4\,1\,2)(1\,2\,3)(4\,5)(4\,1\,2)^{-1} = (2\,4\,3)(1\,5).$$

Proposition 5.2. Every cycle $\alpha = (a_1 a_2 \dots a_n)$ can be decomposed as a product of transpositions:

$$\alpha = (a_1 a_2)(a_2 a_3) \dots (a_{n-1} a_n).$$

Proof. We proceed via induction. Let us prove that $(a_1 a_2 a_3) = (a_1 a_2)(a_2 a_3)$ first:

$$\begin{array}{lcl} (a_1 a_2 a_3) & = & (a_1 a_2)(a_2 a_3) \\ a_1 \mapsto a_2 & & a_1 \mapsto a_1 \mapsto a_2 \\ a_2 \mapsto a_3 & & a_2 \mapsto a_3 \mapsto a_3 \\ a_3 \mapsto a_2 & & a_3 \mapsto a_2 \mapsto a_1. \end{array}$$

As we can see, these two permuations agree on a_i. Then we assume that

$$(a_1 a_2 \dots a_{n-1}) = (a_1 a_2)(a_2 a_3) \dots (a_{n-2} a_{n-1}).$$

We proceed by proving

$$\begin{array}{lll} (a_1a_2\dots a_n) & = & (a_1a_2\dots a_{n-1})(a_{n-1}a_n) \\ a_1 \mapsto a_2 & & a_1 \mapsto a_1 \mapsto a_2 \\ a_2 \mapsto a_3 & & a_2 \mapsto a_2 \mapsto a_3 \\ \vdots & & \vdots \\ a_{n-2} \mapsto a_{n-1} & & a_{n-2} \mapsto a_{n-2} \mapsto a_{n-1} \\ a_{n-1} \mapsto a_n & & a_{n-1} \mapsto a_n \mapsto a_n \\ a_n \mapsto a_1 & & a_n \mapsto a_{n-1} \mapsto a_1. \end{array}$$

Once we have this, we use the assumption:

$$(a_1a_2\dots a_n) = (a_1a_2\dots a_{n-1})(a_{n-1}a_n) = (a_1a_2)(a_2a_3)\dots(a_{n-2}a_{n-1})(a_{n-1}a_n).$$

□

Also, we want to know how to compute orders of permutations. Thankfully, we can use the cycle decomposition!

Theorem 5.3. If α and β are two disjoint cycles, then $\mathrm{ord}(\alpha\beta) = \mathrm{lcm}(\mathrm{ord}(\alpha)\mathrm{ord}(\beta))$.

Arguing by induction, we can prove the following:

Corollary 5.2. Let σ be a permutation with a cycle decomposition $\sigma = \alpha_1 \dots \alpha_k$, where $\{\alpha_i\}_{1\le i\le k}$ are disjoint cycles, then

$$\mathrm{ord}(\sigma) = \mathrm{lcm}(\mathrm{ord}(\alpha_1), \dots, \mathrm{ord}(\alpha_k)).$$

5.1 Parity of permutations

Definition 5.3. An **inversion** of a permutation $\sigma \in S_n$ is an ordered pair (i, j), such that $i < j$ and $\sigma(j) < \sigma(i)$. We will denote the set of all inversions by $\mathrm{inv}(\sigma)$:

$$\mathrm{inv}(\sigma) = \{(i, j) : 1 \le i < j \le n, \sigma(j) < \sigma(i)\}.$$

Example 5.6. Let $\sigma = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$. Then we can see that

$$\begin{array}{ll} (\sigma(1), \sigma(2)) = (1, 3) & \text{(no inversion!)} \\ (\sigma(1), \sigma(3)) = (1, 2) & \text{(no inversion!)} \\ (\sigma(2), \sigma(3)) = (3, 2) & \text{(inversion!).} \end{array}$$

Therefore, $\mathrm{inv}(\sigma) = \{(2, 3)\}$.

Example 5.7. Now choose $\sigma = (3\,2\,1)$. Then

$$\begin{array}{ll} (\sigma(1), \sigma(2)) = (3, 1) & \text{(inversion!)} \\ (\sigma(1), \sigma(3)) = (3, 2) & \text{(inversion!)} \\ (\sigma(2), \sigma(3)) = (1, 2) & \text{(no inversion!).} \end{array}$$

Therefore, $\mathrm{inv}(\sigma) = \{(1, 2), (1, 3)\}$.

Example 5.8. A slightly more complicated example: choose $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{bmatrix}$. Then

$$\begin{array}{ll} (\sigma(1), \sigma(2)) = (3, 1) & \text{(inversion!)} \\ (\sigma(1), \sigma(3)) = (3, 4) & \text{(no inversion!)} \\ (\sigma(2), \sigma(3)) = (1, 4) & \text{(no inversion!)} \\ (\sigma(1), \sigma(4)) = (3, 2) & \text{(inversion!)} \\ (\sigma(2), \sigma(4)) = (1, 2) & \text{(no inversion!)} \\ (\sigma(3), \sigma(4)) = (4, 2) & \text{(inversion!).} \end{array}$$

Therefore, $\mathrm{inv}(\sigma) = \{(1, 2), (1, 4), (3, 4)\}$.

The definition allows us to compute the inversions of any transpositions relatively simply:

Proposition 5.3. If $1 \leq i < j \leq n$, then, denoting $\sigma = (i\, j)$, we have $|\mathrm{inv}(\sigma)| = 2(j-i-1)+1$. In particular, $|\mathrm{inv}(i\, i+1)| = 1$.

Proof. As all elements not equal to i and j are fixed, every inversion has to contain i or j as an element. However, this does not leave us with a lot of choices:

- Let us describe all inversions (i, x), where $i < x \leq n$. This implies that $\sigma(x) < j$, so the resulting inversions we obtain is
$$(i, i+1), (i, i+2), \dots (i, j-1), (i, j),$$
as $x > j+1$ will not work. This yields $j - i$ inversions.
- Let us describe all inversions (x, i), where $1 \leq x < i$. But all such x are fixed, so there are no such inversions.
- Let us describe all inversions (j, x), where $j < x \leq n$. Same argument shows that we don't get new inversions in this case.
- Let us describe all inversions (x, j), where $1 \leq x < j$. This implies that $i < \sigma(x)$, so we get
$$(i, j), (i+1, j), \dots (j-1, j).$$

We got two sets of inversions of size $j - i$, but the inversion (i, j) was in the both sets, so the total number of **distinct** inversions is $2(j-i-1)+1$. □

Remark. Still, as you can see, the actual proof involves checking a number of cases. Doesn't really look that pleasant, what if σ was a longer cycle?

Definition 5.4. Let $n \geq 2$. Then we define the **Vandermonde polynomial**
$$P(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j) \in \mathbb{C}[x_1, \dots, x_n].$$

For example, $P(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$. This polynomial will be extremely useful to us because it is a **skew-symmetric** polynomial. In other words,

Proposition 5.4. For every permutation $\sigma \in S_n$ we have
$$P(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = (-1)^{|\mathrm{inv}(\sigma)|} P(x_1, \dots, x_n).$$

Proof. To prove this proposition, we need to understand what monomials are contained in $P(x_{\sigma(1)}, \dots, x_{\sigma(n)})$. From the definition we know that
$$(x_i - x_j) | P(x_1, \dots, x_n) \Rightarrow (x_{\sigma(i)} - x_{\sigma(j)}) | P(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

However, because σ is invertible, we also have
$$(x_k - x_l) | P(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \Rightarrow (x_{\sigma^{-1}(k)} - x_{\sigma^{-1}(l)}) | P(x_1, \dots, x_n).$$

Because either $\sigma^{-1}(k) < \sigma^{-1}(l)$ or $\sigma^{-1}(l) < \sigma^{-1}(k)$, we get that $P(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ has the same factors as $P(x_{\sigma(1)}, \dots, x_{\sigma(n)})$.

However,
$$x_{\sigma(i)} - x_{\sigma(j)} = \begin{cases} x_{\sigma(i)} - x_{\sigma(j)}, & (i,j) \text{ is not an inversion} \\ (-1)(x_{\sigma(j)} - x_{\sigma(i)}), & (i,j) \text{ is an inversion.} \end{cases}$$

After reordering all inverted monomials, we are going to end up with $P(x_1, \dots, x_n)$, accumulating $(-1)^{\text{number of inversions}}$ on the way. □

This property allows to formulate the following useful definition:

Definition 5.5. The **sign** of a permutation $\sigma \in S_n$ is the number

$$\operatorname{sgn}(\sigma) = \frac{P(x_{\sigma(1)}, \dots, x_{\sigma(n)})}{P(x_1, \dots, x_n)} = (-1)^{|\operatorname{inv}(\sigma)|}.$$

Remark. Equivalently, we could define

$$\operatorname{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Let us list some useful properties of the sign:

Proposition 5.5. Let σ, τ be permutations.

1. $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$.
2. $\operatorname{sgn}(Id) = 1$.
3. $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$.
4. $\operatorname{sgn}(\sigma\tau\sigma^{-1}) = \operatorname{sgn}(\tau)$
5. If $t = (i\, j)$, then $\operatorname{sgn}(t) = -1$.
6. If $\alpha = (a_1 a_2 \dots a_k)$, then $\operatorname{sgn}(\alpha) = (-1)^{n-1}$.
7. If $\gamma = \alpha_1 \dots \alpha_k$, where α_i are disjoint cycles, then

$$\operatorname{sgn}(\gamma) = \prod_{1 \le i \le k} \operatorname{sgn}(\alpha_i) = (-1)^{\operatorname{ord}(\alpha_1) + \dots + \operatorname{ord}(\alpha_k) - k}.$$

Proof.

1. Notice that

$$\operatorname{sgn}(\sigma\tau) = \underbrace{\frac{P(x_{\sigma\tau(1)}, \dots, x_{\sigma\tau(n)})}{P(x_1, \dots, x_n)}}_{\operatorname{sgn}(\sigma\tau)} = \underbrace{\frac{P(x_{\sigma\tau(1)}, \dots, x_{\sigma\tau(n)})}{P(x_{\tau(1)}, \dots, x_{\tau(n)})}}_{\operatorname{sgn}(\sigma)} \underbrace{\frac{P(x_{\tau(1)}, \dots, x_{\tau(n)})}{P(x_1, \dots, x_n)}}_{\operatorname{sgn}(\tau)}.$$

2. $$\operatorname{sgn}(Id) = \frac{P(x_1, \dots, x_n)}{P(x_1, \dots, x_n)} = 1.$$

3. We already know that $1 = \operatorname{sgn}(Id) = \operatorname{sgn}(\sigma\sigma^{-1}) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma^{-1})$.
4. Follows from the first property.
5. We can use Proposition 5.4 that we proved before, which implies

$$\operatorname{sgn}(ij) = (-1)^{2(j-i-1)+1} = (-1)(-1)^{2(j-i-1)} = -1.$$

   Or we can use the (simpler) fact that $\operatorname{inv}(i\, i+1) = 1$, and observe

$$\operatorname{sgn}(ij) = \operatorname{sgn}((i+1\, j)(i\, i+1)(i+1\, j)) = \operatorname{sgn}(i\, i+1) = -1.$$

   The second proof does not rely on the Proposition anymore!

6. Just decompose the cycle into a product of transpositions.
7. Trivially follows from the previous properties.

□

Example 5.9.

- Let $\sigma = (1\,2\,4)(3\,7\,6\,5)$. Then
$$\operatorname{sgn}(\sigma) = \operatorname{sgn}((1\,2\,4))\operatorname{sgn}((3\,7\,6\,5)) = (-1)^2(-1)^3 = -1.$$
- Let $\tau = (1\,3)(4\,6)(5\,2)$. Then
$$\operatorname{sgn}(\tau) = (-1)^3 = -1.$$

Remark. Cycle decomposition provides the most efficient way to compute a sign of a permutation!

Lemma 5.1. Let $\sigma \in S_n$ be a permutation. Suppose that σ is written as a product of transpositions
$$\sigma = (i_1 j_1) \dots (i_m j_m).$$
Then, for any such representation, m is always odd or even, depending on the sign of σ.

This motivates us to call permutations with $\operatorname{sgn}(\sigma) = 1$ **even permutations**, and permutations with $\operatorname{sgn}(\sigma) = -1$ **odd permutations**, as they are represented by products of even number of permutations and products of odd number of permutations, respectively.

Lemma 5.2. The set of all even permutations in S_n forms a subgroup.

Proof. This can be proven by a quick application of a one-step test (see Theorem 3.1). If σ and τ are even, then τ^{-1} is even (the sign is the same), and any product of even permutations is even, as $1 \cdot 1 = 1$. Therefore, $\sigma\tau^{-1}$ also lies in this set. □

We will denote this subgroup by A_n, and it is usually called the **alternating subgroup of degree** n.

Proposition 5.6. The order of A_n equals $n!/2$ for all $n > 1$.

Proof. Let us establish a bijection between A_n and $S_n \setminus A_n$ like this:
$$\varphi : A_n \to S_n \setminus A_n, \quad \varphi(\sigma) = (1\,2)\sigma.$$

- This is a well-defined map as $(1\,2)$ is an odd permutation, and a product of an even and odd permutations is odd.
- This is an injective map due to a cancellation property (see Proposition 2.2):
$$(1\,2)\sigma_1 = (1\,2)\sigma_2 \Rightarrow \sigma_1 = \sigma_2.$$
- This map is surjective, as for any odd τ we can consider $\sigma = (1\,2)\tau$.
$$\varphi(\sigma) = (1\,2)(1\,2)\tau = \tau.$$

Therefore, the orders of A_n and $S_n \setminus A_n$ are equal, but $S_n = A_n \sqcup (S_n \setminus A_n)$. □

Remark. The set of all odd permutations does **not** form a subgroup of S_n. (why?)

Example 5.10. (This is better explained in the handwritten notes) Consider a regular tetrahedron with its vertices labeled by $\{1, 2, 3, 4\}$. Its group of symmetries permutes the vertices – so, it can be identified with a subgroup of S_4. Can we guess which subgroup it is?

Observe that the reflection with respect to plane which passes through an edge and the midpoint of the opposite side corresponds to a transposition. We can obtain every transposition in S_4 in such a way, but they generate S_4. Therefore, the group of symmetries can be identified with the whole S_4. It is only left to observe that all four vertices do not belong to the same plane, so any symmetry is uniquely defined by this action.

Even permutations correspond to orientation-preserving symmetries, and they are precisely the rotations in $\mathbb{R}^3$. We refer to Gallian's illustrations of these rotations.

Open-ended question. Can you try the same method to describe the group of symmetries of a cube? Or any of the remaining regular polyhedra? (this is hard...)

6 Group isomorphisms

Recall that multiplication of elements in cyclic subgroups is closely related to modular arithmetic computations. If $\mathrm{ord}(a) = n$, then

$$a^k a^l = a^{k+l(\mathrm{mod}\ n)}.$$

Let us formalize this intuition!

Definition 6.1. Let $G, \overline{G}$ be groups. A bijective mapping $\varphi : G \to \overline{G}$ is called a **(group) isomorphism**, if for any $a, b \in G$ we have

$$\varphi(ab) = \varphi(a)\varphi(b).$$

If such φ exists, we say that G is **isomorphic** to $\overline{G}$, and we write $G \cong \overline{G}$.

Example 6.1. Let G be a group and let $a \in G$.

- If $\mathrm{ord}(a) = \infty$, then the map $\varphi : \mathbb{Z} \to \langle a \rangle$, where $\varphi(k) = a^k$, is an isomorphism.
- If $\mathrm{ord}(a) = n < \infty$, then the map $\varphi : \mathbb{Z}/n\mathbb{Z} \to \langle a \rangle$, where $\varphi(k) = a^k$, is an isomorphism.

Essentially, we have already proven this earlier, but let us just demonstrate how we show that something is an **isomorphism**.

- **Step 0.** Show that the map is well-defined. In this case out construction is unambiguous.
  Step 1. Show that φ is injective. If $k \neq l$ then $a^k \neq a^l$, otherwise we would have $a^{k-l} = e$.
  Step 2. Show that φ is surjective. If $b \in \langle a \rangle$, then by definition, $b = a^k = \varphi(k)$ for some $k \in \mathbb{Z}$.
  Step 3. Show that φ "respects" the group operations.

$$\varphi(k + l) = a^k a^l = a^{k+l} = \varphi(k)\varphi(l).$$

- **Step 0.** Show that the map is well-defined. This is slightly not trivial, we have to show that if $k \equiv_n l$, then $\varphi(k) = \varphi(l)$. However, we know that $k = k'n + r$ and $l = l'n + r$ for some $k', l' \in \mathbb{Z}$ and $0 \leq r < n$, so

$$\varphi(k) = a^{k'n+r} = a^r (a^n)^{k'} = a^r e^{k'} = a^r e^{l'} = a^r a^{l'n+r} = \varphi(l).$$

  Therefore, it is a well-defined map, as elements in the same equivalence class map to the same element.
  Step 1. Show that φ is injective. This is implied by Theorem 4.1.1.
  Step 2. Show that φ is surjective. If $b \in \langle a \rangle$, then by Theorem 4.1.1., $b = a^k = \varphi(k)$ for some $k \in \mathbb{Z}/n\mathbb{Z}$.
  Step 3. Show that φ "respects" the group operations.

$$\varphi(k + l) = a^k a^l = a^{k+l} = \varphi(k)\varphi(l).$$

In other words, we have proven that every cyclic subgroup is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$.

Example 6.2. Let $G = (\mathbb{R}, 0, +)$, and $\overline{G} = (\mathbb{R}_{>0}, 1, \times)$. Consider

$$\varphi : G \to \overline{G}, \quad \varphi(x) = e^x.$$

This mapping is an isomorphism: this map is well-defined, it is injective, as $e^x = e^y \Rightarrow \ln(e^x) = x = y = \ln(e^y)$. It is surjective, because $e^{\ln(x)} = x$. It respects the group operations, because $e^{x+y} = e^x e^y$.

Moreover, it should be obvious from the above argument that $\varphi^{-1}(y) = \ln(y)$ is the inverse, and it is also an isomorphism.

Example 6.3. Not every bijective mapping between groups is an isomorphism: consider

$$\varphi : (\mathbb{R}, 0, +) \to (\mathbb{R}, 0, +), \quad \varphi(x) = x^3.$$

In this case φ is a bijection, but

$$(x + y)^3 = x^3 + y^3$$

does not hold for every $x, y \in \mathbb{R}$. However, if we consider

$$\varphi : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}, \quad \varphi(x) = x^3,$$

then it is an isomorphism, albeit a trivial one. Despite its triviality, this map is often referred to as the **Frobenius** mapping, and the non-trivial generalizations of this map are extremely useful when working with finite fields.

Proposition 6.1. Isomorphisms behave like equivalence relations. In other words, the following properties hold:

1. Any group is isomorphic to itself: $G \cong G$.
2. If $G \cong \overline{G}$, then $\overline{G} \cong G$.
3. If $G_1 \cong G_2$ and $G_2 \cong G_3$, then $G_1 \cong G_3$.

Proof.

1. The identity map Id is always an isomorphism: it is a bijection, and
$$Id(xy) = Id(x)Id(y) = xy.$$
2. If $\varphi : G \to \overline{G}$ is an isomorphism, then φ^{-1} is an isomorphism as well. It is a bijection, and for every $a, b \in \overline{G}$ we can find elements $x, y \in G$ such that $\varphi(x) = a$, $\varphi(y) = b$. So, we have
$$\varphi^{-1}(ab) = \varphi^{-1}(\varphi(x)\varphi(y)) = \varphi^{-1}(\varphi(xy)) = xy = \varphi^{-1}(a)\varphi^{-1}(b).$$
3. Let $\varphi : G_1 \to G_2$ be an isomorphism, and $\psi : G_2 \to G_3$ be an isomorphism. Then their composition $\psi \circ \varphi$ is an isomorphism as well, because for any $x, y \in G_1$ we have
$$(\psi \circ \varphi)(xy) = \psi(\varphi(x)\varphi(y)) = ((\psi \circ \varphi)(x))((\psi \circ \varphi)(y)).$$

□

Remark (which might be confusing!). Technically, we cannot say that $\cong$ is an equivalence relation on groups in the sense of Definition 2.4 for the most unusual reason: the collection of all groups **does not form a set**! It is just too big...

Definition 6.2. An isomorphism $\varphi : G \to G$ is called an **automorphism** of G. The set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$.

As a simple corollary from Proposition 6.1, we derive that the triple $(\mathrm{Aut}(G), Id, \circ)$ is a group with respect to the composition.

Example 6.4. Let G be a group, and fix an element $g \in G$. Then we define the map $\phi_g : G \to G$ as follows: $\phi_g(h) = ghg^{-1}$ for any $h \in G$. This is an automorphism, and such automorphisms are referred to as **inner automorphisms** of G. In particular, because $\phi_{g_1} \circ \phi_{g_2} = \phi_{g_1 g_2}$, we can see that G itself can always be realized as a subgroup of $\mathrm{Aut}(G)$!

Remark. It is a very non-trivial fact that all automorphisms of S_n are inner...except for $n = 6$. Unfortunately, all proofs require methods which are barely covered in MAT301. If we will ever get to Sylow subgroups or group actions, you can see `https://math.mit.edu/research/highschool/primes/materials/2016/conf/4-3%20Karnik-Jagadeesan.pdf` or `http://settheory.net/Out(S6)` for some expositions of this weird fact.

Also, a sketch of the proof is given in the very last section, Section 17.4.

7 Group homomorphisms

Definition 7.1. Let $G, \overline{G}$ be groups. Then a (not necessarily bijective) mapping $\varphi : G \to \overline{G}$ is called a **homomorphism**, if for every $x, y \in G$ we have

$$\varphi(xy) = \varphi(x)\varphi(y).$$

As you can see, there is only one difference between homomorphisms and isomorphisms – a homomorphism does not need to be bijective! Relaxing this condition, as you might guess, allows for way, way more nice examples!

Example 7.1.

1. First of all, notice that for every group G there is a homomorphism

   $$\mathrm{triv} : G \to \{e\}, \mathrm{triv}(g) = e.$$

   This map is often referred to as a "trivial" homomorphism. Moreover, this implies that for every two groups G and $\overline{G}$ there is a homomorphism $G \to \overline{G}$.

2. Any isomorphism is a homomorphism, as we have observed earlier.

3. Recall that by $\mathrm{GL}_n(\mathbb{R})$ we denote the group of invertible real-valued $n \times n$ matrices. Then the **determinant**, considered as a mapping

   $$\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times = (\mathbb{R} \setminus \{0\}, 1, \times), \quad A \mapsto \det(A),$$

   is a group homomorphism, because for every matrices A, B we have

   $$\det(AB) = \det(A)\det(B).$$

4. If we consider the sign function as a mapping from S_n to $\{-1, 1\}$, considered as a group with respect to multiplication, (check this group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$) is also a homomorphism, because we have shown that for every two permutations $\sigma, \tau \in S_n$ we have

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

5. Absolute value, considered as a map $|\cdot| : \mathbb{R}^\times \to \mathbb{R}^\times_{>0}$ is also a homomorphism, as

   $$|ab| = |a||b|.$$

6. Let G be an Abelian group. Then for any $k \in \mathbb{Z}$ the map $\phi_k : G \to G$, $\phi_k(a) = a^k$, is a group homomorphism.

   $$\phi_k(ab) = (ab)^k = a^k b^k = \phi_k(a)\phi_k(b).$$

7. Let H be a subgroup of G. Then the inclusion map $\iota : H \hookrightarrow G$ is an injective homomorphism due to the second subgroup test:

   $$\iota(ab) = ab = \iota(a)\iota(b) \in \iota(H),$$

   as if $a \in H$ and $b \in H$, then $ab \in H$.

   For example, consider a mapping

   $$\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}, \quad \varphi(0) = 0, \varphi(1) = 2.$$

   We can check that this is a homomorphism:

   $$\begin{aligned} \varphi(0+0) &= 0 = \varphi(0) + \varphi(0), \\ \varphi(0+1) &= 1 = \varphi(0) + \varphi(1), \\ \varphi(1+1) = \varphi(0) &= 0 = 2 + 2\varphi(1) + \varphi(1). \end{aligned}$$

   Moreover, the set-theoretic image of φ is a subgroup of $\mathbb{Z}/4\mathbb{Z}$. This is a general phenomenon for all homomorphisms, as we will see further.

8. Let $n > 1$. Consider the map

$$\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad \phi(x) = [x]_n = x \,(\text{mod } n).$$

Then ϕ is a surjective homomorphism, as the addition is well-defined mod n:

$$\phi(x + y) = [x + y]_n = [x]_n + [y]_n.$$

Now we want to prove several important properties which homomorphisms possess. To do this, we introduce two important subsets associated to a homomorphism:

Definition 7.2. Let $\varphi : G \to H$ be a homomorphism. Then we define

$$\text{Ker}(\phi) = \{g \in G : \varphi(g) = e_H\},$$

(called the **kernel** of φ)

$$\text{Im}(\varphi) = \{h \in H : \text{ there exists } g \in G \text{ such that } \varphi(g) = h\}.$$

(called the **image** of φ)

Proposition 7.1. For any homomorphism $\varphi : G \to H$, its kernel is a subgroup of G and its image is a subgroup in H.

Let us prepare by proving this small lemma about homomorphisms:

Lemma 7.1. Let $\varphi : G \to H$ be a homomorphism. Then

1. $\varphi(e_G) = e_H$,
2. For any $g \in G$ and $n \in \mathbb{Z}$ we have $\varphi(g)^n = \varphi(g^n)$.

Proof.

1. $$\varphi(e_G e_G) = \varphi(e_G) = \varphi(e_G)\varphi(e_G) \Rightarrow e_H = \varphi(e_G).$$

2. Let $n > 0$. Then we apply the standard induction argument. The definition implies that $\varphi(g^2) = \varphi(g)^2$, but if we assume that $\varphi(g^{k-1}) = \varphi(g)^{k-1}$, then we get

$$\varphi(g^k) = \varphi(g^{k-1}g) = \varphi(g^{k-1})\varphi(g) = \varphi(g)^{k-1}\varphi(g) = \varphi(g)^k.$$

If $n = -1$, then we observe that

$$\varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1}) = e_H = \varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g).$$

For $n < -1$ we proceed via a similar induction method.

□

As a corollary, we can easily see that

$$\varphi(g_1 \dots g_k) = \varphi(g_1) \dots \varphi(g_k)$$

for any $g_1, \dots g_k \in G$. Now we are ready to prove the proposition.

Proof of Proposition 7.1: Let us apply the one-step subgroup tests to both kernel and image.

Let $a, b \in \text{Ker}(\varphi)$. Then $\varphi(b^{-1}) = \varphi(b)^{-1} = e_H$, so $b^{-1} \in \text{Ker}(\varphi)$. Finally,

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = e_H e_H = e_H,$$

so $ab^{-1} \in \text{Ker}(\varphi)$.

Now let $a, b \in \text{Im}(\varphi)$. In other words, there are elements $x, y \in G$ such that $\varphi(x) = a$ and $\varphi(y) = b$. However, this implies that $\varphi(y^{-1}) = b^{-1}$, and $\varphi(xy^{-1}) = ab^{-1}$, so $ab^{-1} \in \text{Im}(\varphi)$. □

Remark. The image of a group under a homomorphism is always a subgroup regardless of whether this homomorphism is injective or not!

Example 7.2. Consider the map $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, where $\phi(k) = [k]_n$. Check that

$$\mathrm{Ker}(\phi) = n\mathbb{Z}, \quad \mathrm{Im}(\phi) = \mathbb{Z}/n\mathbb{Z}.$$

In particular, the kernel is, indeed, a subgroup of $\mathbb{Z}$.

Example 7.3. The kernel of $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ is precisely $\mathrm{SL}_n(\mathbb{R})$.

The statements we have proved imply the majority of statements in Theorem 10.1 and Theorem 10.2 in Gallian's textbook!

Theorem 7.1 (part of T10.1 in Gallian)**.** Let $\varphi : G \to \overline{G}$ be a homomorphism, and fix an element $g \in G$. Then we following properties hold:

1. $\varphi(e_G) = e_H$,
2. For any $g \in G$ and $n \in \mathbb{Z}$ we have $\varphi(g)^n = \varphi(g^n)$.
3. If $\mathrm{ord}(g) < \infty$, then $\mathrm{ord}(\varphi(g))|\mathrm{ord}(g)$.
4. $\mathrm{Ker}(\varphi) \subset G$ and $\mathrm{Im}(\varphi) \subset \overline{G}$ are subgroups.
5. $\varphi(a) = \varphi(b)$ if and only if $ab^{-1} \in \mathrm{Ker}(\varphi)$.
6. The homomorphism φ is injective if and only if $\mathrm{Ker}\,\varphi = \{e\}$.

Proof.

1. Proven in Lemma 7.1.
2. Proven in Lemma 7.1.
3. Let us denote $\mathrm{ord}(g) = n < \infty$. This implies $g^n = e$. Let us apply our homomorphism to both parts of this equality:
$$\varphi(g^n) = \varphi(e) \Leftrightarrow \varphi(g)^n = e.$$
This implies that $\mathrm{ord}(\varphi(g))|n$.
Warning. Of course, this does not imply that $\mathrm{ord}(\varphi(g)) = \mathrm{ord}(g)$!
4. Proven in Proposition 7.1.
5. We observe that
$$\varphi(a) = \varphi(b) \Leftrightarrow \varphi(a)\varphi(b)^{-1} = e \Leftrightarrow \varphi(ab^{-1}) = e \Leftrightarrow ab^{-1} \in \mathrm{Ker}(\phi).$$
6. ($\Rightarrow$) Suppose that φ is injective but there exists a non-trivial element $a \in G$ such that $\varphi(a) = e$. However, this would imply $\varphi(a) = \varphi(e) = e$, which contradicts injectivity as $e \neq a$.
($\Leftarrow$) If φ is not injective, then there exist two distinct elements $x, y \in G$ such that $\varphi(x) = \varphi(y)$. However, (5) implies that $xy^{-1} \in \mathrm{Ker}(\varphi)$, and $xy^{-1} \neq e$ due to the elements being distinct.

□

Corollary 7.1. Let $\varphi : G \to \overline{G}$ be an isomorphism. Then

1. For any $g \in G$ we have $\mathrm{ord}(g) = \mathrm{ord}(\varphi(g))$.
2. We have $\mathrm{Ker}(\varphi) = \{e\}$, and $\mathrm{Im}(\varphi) = \overline{G}$.

Proof. 1. We know that $\text{ord}(\varphi(g))|\text{ord}(g)$. However, φ^{-1} is a well-defined homomorphism as well, so $\text{ord}(\varphi^{-1}(\varphi(g)))|\text{ord}(\varphi(g))$. However, $\text{ord}(\varphi^{-1}(\varphi(g))) = \text{ord}(g)$. If $k|l$ and $l = k$ for some numbers k, l, then $k = l$.

2. If $\text{Ker}(\phi)$ containts a non-identity element a, then $\varphi(a) = \varphi(e)$, but this contradicts injectivity.

□

Theorem 7.2 (T10.2 in Gallian)**.** Let $H \subset G$ and $K \subset \overline{G}$ be subgroups. Consider a homomorphism $\varphi : G \to \overline{G}$. Let us denote

$$\varphi(H) = \{\varphi(h) : h \in H\}, \quad \varphi^{-1}(K) = \{g \in G : \varphi(g) \in K\}.$$

Then the following statements hold:

1. The subsets $\varphi(H) \subset G$ and $\varphi^{-1}(K) \subset \overline{G}$ are subgroups.
2. If H is cyclic, then $\varphi(H)$ is also cyclic.
3. If H is an Abelian subgroup, then $\varphi(H)$ is also Abelian.
4. $|\text{Ker}(\varphi)| = |\varphi^{-1}(\{a\})|$ for any $a \in \text{Im}(\varphi)$.

Proof.

1. Let $h_1, h_2 \in H$. Then $\varphi(h_1)\varphi(h_2) = \varphi(h_1h_2)$, $\varphi(e) = e$, and $\varphi(h)^{-1} = \varphi(h^{-1})$. We apply the second subgroup test.

   Now suppose that $g_1, g_2 \in \varphi^{-1}(K)$. It means that $\varphi(g_1) \in K$ and $\varphi(g_2) \in K$, but K is a subgroup, so $\varphi(g_2)^{-1} = \varphi(g_2^{-1}) \in K$, and $\varphi(g_1g_2^{-1}) \in K$. Now we apply the one-step subgroup test.

2. H is cyclic means that $H = \langle a \rangle$ for some $a \in G$. It is easily seen that $\varphi(H) = \{\varphi(a^k) = \varphi(a)^k : k \in \mathbb{Z}\} = \langle \varphi(a) \rangle$.

3. $\varphi(h_1)\varphi(h_2) = \varphi(h_1h_2) = \varphi(h_2h_1) = \varphi(h_2)\varphi(h_1)$

4. Fix an element $x \in \varphi^{-1}(\{a\})$. If $\varphi(x) = a$, and $y \in \text{Ker}(\varphi)$, then

   $$\varphi(xy) = \varphi(x)\varphi(y) = ae = a.$$

   Moreover, if $xy_1 = xy_2$ for some $y_1, y_2 \in \text{Ker}(\varphi)$, then $y_1 = y_2$. This proves that $|\varphi^{-1}(\{a\})|$ has at least $\text{Ker}(\varphi)$ elements.

   However, let us consider the mapping $\varphi^{-1}(\{a\}) \to \text{Ker}(\varphi)$, $x' \mapsto xx'^{-1}$. It is a well-defined map due to Theorem 7.1(5), and this map is injective. Therefore, $|\varphi^{-1}(\{a\})| = \text{Ker}(\varphi)$.

   Remark. In Section 10 we will show that $\varphi^{-1}(\{a\})$ is a **coset** of $\text{Ker}(\varphi)$.

□

Corollary 7.2. If we are given an isomorphism $\varphi : G \to \overline{G}$, then

1. G is cyclic if and only if $\overline{G}$ is cyclic
2. G is Abelian if and only if $\overline{G}$ is Abelian
3. $Z(G) \cong Z(\overline{G})$
4. for any $g \in G$ we have $C_G(g) \cong C_{\overline{G}}(\varphi(g))$.

This corollary suggests that any two isomorphic groups have the same properties: same orders, same centers, same centralizers, the orders of all elements are the same, and so on. Essentially, isomorphic groups can be considered "copies" of each other. (same up to relabeling of elements).

And if you ask what a **property** is – it is a statement about groups or elements in groups which is preserved via isomorphisms! (wait, don't we end up with a vicious circle???)

8 Homomorphisms from cyclic groups

Our goal for this section will be describing all homomorphisms from a cyclic (sub)group $\langle a \rangle$, where a is an element of some ambient group G', to an arbitrary group G.

First of all, we recall that any cyclic group is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$. Therefore, it is enough to describe all homomorphisms $\mathbb{Z} \to G$ and $\mathbb{Z}/n\mathbb{Z} \to G$.

Theorem 8.1. Every homomorphism $\varphi : \mathbb{Z} \to G$ is uniquely defined by $\varphi(1)$. In other words, for every $a \in G$ there is a unique homomorphism φ_a such that $\varphi_a(1) = a$.

Proof. Let $\varphi : \mathbb{Z} \to G$ be a homomorphism. Then for any $k \in \mathbb{Z}$ we have

$$\varphi(k) = \varphi(1 + 1 + \cdots + 1) = \varphi(k \cdot 1) = \varphi(1)^k.$$

This proves uniqueness.

Now we can define $\varphi_a(k) = a^k$ for all $k \in \mathbb{Z}$, and this is a well-defined homomorphism:

$$\varphi_a(k + l) = a^{k+l} = a^k a^l = \varphi_a(k)\varphi_a(l).$$

□

Corollary 8.1. The following 1-1 correspondence takes place:

$$\left\{ \begin{matrix} \text{homomorphisms} \\ \varphi : \mathbb{Z} \to G \end{matrix} \right\} \overset{1:1}{\longleftrightarrow} G,$$
$$\varphi_a \leftarrow g,$$
$$\varphi \to \varphi(1).$$

Keep in mind that we cannot compose any two homomorphisms $\mathbb{Z} \to G$, but, nevertheless, the bijection allows us to endow the set of homomorphisms with the group structure from G itself.

As for $\mathbb{Z}/n\mathbb{Z} \to G$, the argument is similar, but a bit tricker:

Theorem 8.2. Every homomorphism $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$ is uniquely defined by $\varphi(1)$. For every element $a \in G$ such that $a^n = e$ there is a unique homomorphism φ_a such that $\varphi(1) = a$.

Proof. Uniqueness is proven in the same way: for every $[k]_n \in \mathbb{Z}/n\mathbb{Z}$ we have

$$\varphi([k]_n) = \varphi(k \cdot [1]_n) = \varphi([1]_n)^k.$$

However, now we define φ_a by $\varphi_a([k]) = a^k$ for every $[k] \in \mathbb{Z}/n\mathbb{Z}$, and we want to determine when this is a well-defined map! In particular, let k and l be integers such that $k \equiv l \pmod{n}$. Therefore, $k = k'n + r$, and $l = l'n + r$, and we have

$$\varphi_a(k) = a^{k'n+r} = a^r (a^n)^{k'} = a^r (a^n)^{l'} = a^{l'n+r} = \varphi_a(l).$$

The fact that the value does not depend on the representative proves that φ_a is well-defined. Showing that φ_a respects the group operation is similar to the argument in the previous theorem, so we will omit it. □

Corollary 8.2. The following 1-1 correspondence takes place:

$$\left\{ \begin{matrix} \text{homomorphisms} \\ \varphi : \mathbb{Z}/n\mathbb{Z} \to G \end{matrix} \right\} \overset{1:1}{\longleftrightarrow} \{a \in G : a^n = e\},$$
$$\varphi_a \leftarrow g,$$
$$\varphi \to \varphi(1).$$

If G is Abelian, then the set on the right is a group, and we can transfer the group structure to the set of homomorphisms.

9 Cayley's theorem

Theorem 9.1 (Theorem 6.1 in Gallian)**.** Every finite group can be realized as a subgroup of S_n for some $n > 1$. In other words, every finite group is isomorphic to a group of permutations.

Remark. Gallian proves this theorem for infinite groups as well, as he allows for permutations of infinite sets.

Proof. Let G be a finite group. For every $g \in G$ define $T_g(x) = gx$. Then we notice that T_g is a permutation of G: T_g is injective due to the cancellation property, and $T_g(g^{-1}x) = x$ for any x, so T_g is surjective. Moreover,

$$T_g \circ T_h(x) = T_g(hx) = ghx = (gh)x = T_{gh}(x)$$

for every $g, h, x \in G$. Now we define a map

$$T : G \to \mathrm{Perm}(G), \quad T(g) = T_g,$$

where $\mathrm{Perm}(G)$ stands for the set of all permutations of G (in other words, bijections $G \to G$). The identity we proved before ensures that T is a homomorphism. Moreover, T is injective, because $T_g = Id_G \Rightarrow g = e$. Therefore, $\mathrm{Ker}(T) = \{e\}$, so T is injective. But this means that $T : G \to T(G) \subset \mathrm{Perm}(G)$ is an isomorphism of groups.

Finally, we remark that if G is finite, then $\mathrm{Perm}(G) = S_{|G|}$. □

A few remarks about this result: if used naively, this theorem is not really effective at all. For example, we can apply this theorem to D_4, thus obtaining an embedding $D_4 \hookrightarrow S_8$, but we know that, actually, D_4 can be easily realized as a subgroup of S_4.

Moreover, if we apply the Cayley's theorem to S_n itself, we don't get the identity map $S_n \to S_n$, we get an embedding $S_n \hookrightarrow S_{n!}$. What would one even do with this map???

Digression. However, Cayley's theorem becomes more useful when considering some general constructions. For example, in **representation theory**, which is, unfortunately, not covered in MAT301.

The rough idea is to construct, for a finite group G, an $\mathbb{R}$-vector space V_G with the basis v_g for all $g \in G$. In other words,

$$V_G = \left\{ \sum_{g \in G} a_g v_g : a_g \in \mathbb{R} \right\}.$$

Then we realize each element g as a linear operator on V_G be defining them on the basis elements: $g(v_h) = v_{T_g(h)} = v_{gh}$. This induces a mapping

$$T : G \to \mathrm{GL}(V_G),$$

which is called **the left regular representation of** G. The advantage of this construction is that it works for any finite group G, and it allows us to relate many numerical characteristic of the respective operators to any element $g \in G$. If every element acts as a linear operator, then we can correspond the trace, determinant, eigenvectors and eigenvalues (for example) to each element, and study G itself from the point of view of linear algebra.

10 Cosets

Definition 10.1. Let G be a group, and let $H \subset G$ be a subset (but in actual applications it will be a subgroup). For any $a \in G$ we define the following subsets:

$$aH = \{ah : h \in H\} \qquad (\textbf{the left coset of } H \textbf{ containing } a)$$
$$Ha = \{ha : h \in H\} \qquad (\textbf{the right coset of } H \textbf{ containing } a)$$
$$aHa^{-1} = \{aha^{-1} : h \in H\} \quad (\textbf{the conjugate of } H \textbf{ with respect to } a)$$

Example 10.1. Let $G = S_3$, and $H = \{e, (1\,2)\}$. Then we can describe all possible left cosets by going through all six permutations in S^3:

$$\begin{aligned} eH &= H \\ (1\,2)H &= \{(1\,2), e\} = H \\ (1\,3)H &= \{(1\,3), (3\,1\,2)\} \\ (2\,3)H &= \{(2\,3), (3\,2\,1)\} \\ (1\,2\,3)H &= \{(1\,3), (3\,1\,2)\} \\ (1\,3\,2)H &= \{(2\,3), (3\,2\,1)\} \end{aligned}$$

Example 10.2. Let $G = \mathbb{Z}/16\mathbb{Z}$, and let $H = \{0, 4, 8, 12\}$. Once again, we go through all possible elements in G to describe all left cosets:

$$\begin{aligned} 0 + H &= \{0, 4, 8, 12\} & 8 + H &= \{0, 4, 8, 12\} \\ 1 + H &= \{1, 5, 9, 13\} & 9 + H &= \{1, 5, 9, 13\} \\ 2 + H &= \{2, 6, 10, 14\} & 10 + H &= \{2, 6, 10, 14\} \\ 3 + H &= \{3, 7, 11, 15\} & 11 + H &= \{3, 7, 11, 15\} \\ 4 + H &= \{0, 4, 8, 12\} & 12 + H &= \{0, 4, 8, 12\} \\ 5 + H &= \{1, 5, 9, 13\} & 13 + H &= \{1, 5, 9, 13\} \\ 6 + H &= \{2, 6, 10, 14\} & 14 + H &= \{2, 6, 10, 14\} \\ 7 + H &= \{3, 7, 11, 15\} & 15 + H &= \{3, 7, 11, 15\} \end{aligned}$$

As these examples show us, all cosets have the same order, and they either do not intersect, or completely coincide. Indeed, these are very important properties that hold for all G and subgroups H.

Lemma 10.1 (p.193 in Gallian)**.** Let G be a group, and consider a subgroup $H \subset G$. If $a, b \in G$, then the following statements hold:

1. $a \in aH$
2. $aH = H$ if and only if $a \in H$
3. $(ab)H = a(bH)$ and $H(ab) = (Ha)b$
4. $aH = bH$ if and only if $a \in bH$ if and only if $a^{-1}b \in H$
5. We always have $aH = bH$ or $aH \cap bH = \emptyset$. Same for right cosets.
6. $|aH| = |bH|$.
7. $aH = Ha$ if and only if $H = aHa^{-1}$
8. aH is a subgroup of H if and only if $a \in H$.
9. $(aH)^{-1} = Ha^{-1}$.

Proof.

1. Observe that $ae \in aH$, as $e \in H$ but $ae = a$.
2. ($\Rightarrow$) Let $aH = H$. In particular, this means that $aH \subset H$, and $ae = a \in H$.

   ($\Leftarrow$) Let $a \in H$. It is easy to see that $aH \subset H$ due to the fact that H is a subgroup. However, for every $x \in H$ we have $x = a(a^{-1}x)$, and $a^{-1}x$ is also an element of H, so $H \subset aH$.
3. Follows immediately from associativity.

4. ($\Rightarrow$) If $aH = bH$, then (1) implies that $a \in bH$, and this means $a = bh$ for some $h \in H$. Multiplying by a^{-1} from the left, we get $a^{-1}b = h^{-1} \in H$.

   ($\Leftarrow$) If $a^{-1}b \in H$, then $b = ah$ for some element $h \in H$, and $bh^{-1} = a$, so $a \in bH$. But this also implies $(a^{-1}b)H = H$, due to associativity, we get $bH = aH$.

5. Suppose that $aH \cap bH$ is non-empty. Choose an element $x \in aH \cap bH$. So, $x = ah_1 = bh_2$. However, this implies $ah_1 = bh_2 \Leftrightarrow a = bh_2h_1^{-1} \Leftrightarrow b = ah_1h_2^{-1}$, so $a \in bH$ and $b \in aH$, now we use (4).

6. $|aH| = |H|$, as all elements ah for $h \in H$ are distinct.

7. Due to associativity, $aH = Ha \Leftrightarrow (aH)a^{-1} = (Ha)a^{-1} = H$.

8. aH is a subgroup implies that $e \in aH \Leftrightarrow a^{-1} \in H$.

9. For every $a \in G, h \in H$ we have

$$(ah)^{-1} = h^{-1}a^{-1} \in Ha^{-1}.$$

□

Remark. All of these properties carry over to right cosets as well due to property (9).

Example 10.3. Let us find all cosets of $H = \{1, 7\}$ in $G = (\mathbb{Z}/16\mathbb{Z})^\times$. First of all, recall that $G = \{1, 3, 5, 7, 9, 11, 13, 15\}$. And we don't need to try $7H$, as $7 \in H$. Moreover, we know that each coset has order 2. So we can try $3H$, and we get $3H = \{3, 5\}$. We don't need to try $5H$, as $5 \in 3H$, so $3H = 5H$. We can see that $9H = \{9, 15\}$, and the only remaining coset is $\{11, 13\} = 11H$. No need to consider every coset gH for all eight elements $g \in G$!

11 Lagrange's theorem and consequences

Theorem 11.1 (Lagrange's theorem)**.** If $H \subset G$ is a subgroup, then $|H|||G|$. Moreover, $|G|/|H|$ equals the number of left cosets, which, in turn, equals the number of right cosets.

Proof. First of all, notice that every element of G belongs to a left (right) coset. In particular, $g \in gH$ and $g \in Hg$ for all $g \in G$. Therefore,

$$G = \bigcup_{g \in G} gH = \bigcup_{g \in G} Hg.$$

However, due to Lemma 10.1(5), some of these cosets coincide, and some do not intersect at all. So, by throwing away overlapping cosets, we can find elements $g_1, \dots g_k \in G$ such that

$$G = \bigsqcup_{i=1}^{k} g_iH = \bigsqcup_{i=1}^{k} Hg_i.$$

However, as now the cosets g_iH are distinct, we get

$$|G| = \left|\bigsqcup_{i=1}^{k} g_iH\right| = \sum_{i=1}^{k} |g_iH| = \sum_{i=1}^{k} |H| = k|H|.$$

$$|G| = \left|\bigsqcup_{i=1}^{k} Hg_i\right| = \sum_{i=1}^{k} |Hg_i| = \sum_{i=1}^{k} |H| = k|H|.$$

Keep in mind that k is precisely the number of distinct cosets of H in G. □

As you can see, cosets do, indeed, partition G into equal chunks.

Remark. We can identify g_i as follows. If $H \subset G$ is a subgroup, then we can consider the following equivalence relations on G:

$$a \equiv_H b \Leftrightarrow b^{-1}a \in H \Leftrightarrow b \in aH,$$

$$a \,{}_H\!\equiv b \Leftrightarrow ab^{-1} \in H \Leftrightarrow a \in Hb.$$

Let us check that $\equiv_H$ is an equivalence relation. We know that $e \in H$, so $a \equiv_H a$. If $b^{-1}a \in H$, then $a^{-1}b \in H$ as well, and vice versa. So, $\equiv_H$ is symmetric. Finally,

$$b^{-1}a \in H, c^{-1}b \in H \Rightarrow c^{-1}bb^{-1}a = c^{-1}a \in H,$$

so $\equiv_H$ is transitive.

This allows us to consider equivalence classes of every element in G. Any two elements are in the same equivalence class if and only if their cosets coincide. So, to find g_i, we can take a single element from every distinct equivalence class.

This argument is dangerously close to the notion of **quotient groups**, so we will leave further discussion to later lectures.

Notation. If $H \subset G$ is a subgroup, by $|G : H|$ we will denote the number of left (or right) cosets of H in G. This number is called the **index** of H in G.

Corollary 11.1. Let $H \subset G$ be a subgroup. Then the following statements hold.

1. The index of H equals $\frac{|G|}{|H|}$.
2. In a finite group, the order of any element divides the order of G.
3. A group of prime order is cyclic.
4. If G is finite, then $a^{|G|} = e$. In other words, $\exp(G) \leq G$.
5. (Fermat's little theorem) For every integer a and prime p we have $a^p \equiv a (\text{mod } p)$.

Proof.

1. Follows directly from Lagrange's theorem.
2. If $a \in G$, consider $\langle a \rangle \subset G$. It is a subgroup of order $\text{ord}(a)$, so $|\langle a \rangle| = \text{ord}(a)$ has to divide $|G|$.
3. Let $|G| = p$. The order of any non-identity element has to divide p, so it has to equal p. But this means that every non-identity element is a generator of G.
4. Follows directly from the second statement.
5. Apply (4) to any non-trivial element in $(\mathbb{Z}/p\mathbb{Z})^\times$.

□

Remark. Lagrange's theorem **does not** imply the following statement: if k divides G, then G has a subgroup of order k.

This statement is false for A_4, because A_4 does not contain any subgroups of order 6.

Theorem 11.2 (T7.2 in Gallian)**.** Let H, K be two finite subgroups of a group G. Define $HK = \{hk : h \in H, k \in K\}$. Then we have $|HK| = \frac{|H||K|}{|H \cap K|}$.

Remark. HK is a subgroup in G if and only if $HK = KH$ (we will not need this fact for now).

Proof. For every element $x \in HK$ let us correspond a pair $(h(x), k(x)) \in H \times K$, so that

$$h(x)k(x) = x.$$

Of course, there are many ways to do such a correspondence.

Then we consider the following map:

$$\varphi : HK \times (H \cap K) \to H \times K, \quad \varphi(x, t) = (h(x)t, t^{-1}k(x)).$$

This is a well-defined map, now let us show that φ is a bijection.

Suppose that $\varphi(x_1, t_1) = \varphi(x_2, t_2)$. In other words, $(h(x_1)t_1, t_1^{-1}k(x_1)) = (h(x_2)t_2, t_2^{-1}k(x_2))$. Then we have

$$h(x_1)t_1 = h(x_2)t_2, \quad t_1^{-1}k(x_1) = t_2^{-1}k(x_2).$$

Multiplying these two equalities, we get

$$h(x_1)k(x_1) = h(x_2)k(k_2) \Leftrightarrow x_1 = x_2.$$

Now we just get $h(x_1)t_1 = h(x_1)t_2 \Rightarrow t_1 = t_2$.

Why is φ a surjection? Let $(h, k) \in H \times K$. If $\varphi(x, t) = (h', k')$, then $h'k' = x$. Moreover, $h(x)t = h'$, so we get

$$x = h'k', \quad t = (h(h'k'))^{-1}h'.$$

We can check that our choice is correct:

$$\varphi(x, t) = ((h(h'k'))(h(h'k'))^{-1}h', (h')^{-1}h(h'k')k(h'k')) = (h'k').$$

Therefore, φ is a bijection, and

$$|HK||H \cap K| = H \times K.$$

□

11.1 Classification of all groups of order $2p$ for prime $p > 2$

. We have already classified all groups of order p, where p is prime. All such groups are cyclic.

Theorem 11.3. Every group of order $2p$ for a prime $p > 2$ is isomorphic to $\mathbb{Z}/2p\mathbb{Z}$ or D_p.

First of all, let us formulate a lemma.

Lemma 11.1. If $|G| = 2p$, then G contains an element of order p.

Proof. Lagrange's theorem implies that every non-identity element has order 2 or p. Suppose there are no elements of order p, then for all $a \in G$ we have $a^2 = e$. However, this implies that G is Abelian, as $a = a^{-1}$ and $b = b^{-1}$ for every $a, b \in G$:

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

If $a \neq b$, then the subset $\{e, a, b, ab\}$ is a subgroup of G, but 4 cannot divide $2p$, thus we get a contradiction. □

Proof of Theorem 11.3. If G contains an element of order $2p$, then G is automatically isomorphic to $\mathbb{Z}/2p\mathbb{Z}$, so let's assume right away that G is not cyclic.

The above lemma shows that there is an element a of order p. Let us consider the cyclic subgroup $\langle a \rangle \subset G$. Fix an element $b \notin \langle a \rangle$. Once again, we know that the order of b equals 2 or p. Moreover, the order of the intersection $\langle a \rangle \cap \langle b \rangle$ has to divide the order of $\langle a \rangle = p$, therefore, $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Now we can apply Theorem 11.2, and we get

$$p| \langle b \rangle | = | \langle a \rangle \langle b \rangle | \leq 2p \Rightarrow | \langle b \rangle | \leq 2.$$

So, $| \langle b \rangle | = \text{ord}(b) = 2$.

Finally, let us consider ab. This is not an element of $\langle a \rangle$, so $\mathrm{ord}(ab) = 2$. This implies

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{-1}.$$

However, this is precisely the fundamental relation in D_p: $bab = a^{-1}$. Together with $a^p = e$ and $b^2 = e$, it uniquely defined the multiplication in G. Therefore, the correspondence $G \to D_p, a \mapsto r, b \mapsto s$, is a group isomorphism. □

As a corollary, all groups of order 6 are either cyclic or isomorphic to D_3. In particular, S_3 and D_3 are isomorphic.

12 Normal subgroups and quotient groups

12.1 Normal subgroups

Theorem 12.1. Let $H \subset G$ be a subgroup. Then the following statements are equivalent:

1. $Hg = gH$ for all $g \in G$.
2. $gHg^{-1} = H$ for all $g \in G$
3. $g^{-1}Hg = H$ for all $g \in G$
4. H is fixed by all inner automorphisms of G.

If any of these statements hold, we call H a **normal subgroup** of G.

Proof. (1) ⇒ (2) For every $g \in G$ and $h \in H$ we have

$$ghg^{-1} = x \Leftrightarrow gh = xg,$$

so $xg \in gH$. However, $gH = Hg$, so $xg \in Hg$, and $x \in Hgg^{-1}H$.

Alternatively, we could argue like this:

$$Hg = gH \Leftrightarrow H = Hgg^{-1} = (gH)g^{-1},$$

we use coset associativity in both arguments.

(2) ⇒ (3) Just replace g with g^{-1}.

(3) ⇒ (4) For every $g \in G$ and $h \in H$ we consider the inner automorphism $\varphi_g : x \mapsto gxg^{-1}$, so

$$\varphi_{g^{-1}}(h) = g^{-1}hg \in H,$$

so $\varphi_{g^{-1}}(H) = H$ for all $g \in G$.

(4) ⇒ (1) Let $x \in Hg$. Then $xg^{-1} \in H$, but $\varphi_{g^{-1}}(xg^{-1}) = g^{-1}x \in H$. □

Remark. As for subgroups, there is a special notation for normal subgroups: if $H \leq G$ is normal, we denote $H \triangleleft G$. Even then, there is a simpler way to check normality:

Theorem 12.2. Let H be a subgroup of G. Then $gHg^{-1} = H$ for all $g \in G$ is equivalent to $gHg^{-1} \subseteq H$.

Proof. One direction of this equivalence is trivial, so we assume that $gHg^{-1} \subseteq H$ for all $g \in G$. Then we can multiply both sides by g^{-1} from the left to get

$$g^{-1}gHg^{-1} = Hg^{-1} \subseteq g^{-1}H \Rightarrow H \subseteq g^{-1}Hg \subseteq H$$

for all $g \in G$. But

$$H \subseteq g^{-1}Hg \subseteq H \Rightarrow g^{-1}Hg = H,$$

and we apply Theorem 1.1. □

Here we provide several examples of normal subgroups.

Example 12.1.

1. Any group has two **trivial normal subgroups**: $H = \{e\}$ and $H = G$.
2. Any subgroup in abelian group is a normal subgroup.
3. $Z(G) \subset G$ is a normal subgroup.
4. $A_n \subset S_n$ is a normal subgroup due to the parity arguments.
5. The **Klein subgroup** $V_4 = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\} \subset A_4$ is a normal subgroup.
6. Let $G = D_n$ be the dihedral group. The rotation subgroup is a normal subgroup of index 2.
7. In general, (Minkovskii) product HK of two subgroups H, K is **not a subgroup**. However, it is a subgroup when H, K are both normal.

   If $h_1, h_2 \in H$ and $k_1, k_2 \in K$, then

   $$(h_1k_1)(h_2k_2) = h_1h_2k_1'k_2 \in HK$$

   for some $k_1' \in K$, due to the fact that $Kh_2 = h_2K$. Also, it is easily seen that $(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH = HK$, and $e \in HK$ as well.
8. If G has a unique subgroup H of a particular order, then H is also normal, as gHg^{-1} is a subgroup of same order.

12.2 Quotient (factor) groups

Theorem 12.3. Let $H \subset G$ be a normal subgroup. Let us denote

$$G/H = \{gH : g \in G\},$$

and define a binary operation $\cdot : G/H \times G/H \to G/H$ as follows:

$$aH \cdot bH = (ab)H.$$

Then $(G/H, \cdot, eH = H)$ is a well-defined group, which is called the **quotient (or factor) group** of G by H.

Proof. First of all, we need to show that the operation is well-defined. Suppose that $aH = a'H$ and $bH = b'H$. Equivalently, $a^{-1}a' \in H$ and $b^{-1}b' \in H$. Then we proceed as follows:

$$(ab)^{-1}ab' = b^{-1}a^{-1}ab' = b^{-1}b' \in H.$$

So, $(ab)H = (ab')H$.

$$(ab')^{-1}(a'b') = b'^{-1}a^{-1}a'b' \in b'^{-1}Hb = H.$$

Therefore,

$$ab'H = a'b'H,$$

and we have shown that the operation is well-defined. Now it remains to see that $H \in G/H$ acts as an identity element:

$$H(aH) = eHaH = (ea)H = aH, \quad (aH)H = (ae)H = a,$$

and

$$(aH)(a^{-1})H = (a^{-1}H)(aH) = H.$$

Finally, coset associativity shows that $\cdot$ is associative. □

Remark. Normality also allows us to replace left cosets with right cosets, the construction and the arguments are the same.

This is an incredibly important construction, and below we will show some examples.

Example 12.2.

1. If $H = \{e\}$, then $G/H \cong G$, because $gH = \{g\}$. If $H = G$, then $G/H \cong \{e\}$, as the only coset is $H = G$.

2. If $G = \mathbb{Z}$ and $H = n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$, then $G/H \cong \mathbb{Z}/n\mathbb{Z}$ **by definition** of $\mathbb{Z}/n\mathbb{Z}$.

3. S_n/A_n is a group of order 2, as there are $n!/2$ even and odd permutations. And it is easy realize this group as $\mathbb{Z}/2\mathbb{Z}$ as follows:

$$S_n/A_n = \{A_n, (1\,2)A_n\} \to \{1, -1\},$$
$$A_n \mapsto 1, \quad (1\,2)A_n \mapsto -1,$$

   so that all even permutations to go 1, and all odd permutations go to -1.

4. Same idea applies for $D_n = \{r^k, sr^k\}_{k=1,\dots,n}$,

$$D_n/\langle r\rangle = \{1, -1\} = \mathbb{Z}/2\mathbb{Z}.$$

5.

   Lemma 12.1. Any quotient of a cyclic group is cyclic.

   Proof. Let us denote $G = \langle a\rangle$, where $\mathrm{ord}(a) = n$. Every subgroup $H \subset G$ is also cyclic and is generated by a^k for some divisor $k|n$. Therefore,

$$G/H = \{H, aH, a^2H, \dots a^{k-1}H\},$$

   and aH generates G/H. □

6. It is also easily seen that any quotient of an Abelian group is Abelian once again, as

$$aHbH = abH = baH = bHaH.$$

   However, S_n is not Abelian, as its quotient S_n/A_n is.

Theorem 12.4 (Theorems 9.3, 9.4 in Gallian)**.** Let G be a group with the center $Z(G)$.

1. If $G/Z(G)$ is cyclic then G is Abelian.

2. $G/Z(G) \cong \mathrm{Inn}(G)$

Proof. We refer to Gallian, p.181-182 for proofs. □

Lemma 12.2. Let $aH \in G/H$. Then $\mathrm{ord}_{G/H}(aH)$ is the smallest positive integer k such that $a^k \in H$.

Proof. This immediately follows from the fact that $(aH)^k = a^kH = H$ if and only if $a^k \in H$. □

Remark. This lemma justifies the ord notation, as using $|aH|$ is rather ambiguous, as it stands for the number of elements in the coset as well!

Theorem 12.5. If G is a finite Abelian group and p is a prime divisor of $|G|$, then there is an element $a \in G$ of order p.

Proof. We will proceed by induction on $|G|$. The statement obviously holds for all G with $|G| = 2$, so we will assume that we have already proven the theorem for all groups of order smaller than G.

Choose an arbitrary non-identity element $x \in G$. WLOG we can assume that $\operatorname{ord}(x) = m$ is prime, otherwise we consider a suitable power x^k. If $m = p$, we are done. Otherwise, we define $H = \langle x \rangle$ and we consider $\overline{G} = G/H$. Keep in mind that $|\overline{G}| < |G|$, and $|\overline{G}|$ still divides p as $m \neq p$, so the induction hypothesis ensures that there is an element yH such that $\operatorname{ord}(yH) = p$.

In particular, $y \notin H$, and Lemma 12.2 implies that $y^p \in H$.

1. If $y^p = e$, we are done by setting $a = y$.
2. If $y^p = x^k$ for some k not dividing m, then

$$y^{pm} = x^{km} = (x^m)^k = e.$$

Now we have to prove that $\operatorname{ord}(y) = pm$: we already know that $y^p \neq e$, so either $\operatorname{ord}(y) = pm$ or $\operatorname{ord}(y) = m$. In the first case we finish the proof by setting $a = y^m$, and the second case does not happen because $y^m = e$ would imply $(yH)^m = (yH)^p = H$, but $\gcd(p, m) = 1$, so $(yH)^{\gcd(p,m)} = yH = H \Rightarrow y \in H$, which causes a contradiction.

□

Remark. Indeed, this theorem also holds for **any** finite group, and it follows from a theorem called **the first Sylow theorem**, and the proof also proceeds via induction by $|G|$. However, the issue lies in finding a suitable normal subgroup: in the Abelian case every subgroup is normal!

12.3 The first isomorphism theorem

Lemma 12.3. Let $\varphi : G \to \overline{G}$ be a homomorphism. Then $\operatorname{Ker}(\varphi) \subset G$ is a normal subgroup.

Proof. Let us show that for every $g \in G$ we have $g\operatorname{Ker}(\varphi)g^{-1} \subset \operatorname{Ker}(\varphi)$. However, for all $h \in \operatorname{Ker}(\varphi)$ we have

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e_{\overline{G}}.$$

Therefore, $ghg^{-1} \in \operatorname{Ker}(\varphi)$. □

Theorem 12.6 (The first isomorphism theorem)**.** Let $\varphi : G \to \overline{G}$ be a homomorphism. Consider a mapping

$$\overline{\varphi} : G/\operatorname{Ker}(\varphi) \to \operatorname{Im}(\varphi),$$
$$\overline{\varphi}(g\operatorname{Ker}(\varphi)) = \varphi(g) \in \operatorname{Im}(\varphi).$$

Then this is a well-defined group isomorphism. (usually called **the natural homomorphism** or **the quotient map**)

Proof. As always, we will separate the argument into four steps. Let us denote $K = \operatorname{Ker}(\varphi)$.

The map is well-defined. Let $gK = g'K$. Then $g^{-1}g' \in K$ and therefore,

$$\overline{\varphi}(g'K) = \varphi(g') = \varphi(g)\underbrace{\varphi(g^{-1}g')}_{\in \operatorname{Ker}(\varphi)} = \varphi(g) = \overline{\varphi}(gK).$$

The map is a homomorphism. For every $g, h \in G$ we have

$$\overline{\varphi}(ghK) = \varphi(gh) = \varphi(g)\varphi(h) = \overline{\varphi}(g)\overline{\varphi}(h).$$

Injectivity. Follows from the definition of kernel:

$$\overline{\varphi}(gK) = e \Leftrightarrow \varphi(g) = e \Leftrightarrow g \in \operatorname{Ker}(\varphi) \Leftrightarrow gK = K.$$

Surjectivity. Follows from the definition.

Therefore, $\overline{\varphi}$ is a well-defined group homomorphism. □

Let us consider a few examples:

Example 12.3.

1. The determinant defines a homomorphism $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$). We can check that $\mathrm{Ker}(\det) = \mathrm{SL}_n(\mathbb{R})$ and $\mathrm{Im}(\det) = \mathbb{R}^\times$, therefore,
$$\mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{R}) \cong \mathbb{R}^\times.$$
2. For every $n > 1$ we can consider the natural projection
$$p_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto [x]_n = x(\mathrm{mod}\ n).$$
Then, once again, we get
$$\mathbf{Z}/\mathrm{Ker}(p_n) = \mathbb{Z}/n\mathbb{Z}$$
from the first isomorphism theorem.
3. Consider the map $\exp : (\mathbb{R}, +) \to \mathbb{C}^\times$, $t \mapsto e^{2\pi i t}$. Then the kernel is isomorphic to $\mathbb{Z}$, and the image is the unit circle $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. Therefore,
$$\mathbb{R}/\mathbb{Z} \cong S^1,$$
and this identification is another convenient way to think about the unit circle!
4. Let $H \leq G$ be a (not necessarily normal) subgroup. Then we define
$$N(H) = \{x \in G : xHx^{-1} = H\} \quad (\textbf{normalizer } of H)$$
$$C(H) = \{x \in G : xhx^{-1} = h \forall h \in H\} \quad (\textbf{centralizer } of H).$$
Then we consider a homomorphism $\varphi : N(H) \to \mathrm{Aut}(H)$, $g \mapsto \varphi_g : x \mapsto gxg^{-1}$.
Its kernel is precisely $C(H)$, so the quotient $N(H)/C(H)$ can be realized as a subgroup of $\mathrm{Aut}(H)$.

Theorem 12.7 (Theorem 10.4)**.** Every normal subgroup is the kernel of a homomorphism.

Proof. If $H \subset G$ is a normal subgroup, then we just consider the quotient map $G \to G/H$, $g \mapsto gH$. This is a homomorphism with kernel H. □

13 Remaining isomorphism theorems

Definition 13.1. Let G be a group, and let H be a subgroup. The **normailzer** of H is a set
$$N_G(H) = N(H) = \{g \in G : gHg^{-1} = H\}.$$

Proposition 13.1. Let $H \subset G$ be a subgroup.

1. The normalizer is a subgroup of G.
2. $H \subseteq N(H)$,
3. H is a normal subgroup of $N(G)$. Moreover, $N(G)$ is the largest subgroup of G with this property.
4. $N(H) = G$ if and only if H is normal.

Proof. Let us apply the one-step subgroup test. Let $g_1, g_2 \in N(G)$. Then

$$(g_1^{-1}g_2)H(g_1^{-1}g_2)^{-1} = g_1^{-1}(g_2Hg_2^{-1})g_1 = g_1^{-1}Hg_1 \in H.$$

As $h \in H$, then $hHh^{-1} = H$, so $H \subset N(H)$.
If $g \in N(G)$, then

$$(g^{-1}hg)H(g^{-1}hg)^{-1} = g^{-1}h(gHg^{-1})h^{-1}g = g^{-1}hHh^{-1}g = g^{-1}Hg = H.$$

So, $H \triangleleft N(H)$. □

Theorem 13.1 (Second Isomorphism Theorem)**.** Let A, B be subgroups of G, and assume that A is a subgroup of $N(B)$. Then the following statements hold:

1. AB is a subgroup of G
2. B is normal in AB, $A \cap B$ is normal in A,
3. $AB/B \cong A/A \cap B$.

Proof. Let $a_1, a_2 \in A$, $b_1, b_2 \in B$. We want to show that $b_1^{-1}a_1^{-1}a_2b_2 \in AB$ and then use the one-step subgroup test!

$$b_1^{-1}a_1^{-1}a_2b_2 = a_1^{-1}a_2\underbrace{(a_1^{-1}a_2)^{-1}b_1^{-1}(a_1^{-1}a_2)}_{b' \in B}b_2 = a_1^{-1}a_2b'b_2 \in AB.$$

Now we have to show that for any $a \in A$ and $b_1, b_2 \in B$ we have $(ab_1)^{-1}b_2(ab_1) \in B$:

$$(ab_1)^{-1}b_2(ab_1) = b_1^{-1}\underbrace{a^{-1}b_2a}_{\in B}b_1 \in B.$$

Now, let us show that for any $b \in A \cap B$ and $a \in A$ we have $a^{-1}ba \in A \cap B$:

$$b \in A \Rightarrow a^{-1}ba \in A \quad b \in B, a \in N(B) \Rightarrow a^{-1}ba \in B.$$

Finally, we need to establish the isomorphism between quotients. Consider the composition

$$\phi : A \to AB \to AB/B, \quad a \mapsto a \mapsto aB.$$

Both natural maps are homomorphisms, therefore, ϕ is also a homomorphism. Let us determine the kernel of ϕ:

$$\phi(a) \in \mathrm{Ker}(\phi) \Leftrightarrow aB = B \Leftrightarrow a \in A \cap B.$$

Finally, we need to show that ϕ is surjective. However, every coset of AB/B satisfies $(ab)B = a(bB) = aB$, so we can define $\phi^{-1}(abB) = a$. Then we finish the argument by applying the First Isomorphism Theorem. □

Theorem 13.2 (Third Isomorphism Theorem)**.** Let G be a group, and consider two normal subgroups H, K such that H is a subgroup of K. Then

1. K/H is a normal subgroup of G/H,
2. $(G/H)/(K/H) \cong G/K$.

Proof. Let $kH \in K/H$ and $gH \in G/H$. Then normality of K ensures,

$$(g^{-1}kg) \in K,$$

but

$$(gH)^{-1}(kH)gH = (g^{-1}kg)H \in K/H.$$

Once again, let us consider a certain composition of quotient (natural) homomorphisms:

$$\psi : G/H \to G/K, \quad gH \mapsto gK.$$

This map is well-defined as $H \subset K$. So, this is a homomorphism, and it is trivial to show that it is surjective. Now let us find its kernel:

$$gH \in \mathrm{Ker}(\psi) \Leftrightarrow gK = K \Leftrightarrow g \in K,$$

so $\mathrm{Ker}(\psi) = \{kH : k \in K\} = K/H$. □

14 Direct products

14.1 External direct products

Definition 14.1. Let $G_1, \dots G_n$ be groups. Then, with respect to the group operation on $G_1 \times \cdots \times G_n$ is defined as follows:

$$(g_1, \dots, g_n) \cdot (g_1', \dots, g_n') = (g_1 g_1', \dots g_n g_n'),$$

the product $G_1 \times \cdots \times G_n$ becomes a group. This group is called the **(external) direct product of** G_i.

The identity is $(e_{G_1}, \dots, e_{G_n})$, and $(g_1, \dots, g_n)^{-1} = (g_1^{-1}, \dots, g_n^{-1})$. In other words, all operations are component-wise.

Remark. Usually, when all groups G_i are equipped with addition, the operation $\times$ is replaced by $\oplus$, just like in linear algebra! However, this distinction is known to cause confusion because of perceived difference between $\oplus$ and $\times$, which, in fact, does not exist: these are the same operations.

Example 14.1.

1. Let all $G_i = (\mathbb{R}, +)$. Then $G_1 \times \cdots \times G_n = (\mathbb{R}^n, +) = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$. Same applies for any field F considered as an additive group. Finally,

$$(\mathbb{Z}, +) \times \cdots \times (\mathbb{Z}, +) = (\mathbb{Z}^n, +).$$

2. Let us consider $G_1 \times G_2 = (\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/10\mathbb{Z})^\times = U(8) \times U(10)$. As $U(8) = \{1, 3, 5, 7\}$ and $U(10) = \{1, 3, 7, 9\}$, we have

$$\begin{aligned} U(8) \times U(10) = \{&(1,1), (1,3), (1,7), (1,9),\\ &(3,1), (3,3), (3,7), (3,9),\\ &(5,1), (5,3), (5,7), (5,9),\\ &(7,1), (7,3), (7,7), (7,9)\}. \end{aligned}$$

   For example, $(3,3)(7,9) = (21 (\mathrm{mod}\ 8), 27 (\mathrm{mod}\ 10)) = (5,7)$.

3. Let us consider $G_1 = \mathbb{Z}/2\mathbb{Z}$ and $G_2 = \mathbb{Z}/3\mathbb{Z}$. Then

$$\begin{aligned} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{&(0,0), (0,1), (0,2),\\ &(1,0), (1,1), (1,2)\}. \end{aligned}$$

   Moreover, this is a **cyclic group**, as $(1,1)$ is a generator:

$$\begin{aligned} (1,1) + (1,1) &= (0,2),\\ (0,2) + (1,1) &= (1,0),\\ (1,0) + (1,1) &= (0,1),\\ (0,1) + (1,1) &= (1,2),\\ (1,2) + (1,1) &= (0,0). \end{aligned}$$

   Therefore, $\mathrm{ord}_{G_1 \times G_2}((1,1)) = 6$.

4. In one of the earlier assignments we asked you to classify all groups of order 4. Now we have enough tools at our disposal to establish this classification as cleanly as possible.

   Let $G = \{e, a, b, c\}$, where e is the identity. Due to Lagrange's theorem, orders of all elements divide 4. Therefore, we have two cases:

   - If there is an element of order 4, then G is cyclic and generated by this element.
   - If all elements have order 2, then G is Abelian. Moreover, we can't have $ab = a$ or $ab = b$, as this would imply $a = e$ or $b = e$. Therefore, $ab = c$, $ac = b$ and $bc = a$, so the mapping

   $$(0,0) \mapsto e,$$
   $$(0,1) \mapsto a,$$
   $$(1,0) \mapsto b,$$
   $$(1,1) \mapsto c,$$

   is a group isomorphism. It is a bijection and it respects the group operations as we have recovered the multiplication table for G. In this case $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

   So, $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $G \cong \mathbb{Z}/4\mathbb{Z}$.

Let us establish some properties of direct products.

Theorem 14.1. Direct products are commutative in the following sense: there is a "natural" group isomorphism

$$G_1 \times G_2 \cong G_2 \times G_1.$$

Theorem 14.2. Direct products are associative in the following sense: there is a "natural" group isomorphism

$$(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3).$$

Proof. Just consider the mapping

$$((g_1, g_2), g_3) \mapsto (g_1, (g_2, g_3)).$$

Obviously, this is a group homomorphism and it is a bijection. □

Theorem 14.3. Let G_1, G_2 be finite groups. Then

1. $|G_1 \times G_2| = |G_1||G_2|$.
2. If G_1 and G_2 are Abelian, then their product is Abelian, as well.
3. For any $g_1 \in G$ and $g_2 \in G_2$ we have

   $$\mathrm{ord}_{G_1 \times G_2}((g_1, g_2)) = \mathrm{lcm}(\mathrm{ord}(g_1), \mathrm{ord}(g_2)).$$

4. Recall that $\exp(G) = \mathrm{lcm}\{\mathrm{ord}(g) : g \in G\}$. Then

   $$\exp(G_1 \times G_2) = \mathrm{lcm}(\exp(G_1), \exp(G_2)).$$

5. $Z(G_1 \times G_2) \cong Z(G_1) \times Z(G_2)$.

Proof.

1. This follows immediately from the definition of a direct product.
2. $$(g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2 h_2) = (h_1 g_1, h_2 g_2) = (h_1, h_2)(g_1, g_2).$$

3. For convenience, let us denote $m = \text{ord}(g_1)$ and $n\text{ord}(g_2)$. As $m|\text{lcm}(m,n)$ and $n|\text{lcm}(m,n)$, we have
$$g_1^{\text{lcm}(m,n)} = e, \quad g_2^{\text{lcm}(m,n)} = e.$$
Therefore, $(g_1, g_2)^{\text{lcm}(m,n)} = (e, e)$, so $\text{ord}_{G_1 \times G_2}((g_1, g_2))|\text{lcm}(m,n)$.
However, $(g_1, g_2)^k = e$ means that $g_1^k = e$ and $g_2^k = e$, so k has to be a divisor of both n and m. But the smallest such k is precisely the least common multiple.

4. Follows from the associativity of lcm.

5. Let $(c_1, c_2) \in Z(G_1 \times G_2)$. Then, for every $(g, h) \in G_1 \times G_2$ we have
$$(c_1 g, c_2 h) = (c_1, c_2)(g, h) = (g, h)(c_1, c_2) = (gc_1, hc_2).$$
Therefore, $c_1 \in Z(G_1)$ and $c_2 \in Z(G_2)$, so the mapping
$$(c_1, c_2) \to (c_1, c_2) \in Z(G_1) \times Z(G_2)$$
is a group isomorphism.

□

Remark. These results immediately can be generalized to arbitrary finite group products via induction by the number of groups involved.

Example 14.2.

1. Using direct products, we can list many (potentially) pairwise non-isomorphic groups of order 100 by going over all groups with orders that divide 100:
$$\begin{aligned}
\exp(\mathbb{Z}/100\mathbb{Z}) &= 100,\\
\exp(\mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) &= 50,\\
\exp(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) &= 20,\\
\exp(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) &= 10\\
\exp(D_{50}) &= 50,\\
\exp(D_{10} \times \mathbb{Z}/5\mathbb{Z}) &= 10,\\
\exp(D_5 \times \mathbb{Z}/10\mathbb{Z}) &= 10\\
\exp(D_5 \times D_5) &= 10.
\end{aligned}$$
The first four groups are Abelian due to Theorem 14.3(2), the last four groups are non-abelian. The last three groups can be shown to be non-isomorphic by comparing the number of elements of orders $2, 5$ and 10.

2. For example, let us count all elements of orders $2, 5$, and 10 in $D_5 \times \mathbb{Z}/10\mathbb{Z}$.
   - The order of (g_1, g_2) equals 2 is and only if one of g_1, g_2 has order 2. There are 5 elements or order 2 in D_5 and only one element of order 2 in $\mathbb{Z}/10\mathbb{Z}$. Therefore, there are $5+5+1 = 11$ elements of order 2 in the direct product.
   - The order of (g_1, g_2) equals 5 is and only if one of g_1, g_2 has order 5. There are 4 elements or order 5 in D_5 and 4 elements of order 5 in $\mathbb{Z}/10\mathbb{Z}$. Therefore, there are $16 + 4 + 4 = 24$ elements of order 5 in the direct product.
   - The remaining $100 - 1 - 11 - 24 = 64$ elements have order 10.

Lemma 14.1. The direct product of **two** cyclic groups is cyclic if and only if their orders are coprime.

Proof. Let $G_1 = \langle g \rangle$ and $G_2 = \langle h \rangle$, so that $|G_1| = n$ and $|G_2| = m$.

($\Rightarrow$) Suppose that $G_1 \times G_2$ is cyclic, then it is generated by (g^k, h^l) for some k, l. Theorem 14.3 implies that

$$nm = \operatorname{ord}(g^k, h^l) = \operatorname{lcm}(\operatorname{ord}(g^k), \operatorname{ord}(h^l)) = \operatorname{lcm}(n/\gcd(n,k), m/\gcd(m,l)).$$

However,

$$nm = \operatorname{lcm}(n/\gcd(n,k), m/\gcd(m,l)) \leq \frac{nm}{\gcd(n,k)\gcd(m,l)},$$

so $\gcd(n,k) = \gcd(m,l) = 1$ and m, n are coprime.

($\Leftarrow$) If $\gcd(n,m) = 1$, then (g,h) generates the product due to Theorem 1.2. □

Applying induction by the number of groups, we get the following corollary immediately:

Corollary 14.1. The direct product of **any** number of cyclic groups is cyclic if and only if their orders are pairwise coprime.

Corollary 14.2. Let $m = n_1 \dots n_k$. Then $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$ if and only if n_i are pairwise coprime.

Proof. If n_i are pairwise coprime, we apply the Corollary 1.1. But if these groups are isomorphic, then their exponents are the same:

$$\exp(\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}) = \operatorname{lcm}(n_1, \dots, n_k) = n_1 \dots n_k.$$

The equality is only attained when n_i are pairwise coprime. □

Example 14.3. $\mathbb{Z}/12\mathbb{Z}$ can be decomposed as a product of $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$, as $\gcd(3,4) = 1$.

Also, $\mathbb{Z}/24\mathbb{Z}$ can be decomposed as a product of $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/8\mathbb{Z}$, as $\gcd(3,8) = 1$.

However, $\mathbb{Z}/25\mathbb{Z}$ **cannot** be decomposed as a product of non-trivial cyclic subgroups, as $\mathbb{Z}/25\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, as the exponents are different.

Theorem 14.4.

1. The projection maps $\pi_G : G \times H \to G$ and $\pi_H : G \times H \to H$ are group homomorphisms.
2. If $K \subset G \times H$ is a normal subgroup, then $\pi_G(K)$ and $\pi_H(K)$ are also normal subgroups of G and H, respectively.
3. Let G_i be groups and consider $H_i \triangleleft G_i$. Then

$$\frac{G_1 \times \dots \times G_n}{H_1 \times \dots \times H_n} \cong G_1/H_1 \times \dots \times G_n/H_n.$$

In particular, $H_1 \times \dots H_n$ is a normal subgroup.

Proof. Let us construct a homomorphism

$$\psi : G_1 \times \dots \times G_n \to G_1/H_1 \times \dots \times G_n/H_n,$$

$$\psi(g_1, \dots, g_n) = (g_1H_1, g_2H_2, \dots, g_nH_n).$$

It remains to apply the First Isomorphism Theorem to get the isomorphism. □

Example 14.4. Let us, finally, establish the fact that $D_5 \times D_5, D_5 \times \mathbb{Z}/10\mathbb{Z}$, and $D_{10} \times \mathbb{Z}/5\mathbb{Z}$ are non-isomorphic.

Recall that $C(D_{10}) \cong \mathbb{Z}/2\mathbb{Z}$, and $C(D_5) = \{e\}$. So,

$$C(D_5 \times D_5) = \{e\},$$
$$C(D_5 \times \mathbb{Z}/10\mathbb{Z}) = \mathbb{Z}/10\mathbb{Z},$$
$$C(D_{10} \times \mathbb{Z}/5\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

So, we managed to isolate $D_5 \times D_5$, and we are left with $D_5 \times \mathbb{Z}/10\mathbb{Z}$ and $D_{10} \times \mathbb{Z}/5\mathbb{Z}$. Unfortunately, their centers are also isomorphic, so we have to come up with another invariant to separate the groups.

Let us identify $\mathbb{Z}/2\mathbb{Z} = \{\pm 1\}$. Suppose that one aims to construct an isomorphism $\varphi : D_{10} \to D_5 \times \mathbb{Z}/2\mathbb{Z}$. One can verify that both groups have a unique element of order 10, so $\varphi(r) = (r, -1)$. This forces φ to be defined on every rotation in D_{10}. Now let's just try $\varphi(s) = (s, 1)$. First of all, we want to show that φ is well-defined by finding the images of sr^j for $0 = 1, \ldots, 9$:

$$\varphi(sr^j) = (s, 1)(r^j, (-1)^j) = (sr^j, (-1)^j).$$

In other words, we have $\varphi(s^\varepsilon r^j) = (s^\varepsilon r^j, (-1)^j)$. For $j' = j + 5$ we have

$$\varphi(s^\varepsilon r^{j'}) = (s^\varepsilon r^{j+5}, (-1)^{j+5}) = (s^\varepsilon r^j, -(-1)^j),$$

so φ is a well-defined bijection. Checking that this map respects the group operations is left as an exercise.

14.2 Internal direct products

Definition 14.2. Let G be a group. Suppose there exist two **normal** subgroups $H, K \leq G$ that satisfy the following properties:

1. $HK = G$,
2. $H \cap K = \{e\}$.

Then G is the **internal direct product** of H and K, and we write $G = H \times K$.

This notation is compatible with the notion of an external direct product:

Theorem 14.5. If H, K satisfy the conditions of the above definition, then the map

$$i : H \times K \to G, \quad i(h, k) = hk$$

is a group isomorphism.

Proof. First of all, we need to show that this is a group homomorphism.

$$i((h_1, k_1)(h_2, k_2)) = h_1 h_2 k_1 k_2 = h_1 k_1 (k_1^{-1} h_2 k_1) k_2.$$

As H is normal, we have $k_1^{-1} h_2 k_1 \in H$. However, this would force $h_2^{-1}(k_1^{-1} h_2 k_1) \in H$, and normality of K implies

$$h_2^{-1}(k_1^{-1} h_2 k_1) = (h_2^{-1} k_1^{-1} h_2) k_1 \in K k_1 = K.$$

Therefore, $h_2^{-1} k_1^{-1} h_2 k_1 \in H \cap K = \{e\}$, therefore, $h_2 k_1 = k_1 h_2$. In particular,

$$i((h_1, k_1)(h_2, k_2)) = h_1 k_1 (k_1^{-1} h_2 k_1) k_2 = (h_1 k_1)(h_2 k_2) = i((h_1, k_1)) i((h_2, k_2)).$$

Injectivity follows from $H \cap K = \{e\}$, and surjectivity follows from $G = HK$. Therefore, i is an isomorphism. □

We can define internal direct products for any finite collection of normal subgroups.

Definition 14.3. Let G be a group and consider a finite family $(H_i)_{i=1,\ldots,}$ of normal subgroups. Suppose that the following conditions are satisfied:

1. $G = H_1 \ldots H_n = \{h_1 h_2 \ldots h_n : h_i \in H_i\}$,
2. $(H_1 H_2 \ldots H_i) \cap H_{i+1} = \{e\}$ for all $i = 1, \ldots, n-1$.

Then G is the **internal direct product** of H_i and we write $G = H_1 \times \ldots H_n$

Theorem 14.6. If H_i saisfy the conditions outlined above, then the map

$$H_1 \times \dots H_n \to G, \quad (h_1, \dots, h_n) \mapsto h_1 h_2 \dots h_n$$

is a group isomorphism.

Lemma 14.2. If G is an internal direct product of two normal subgroups H, K, then

$$G/H \cong K, \quad G/K \cong H.$$

Proof. Theorem 14.5 allows us to consider $i^{-1} : G \to H \times K \to K$, where $H \times K \to K$ is the projection map. This is a surjective homomorphism with the kernel being H, now it remains to use the first isomorphism theorem. We can interchange H and K to get the other isomorphism. □

Knowing about internal direct products, we are now also able to classify all groups of order p^2 for a prime p.

Theorem 14.7. Every group of order p^2 is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proof. Let us denote the group by G. Lagrange's theorem implies that order of any element divides p^2. If there is an element of order p^2, then G is cyclic.

So let us assume that all elements have order p. Choose a non-identity element $a \in G$. Then we will prove that $\langle a \rangle$ is normal in G. If it is not normal, then there exists $b \in G$ such that bab^{-1} is not in $\langle a \rangle$. Therefore, $\langle a \rangle$ and $\left\langle bab^{-1} \right\rangle$ are two distinct subgroups of G. Moreover, their intersection is a subgroup in $\langle a \rangle$, but this means that $\langle a \rangle \cap \left\langle bab^{-1} \right\rangle = \{e\}$.

In particular, every left coset with repsect to $\left\langle bab^{-1} \right\rangle$ can be written as $a^i \left\langle bab^{-1} \right\rangle$ for some $i\mathbb{Z}$.

The element b^{-1} has to belong to a left coset with respect to $\left\langle bab^{-1} \right\rangle$, so there exists $i \in \mathbb{Z}$ such that $b^{-1} = a^i (bab^{-1})^j = a^i b a^j b^{-1}$. Cancelling out b^{-1}, we get $e = a^i b a^j$, but this would imply that $b = a^{-i-j}$, which would cause a contradiction.

Therefore, any subgroup of order p is normal, now we can choose two elements x and y, such that $y \notin \langle x \rangle$. Both $\langle x \rangle$ and $\langle y \rangle$ are normal subgroups which satisfy the conditions in the Definition 14.2: their intersection has to be empty and $< x >, < y >$ generate G. □

Corollary 14.3. Any group of order p^2 for a prime p is Abelian.

We might see an alternative proof of this fact if we will discuss Sylow's theorems.

15 Classification of finite abelian groups

We are very close to achieving one of the main goals of MAT301! Finally, we have (almost) every definition and theorem needed to formulate the classification. In fact, we will prove a **slightly stronger** result, as you will see right now.

Definition 15.1. A group G is called finitely generated if it admits a finite generating set $\{g_1, \dots, g_m\} \subset G$. (every element can be written down as a product of g_i and their inverses.)

Theorem 15.1 (classification of finitely generated Abelian groups)**.** Let G be a **finitely generated Abelian group**. Then there exists a non-negative integer $t \in \mathbb{Z}_{\geq 0}$ and positive numbers $(k_i)_{i=1,\dots,m} \in \mathbb{N}$ (called **invariant factors**), satisfying $k_1 | k_2 | k_3 | \dots | k_m$, such that the following group isomorphism takes place:

$$G \cong \mathbb{Z}^t \times \mathbb{Z}/k_1\mathbb{Z} \times \dots \times \mathbb{Z}/k_m\mathbb{Z}.$$

Moreover, all parameters t and k_i are uniquely defined by the group G itself.

Finally, we can also rewrite

$$G \cong \mathbb{Z}^t \times \prod_i \mathbb{Z}/p_i^{m_i}\mathbb{Z}$$

for some prime numbers p_i and $m_i > 0$, which are also defined uniquely up to a permutation.

Remark. If G is finite, then $t = 0$, $\mathbb{Z}^t = \{0\}$, and we recover the classification of **finite Abelian groups**.

As with many fundamental theorems, this classification does not admit a short and concise proof. However, we will present a more or less intuitive and a memorable argument which also has a benefit of being highly adaptable to more general algebraic structures. This prove does require minimal knowledge of linear algebra, though. We are not going to use Gallian's proof but we will separate the argument into several steps.

Step 1. First of all, let us adopt the additive notation for the remainder of this section.

Definition 15.2. Let G be a finitely generated Abelian group. A set of elements $\{a_1, \dots, a_n\}$ is called a **basis** of G is every element of G can be uniquely written down as $k_1a_1 + \dots + k_na_n$ for some integers k_i.

A finitely generated Abelian group with a basis is called **a free Abelian group**.

First of all, we need to classify all free Abelian groups.

Lemma 15.1. All bases of a free Abelian group G have the same number of elements. In particular, every free Abelian group is isomorphic to $\mathbb{Z}^n$.

Proof. Let $\{e_1, \dots, e_n\}$ and $\{e'_1, \dots, e'_m\}$ be two bases of G. Then

$$(e'_1, \dots, e'_m) = (e_1, \dots, e_n)C$$

for some integer matrix $C \in \mathrm{Mat}_{n\times m}(\mathbb{Z})$. If $n < m$, then the columns of $C = \begin{pmatrix} v_1 & \dots & v_m \end{pmatrix}$ are linearly dependent in $\mathbb{Q}^n$. In other words, there exist integers λ_i such that $\lambda_1 v_1 + \dots \lambda_m v_m = 0$. However, $e'_i = (e_1, \dots, e_n)v_i$ for all $i = 1, \dots, m$, so

$$\lambda_1 e'_1 + \dots \lambda_m e'_m = \lambda_1(e_1, \dots, e_n)v_1 + \dots + \lambda_m(e_1, \dots, e_n)v_m = (e_1, \dots, e_n)(\lambda_1 v_1 + \dots \lambda_m v_m) = 0.$$

If $(e_1, \dots, e_n)$ is a basis of G, then the map $\mathbb{Z}^n \to G$, $(k_i) \mapsto \sum k_i e_i$ is a group isomorphism. □

If $G \cong \mathbb{Z}^n$, we will define its **rank** like this: $\mathrm{rk}(G) = n$.

Step 2. Now let us show that every subgroup of a free group is free. First of all, recall that any subgroup of $\mathbb{Z}$ is of the form $k\mathbb{Z}$ by Euclid's algorithm.

Lemma 15.2. Let $N \subset L$ be a subgroup of a free Abelian group of rank n. Then N is also a free group of rank $\le n$.

Proof. We will argue via induction by n. Base case is trivial.

Suppose that $\{e_1, \dots, e_n\}$ is a basis of L. Then we consider $L_1 = \{e_1, \dots, e_{n-1}\}$ – it is a free subgroup of L. Moreover, the induction assumption allows us to consider $N_1 = L_1 \cap N \subset L_1$, and $L_1 \cap N$ will be a free Abelian group of rank $\le n - 1$. Let $\{f_1, \dots, f_m\}$ be a basis of N_1.

Now let us define $N' = \{k_n : n = k_1e_1 + \dots k_ne_n \in N\}$. This is a subgroup of $\mathbb{Z}$ which has the form $k\mathbb{Z}$. If $k = 0$, then $N_1 = N$ and we are good to go. If not, that we choose f_{m+1} in such a way that $f_{m+1} = k'_1e_1 + \dots + k'_{n-1}e_{n-1} + ke_n$, and then $\{f_1, \dots f_m, f_{m+1}\}$ is the basis of N.

To prove this, we just remember that f_i for $1 \le i \le m$ has no e_n component, so f_{m+1} and f_i are linearly independent.

And if $x = k_1e_1 + \dots + k_ne_n \in N$, then we write

$$x = x - \frac{k_n}{k}f_{m+1} + \frac{k_n}{k}f_{m+1} = \underbrace{\left(k_1 - \frac{k'_1k_n}{k}\right)e_1 + \dots + \left(k_{n-1} - \frac{k'_{n-1}k_n}{k}\right)e_{n-1}}_{\in N_1} + \frac{k_n}{k}f_{m+1},$$

and as the highlighted term is in N_1, we can express it as a linear combination of $\{f_1, \dots, f_m\}$.

□

Step 3. This is the key part of the proof: we need to prove that, given a subgroup of a free Abelian group, we can choose both bases so that they would be "compatible" with each other.

Definition 15.3. The following types of transformations of an integer-valued matrix A are called **integer-valued elementary transformations**, or just **elementary transformations** of A:

1. if v_i, v_j are rows/columns, and $a \in \mathbb{Z}$ then $v_i \mapsto v_i + av_j$
2. any transposition of two rows/columns
3. multiplying a row/column by -1.

A (not necessarily square) matrix $D = (d_{ij}) \in \mathrm{Mat}_{n\times m}(\mathbb{Z})$ is called **diagonal**, if $d_{ij} = 0$ for $i \neq j$, and $d_{ii} = d_i$ for $1 \leq i \leq \min(n, m)$. We will denote $D = \mathrm{diag}(d_1, \dots d_{\min(n,m)})$.

Lemma 15.3. Any integer-valued matrix $C = (c_{ij}) \in \mathrm{Mat}_{n\times m}(\mathbb{Z})$ can be transformed via elementary transformations into a diagonal matrix $\mathrm{diag}(d_1, \dots d_p)$ where $d_i \geq 0$ and $d_1|d_2|\dots|d_p$.

Proof. Let us assume that $C \neq 0$. Once again, we will argue by induction on $n + m$. Base cases are trivial, so let us just start with C itself:

$$C = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1m} \\ c_{21} & c_{22} & \dots & c_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \dots & c_{nm}. \end{pmatrix}$$

The idea is the same as in the Gaussian elimination – the problem is, when dividing integers, we have to deal with remainders. But this is why we can just use the Euclid's algorithm once again!

So, first thing we need to do is to ensure that $c_{11} \neq 0$ by transposing some rows and/or columns. Then we multiply by -1 to ensure that $c_{11} > 0$.

The we concentrate our attention on the first row of C. Because we can add columns to each other (maybe with an integer cofficient), we can implement the Euclid's algorithm to non-zero c_{1j}, turning a pair (c_{11}, c_{1j}) to $(c'_{11}, 0)$. Thus we make sure that at some point all elements of the first row will become zero except for c'_{11}:

$$\begin{pmatrix} c'_{11} & 0 & \dots & 0 \\ c'_{21} & c'_{22} & \dots & c'_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ c'_{n1} & c'_{n2} & \dots & c'_{nm}. \end{pmatrix}$$

As we are allowed to apply row transformations as well, we can arrive at a matrix which looks as follows:

$$\begin{pmatrix} c''_{11} & 0 & \dots & 0 \\ 0 & c''_{22} & \dots & c''_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c''_{n2} & \dots & c''_{nm}. \end{pmatrix}$$

It might seem if we can just apply the induction step to the smaller matrix (c''_{ij}), however, we still have to ensure that $c''_{11} | \gcd(c''_{ij})$. But this does not need to be true! In this case we pick an element c''_{ij} with $i > 1, j > 1$ such that $\gcd(c''_{11}, c''_{ij}) < \min(c''_{11}, c''_{ij})$, and we add the i-th row to the first one, thus reducing the total gcd of the first row:

$$\begin{pmatrix} c''_{11} & -c''_{i2} & \dots & -c''_{im} \\ 0 & c''_{22} & \dots & c''_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c''_{n2} & \dots & c''_{nm}. \end{pmatrix}$$

We repeat until $c''_{11} | \gcd(c''_{ij})$. And only then we pass to the $(n-1) \times (m-1)$ block. □

Example 15.1. Consider the following matrix:

$$C = \begin{pmatrix} 2 & 6 & 2 \\ 2 & 3 & 4 \\ 4 & 2 & 4 \end{pmatrix}.$$

First of all, we apply the Euclid's algrotihm to the first row.

$$\begin{pmatrix} 2 & 6 & 2 \\ 2 & 3 & 4 \\ 4 & 2 & 4 \end{pmatrix} \mapsto \begin{pmatrix} 2 & 0 & 2 \\ 2 & -3 & 4 \\ 4 & -10 & 4 \end{pmatrix} \mapsto \begin{pmatrix} 2 & 0 & 0 \\ 2 & -3 & 2 \\ 4 & -10 & 0 \end{pmatrix}.$$

Then we get rid on entries in the first column:

$$\begin{pmatrix} 2 & 0 & 0 \\ 2 & -3 & 2 \\ 4 & -10 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 2 & 0 & 0 \\ 0 & -3 & 2 \\ 0 & -10 & 0 \end{pmatrix}.$$

However, the entires in the smaller block are not divisible by 2, so we have to make c_{11} even smaller:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -3 & 2 \\ 0 & -10 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 2 & -3 & 2 \\ 0 & -3 & 2 \\ 0 & -10 & 0 \end{pmatrix}.$$

Then we repeat the procedure until we get $c_{11} = 1$.

$$\begin{pmatrix} 2 & -3 & 2 \\ 0 & -3 & 2 \\ 0 & -10 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 2 & -1 & 0 \\ 0 & -3 & 2 \\ 0 & -10 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 & -1 & 0 \\ -3 & -3 & 2 \\ -10 & -10 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ -3 & -6 & 2 \\ -10 & -20 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & -6 & 2 \\ 0 & -20 & 0 \end{pmatrix}.$$

And only now we pass to the block $\begin{pmatrix} -6 & 2 \\ -20 & 0 \end{pmatrix}$:

$$\begin{pmatrix} -6 & 2 \\ -20 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 2 & -6 \\ 0 & -20 \end{pmatrix} \mapsto \begin{pmatrix} 2 & 0 \\ 0 & -20 \end{pmatrix} \mapsto \begin{pmatrix} 2 & 0 \\ 0 & 20 \end{pmatrix}.$$

Lemma 15.4. Let L be a free Abelian group of rank n with a subgroup N of rank $m \leq n$. Then there exists a basis $\{e_1, \dots, e_n\}$ of L and positive integers k_i such that $\{k_1 e_1, \dots, k_m e_m\}$ is a basis of N, and $k_1 | k_2 | \dots | k_m$.

Proof. Lemma 15.2 ensures there exist **some** bases $\{e_i\}$ for L and $\{f_j\}$ for N. Now we consider

$$f_j = c_{1j} e_1 + c_{2j} e_2 + \dots c_{nj} e_n,$$

and we define $C = (c_{ij})$. Any elementary transformation of C corresponds to a valid change of basis in L or N.

- If we replace $e_i \mapsto e_i + a e_1 = e_i'$, then for every j we would have

  $$\begin{aligned} f_j &= c_{1j} e_1 + c_{2j} e_2 + \dots c_{nj} e_n = c_{1j} e_1 + c_{2j} e_2 + \dots c_{nj} e_n + c_{ij} a e_1 - c_{ij} a e_1 = \\ &= (c_{1j} - a e_{ij}) e_1 + \dots + c_{ij} e_i' + \dots c_{nj} e_n. \end{aligned}$$

  This change of basis corresponds to adding the i-th column to the first one with the coefficient a.

- If we replace $f_j \mapsto f_j + a f_1 = f_j'$, then

  $$f_j' = f_j + a f_1 = (c_{1j} + a c_{11}) e_1 + (c_{2j} + a c_{21}) e_2 + \dots (c_{nj} + a c_{n1}) e_n.$$

  This transformation corresponds to adding the first row to the j-th one with the coefficient a.

So, applying Lemma 15.3, we transform C into a diagonal matrix. But if C is diagonal, then we get precisely what we need: $f_j = c_{jj}e_j$ for all j. Then we just choose $k_i = c_{ii}$. □

Step 4. We are almost done, now we are fully prepared to prove the classification.

Lemma 15.5. *G is a finitely generated Abelian group if and only if there exists a surjective homomorphism $\psi : \mathbb{Z}^n \to G$ for some $n > 0$.*

The proof is left as a simple exercise.

Proof of Theorem 15.1. **Existence.** Lemma 15.5 implies that there is a surjective homomorphism $\psi : \mathbb{Z}^n \to G$. The first isomorphism theorem implies that

$$\mathbb{Z}^n/\mathrm{Ker}(\psi) \cong G.$$

The kernel is a subgroup of $\mathbb{Z}^n$, therefore, we can choose a basis $\{e_1, \dots, e_n\}$ in $\mathbb{Z}^n$ such that $\{k_1e_1, \dots, k_me_m\}$ form a basis of $\mathrm{Ker}(\psi)$ for some integers k_i due to Lemma 15.4. Now it is left to apply Theorem 14.6 to

$$\begin{aligned} H_1 &= \langle e_1\mathrm{Ker}(\psi)\rangle \cong \mathbb{Z}/k_1\mathbb{Z}, \\ H_2 &= \langle e_2\mathrm{Ker}(\psi)\rangle \cong \mathbb{Z}/k_2\mathbb{Z}, \\ &\vdots \\ H_m &= \langle e_m\mathrm{Ker}(\psi)\rangle \cong \mathbb{Z}/k_m\mathbb{Z}, \\ H_{m+1} &= \langle e_{m+1}\mathrm{Ker}(\psi)\rangle \cong \mathbb{Z}, \\ &\vdots \\ H_n &= \langle e_n\mathrm{Ker}(\psi)\rangle \cong \mathbb{Z}. \end{aligned}$$

As $\{e_i\}$ form a basis, every element in the quotient can be realized as $(a_1e_1 + \dots a_ne_n)\mathrm{Ker}(\psi)$, and

$$H_1 + \dots + H_k = \{(a_1e_1 + \dots + a_ke_k)\mathrm{Ker}(\psi)\},$$

$$H_{k+1} = \{a_{k+1}e_{k+1}\mathrm{Ker}(\psi)\} \cap (H_1 + \dots + H_k) = \{0\},$$

as e_{k+1} is linearly independent from $e_1, \dots e_k$. So, Theorem 14.6 implies that

$$G \cong H_1 \times \dots \times H_n = \mathbb{Z}/k_1\mathbb{Z} \times \dots \times \mathbb{Z}/k_m\mathbb{Z} \times \mathbb{Z}^{n-m}.$$

Finally, $k_1|k_2|\dots|k_m$, as this follows from Lemma 15.4. Alternatively, we could have noticed that

$$\mathrm{Ker}(\psi) = k_1\mathbb{Z} \times \dots \times k_n\mathbb{Z} \subset \mathbb{Z}^n,$$

and then apply Theorem 5(3).

Uniqueness. To finish the proof, we need to show that the parameters **do not depend** on the choice of the surjection $\mathbb{Z}^n \to G$.

Let $G \cong \mathbb{Z}/k_1\mathbb{Z} \times \dots \times \mathbb{Z}/k_m\mathbb{Z} \times \mathbb{Z}^t$ For this we can make use of the following invariants of an Abelian group:

$$\mathrm{Tor}(G) = \{x \in G | \exists 0 \neq m \in \mathbb{Z} \text{ s.t. } mx = 0\}.$$

Then we can see that $G/\mathrm{Tor}(G) = \mathbb{Z}^t$, and $\mathrm{Tor}(G) = \mathbb{Z}/k_1\mathbb{Z} \times \dots \times \mathbb{Z}/k_m\mathbb{Z}$, so it is uniquely determined by G.

For convenience, let's set $H = \mathrm{Tor}(G)$. Let's define

$$\mathrm{Tor}_p(H) = \{x \in H : p^kx = 0 \text{ for some } k > 0\}.$$

Then we claim

$$H = \prod_p \mathrm{Tor}_p(H), \mathrm{Tor}_p(H) \simeq \mathbb{Z}/p^{l_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{l_i}\mathbb{Z}$$

for some numbers p_{l_t}. If we prove that p^{l_i} are uniquely defined by H, we are good to go. For that we consider $p\mathrm{Tor}_p(H)$: it is is a well-defined subgroup of H. Moreover, we have the isomorphism

$$p\mathrm{Tor}_p(H) = \mathbb{Z}/p^{l_1-1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{l_m-1}\mathbb{Z}.$$

In particular, $\log_p(|\mathrm{Tor}_p(H)|/|p\mathrm{Tor}_p(H)|) = m$. Now we can argue by induction: $p\mathrm{Tor}_p(H)$ is also a smaller finitely generated Abelian group, so the factors p^{l_t} are uniquely defined. But if we know these factors and p, we can define p^{l_t} uniquely. □

15.1 Applications of the classification

Corollary 15.1. A finite abelian group G is cyclic **if and only if** $\exp(G) = |G|$.

In an earlier assignment you proved $\exp((\mathbb{Z}/p\mathbb{Z})^\times) = p-1$. Then the above Corollary immediately implies that $(\mathbb{Z}/p\mathbb{Z})^\times$ is always cyclic for prime p!

Proposition 15.1. Let $n > 1$. Then $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic only for $n = 2, 4, p^k, 2p^k$ where p is an odd prime and $k \geq 1$.

16 Group actions

16.1 Basic definitions and examples

Definition 16.1. Let G be a group and X be a set. Then an **action** of G on X is a map $\varphi : G \times X \to X$ which satisfies the following two conditions:

1. For every $x \in X$ we have $\varphi(e, x) = x$. (identity)
2. For every $g, h \in G$ and $x \in X$ we have

$$\varphi(g, \varphi(h, x)) = \varphi(gh, x). \quad \text{(associativity)}$$

If such a map is defined, we will denote

$$\varphi(g, x) = \varphi_g(x) = g \cdot x = g.x = gx.$$

All of these notations are frequently used in mathematical literature, as all of these notations emphasize that every element $g \in G$ "acts" as a map $X \to X$. The map itself is often omitted if it is clear which action we are talking about at the moment.

If a set X is equipped with **an** action of G, then we will denote $G \curvearrowright X$.

Proposition 16.1. Let X be equipped with an action of G.

1. For every $g \in G$ the map $\varphi_g : X \to X$ is a bijection.
2. Any action φ uniquely defines a homomorphism $\psi : G \to \mathrm{Perm}(X)$. And vice versa, every such homomorphism defines an action of G on X.

Proof.

1. To prove this we just need to prove that the inverse of φ_g is $\varphi_{g^{-1}}$. This can be achieved by using the conditions:

$$\varphi_g \circ \varphi_{g^{-1}}(x) \overset{(2)}{=} \varphi(gg^{-1})(x) = \varphi_e(x) \overset{(1)}{=} x = \varphi(g^{-1}g)(x) = \varphi_{g^{-1}} \circ \varphi_g(x).$$

2. And this follows immediately from the second condition.

□

Definition 16.2. Let X be a set equipped with an action of a group G. Let $x \in X$.

- The **orbit** of x is a set $Gx := \{g.x : g \in G\} \subseteq X$.
- The **stabilizer** of x is a set $\mathrm{Stab}_x = G_x := \{g \in G | g.x = x\} \subseteq G$.

Proposition 16.2. Let X be a set equipped with an action of a group G. Let $x \in X$.

1. The stabilizer of x is a subgroup of G.
2. The set X is a disjoint union of its orbits with respect to G. In other words, we can define the following equivalence relation:

$$x \sim_G y \iff y = gx \quad \text{for some } g \in G.$$

   Then orbits are precisely the equivalence classes with respect to this relation.

Proof.

1. Let us use the 1-step subgroup test. Let $g, h \in G_x$.

$$(gh^{-1}).x = g.(h^{-1}.x) = g.x = x,$$

   as $h.x = x$. Therefore, G_x is a subgroup. It does not need to be normal, though.

2. Let us just show that the relation we just introduced is, indeed, an equivalence relation.

   - $$x \sim_G x \iff x = e.x.$$
   - $$x \sim_G y \iff y = g.x \iff g^{-1}.y = x \iff y \sim_G x.$$
   - $$x \sim_G y, y \sim_G z \iff y = g.x, z = h.y \Rightarrow z = (hg).x \Rightarrow x \sim_G z.$$

   By definition, orbits are the equivalence classes under this relation. And we already know that two equivalence classes either never intersect or they coincide.

□

Before introducing important examples of group actions, we need to define some important types of actions. There are many different adjectives you use to describe an action,but we will only discuss the most frequently used types in these notes.

Definition 16.3. Let X be a set equipped with an action φ of a group G.

- The action is called **faithful**, if the kernel of the respective homomorphism $\varphi : G \to \mathrm{Perm}(X)$ is trivial. Equivalently, for each $x \in X$ there exists an element $g \in G$ such that $g.x \neq x$.
- The action is called **transitive**, if the action admits only one orbit, which coincides with X. Equivalently, for every $x, y \in X$ there exists $g \in G$ such that $g.x = y$.

Also, transitivity can be generalized to n-transitive, where for every two n-tuples $(x_1, \ldots, x_n) \in X^n$ and $(y_1, \ldots, y_n) \in Y^n$ we require the existence of $g \in G$ such that $(g.x_i) = (y_i)$.

Example 16.1.

- One of the most important group actions we are going to consider is a group G acting on itself via left multiplication: $\varphi_l(g, h) = gh$. Group associativity implies that this is a group action. Moreover, it is a transitive and a faithful action. This action is used to prove Cayley's theorem.

- Keep in mind that for a non-abelian group G the right multiplication does not define an action of G on itself.
- Any subgroup of S^n acts on the n-element set $\{1, \dots, n\}$.
- Let G be a subgroup of $\mathrm{Isom}(\mathbb{R}^2)$ (the group of all isometries $\mathbb{R}^2 \to \mathbb{R}^2$). Then G is equipped with the natural action on $\mathbb{R}^2$ via isometries. Such actions are always faithful.
- More generally, every subgroup of $\mathrm{GL}_n(\mathbb{R}^n)$ is equipped with the natural action on $\mathbb{R}^n$ via matrix multiplication. Such actions are always faithful.
- Let us return to abstract groups. Let G be a group. Then we can define the action **via conjugation** of G on itself:
$$g.h = ghg^{-1}.$$
This action is, in general, **not** faithful, nor **transitive** (consider an Abelian G). Nevertheless, this action is still a powerful tool which is used to study non-Abelian groups, and we will use this action to prove **Sylow's theorems** later.
The orbits of this action are called **conjugacy classes**, and for every $g \in G$ its stabilizer is precisely the **centralizer** $C_G(g)$.
- Let $H \leq G$ be a (not necessarily normal) subgroup. At some point we will need to consider the action of G on its set of left cosets G/H with respect to H via left multiplication:
$$g_1.g_2H := (g_1g_2)H.$$
- Finally, let $G \curvearrowright X$ be an action. Then for every $x \in X$ the **restriction** of the action on Gx is still an action, as for every $g \in G$ and $y = h.x$ in Gx we have
$$g.(h.x) = (gh).x \in Gx.$$

16.2 The orbit-stabilizer theorem and the Burnside's lemma

Definition 16.4. Let X, Y be two sets equipped with actions φ_X, φ_Y of a single group G. Then a map $f : X \to Y$ is called G**-equivariant**, if the following diagram commutes:

$$\begin{array}{ccc} X & \xrightarrow{\varphi_X} & X \\ \downarrow f & & \downarrow f \\ Y & \xrightarrow{\varphi_Y} & Y \end{array}$$

commutes. In other words, for every $x \in X$ and $g \in G$ we have

$$f((\varphi_X)_g(x)) = (\varphi_Y)_g(f(x)),$$

or

$$f(g.x) = g.f(x).$$

If f is a bijective map, then we will say that f is **an isomorphism of group actions**.

Theorem 16.1 (orbit-stabilizer theorem)**.** Let G be a group with an action $G \curvearrowright X$, and fix $x \in X$. Then the map $f : Gx \to G/G_x$
$$y \mapsto \{g \in G | gx = y\}$$
is an isomorphism of group actions (via left multiplication) of G.

Proof. The proof will consist of several steps.

1. Let us show that this map is well-defined, that is, we need to show that for every $y \in Gx$ the set $f(y) = \{g \in G | g.x = y\}$ is, indeed, a coset. Suppose that $y = g.x$ for some $g \in G$. Then we claim that $f(y) = gG_x$. We will prove this by explicitly presenting an equivalence chain:

$$g_1 \in \{g \in G | g.x = y\} \iff g_1 x = y \iff g^{-1} g_1 x = x \iff g^{-1} g_1 \in G_x \iff g_1 \in gG_x.$$

2. Then we need to show that f is a bijection. Well, this map is a surjection, because $f^{-1}(gG_x) = g.x \in Gx$. And it is an injection: let $y_1 \neq y_2$ be two elements of Gx. Then $g_1 x = y_1$ and $g_2 x = y_2$. If $g_1 G_x = g_2 G_x$ then $g_2^{-1} g_1 \in G_x$, but then

$$g_2^{-1} g_1 x = g_2^{-1} y_1 = x = g_2^{-1} y_2.$$

   But this means that $y_1 = y_2$, as g_2^{-1} is an injection.

3. Finally, we need to show that this map is G-equivariant. Let $h \in G$ and $y \in Gx$. If $y = g.x$, then

$$f(h.y) = \{g' \in G | g'.x = h.y\},$$
$$h.(f(y)) = h\{g' \in G | g'.x = y\}.$$

   However, we know that $h.y = (hg).x$, so $\{g' \in G | g'.x = h.y\} = (hg)G_x$. Finally,

$$h\{g' \in G | g'.x = y\} = h(gG_x) = (hg)G_x,$$

   and this finishes the proof.

□

Corollary 16.1. Let X be equipped with an action of a finite group G. Then for every $x \in X$ we have

$$|Gx| = \frac{|G|}{|G_x|}. \tag{2}$$

Lemma 16.1 (Burnside's lemma)**.** Let X be a finite set, equipped with an action of a finite group G. For each $g \in G$ let us denote

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

Also, by X/G we will denote the set of orbits w.r.t. the action of G. Then

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g| \tag{3}$$

Proof. Our proof will use a useful trick, called "counting the elements of the same set in two different ways". Define

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

Then

$$|F| = \sum_{(g,x) \in G \times X} 1.$$

There are two different ways to write this as a double sum:

$$|F| = \sum_{g \in G} \sum_{x:(g,x) \in F} 1 = \sum_{x \in X} \sum_{g:(g,x) \in F} 1.$$

Let us deal with the first sum first:

$$\sum_{g \in G} \left(\sum_{x:(g,x) \in F} 1 \right) = \sum_{g \in G} |\{x \in X : g.x = x\}| = \sum_{g \in G} |X^g|.$$

As we can see, we have obtained part of the RHS in (3). Now, let us deal with the second sum:

$$\sum_{x\in X}\left(\sum_{g:(g,x)\in F} 1\right) = \sum_{x\in X} |\{g\in G : g.x = x\}| = \sum_{x\in X} |G_x|.$$

Now we use (2) to get

$$\sum_{x\in X} |G_x| = \sum_{x\in X} \frac{|G|}{Gx} = |G| \sum_{x\in X} \frac{1}{|Gx|}.$$

Now recall that X is a disjoint union $X = Gx_1 \sqcup \cdots \sqcup Gx_j$ of its orbits. In particular, $j = |X/G|$. Therefore,

$$|G| \sum_{x\in X} \frac{1}{|Gx|} = |G| \sum_{i=1}^{|X/G|} \sum_{x\in Gx_i} \frac{1}{|Gx|} = |G| \sum_{i=1}^{|X/G|} \sum_{x\in Gx_i} \frac{1}{|Gx_i|}$$

as $x \in Gx_i$ implies $Gx = Gx_i$. So,

$$|G| \sum_{x\in X} \frac{1}{|Gx|} = |G| \sum_{i=1}^{|X/G|} 1 = |G||X/G|.$$

Therefore,

$$|F| = \sum_{g\in G} |X^g| = |G||X/G|,$$

we finish the proof by dividing both parts by $|G|$. □

17 Sylow theorems

17.1 Preparation

Before stating the Sylow theorems, let us provide some applications of Corollary 16.1 and Lemma 16.1. the following proposition will be given without proof, as it immediately follows from these theorems.

Proposition 17.1. Let G be a finite group. By $\mathrm{Conj}(x)$ let us denote the **conjugacy class** of x. Equivalently, it is the orbit of x w.r.t to the conjugation. Let us denote the **centralizer** of $x \in G$ by $Z(x)$:

$$Z(x) = \{g \in G : gx = xg\}.$$

1. For every $g \in G$ we have
$$|\mathrm{Conj}(g)| = \frac{|G|}{|Z(g)|}. \tag{4}$$
2. Let us denote $\mathrm{Conj}(G)$ the set of conjugacy classes of G. Then
$$|G| = Z(G) + |\mathrm{Conj}(g_1)| + \cdots + |\mathrm{Conj}(g_k)|, \tag{5}$$
where $\mathrm{Conj}(g_k)$ are non-intersecting conjugacy classes which span $G \setminus Z(G)$.

17.2 A little bit of warm-up

Definition 17.1. Let G be a finite group, and $|G| = p^n q$ for some $n > 0$, prime p with $\gcd(p^n, q) = 1$. Then a subgroup of order p^k for $k \le n$ is called a **p-subgroup**. A **maximal** p-subgroup is a p-subgroup of order p^n. Such subgroups are also called Sylow p-subgroups.

Moreover, if $|G| = p^n$, then G itself is called a p-group.

Before stating the main theorems themselves, let us practice using Proposition 17.1.

Lemma 17.1. Any non-trivial p-group has a non-trivial center.

Proof. If $g \notin Z(G)$, then (4) implies that $|Z(g)| < |G|$ and $|\mathrm{Conj}(g)| = p^k$ for some $k > 0$. In particular, $p \,|\, |\mathrm{Conj}(g)|$. However, looking at (5), we see that p divides all terms except for, maybe, $Z(G)$. Therefore, $Z(G)$ also divides p. □

As a corollary, we get the fact which we already observed earlier in the course.

Corollary 17.1. Any group of order p^2 is Abelian.

Proof. Let us denote the group by G. Lemma 17.1 plus Lagrange imply that $|Z(G)| = p$ or $|Z(G)| = p^2$. Let us assume that $|Z(G)| = p$. Then both $Z(G)$ and $G/Z(G)$ are cyclic, as they are of prime order. If aZ is a generator of $G/Z(G)$, then we can see that every element of G can be written as $a^k z$ for $k \in \mathbb{Z}$ and $z \in Z(G)$. However, such elements commute with each other, which contradicts the assumption. □

17.3 The theorems themselves

The warm-up is over, let's get to the main attraction!

Theorem 17.1 (Sylow theorems)**.** Let G be a finite group, and $|G| = p^n q$ for some $n > 0$, prime p with $\gcd(p^n, q) = 1$.

1. There exists a maximal p-subgroup.
2. Every p-subgroup is contained in a maximal p-subgroup. Moreover, all maximal p-subgroups are conjugate to each other.
3. The number of maximal p-subgroups is congruent to 1 modulo p. Moreover, if $H \subset G$ is a maximal p-subgroup, then this number is precisely the index of $N_G(H)$ in G.

Proof.

1. If G is a finite Abelian group, we just use the classification of finite Abelian groups. Just take the direct component corresponding to p as such subgroup.

   Otherwise we consider induction by $|G|$. For small $|G|$ the existence is trivial.

   Now, for an arbitrary G, we consider the conjugacy class partition of G. There are two cases we need to consider:

   - Suppose there is a **non-trivial** conjugacy class $\mathrm{Conj}(g)$ with p **not dividing** its order. However, (4) would imply that $p^n | Z(x)$, as $|\mathrm{Conj}(g)|$ does not contain p in its prime decomposition. However, this just means that we can apply induction hypothesis to $Z(x)$.
   - If all orders of **non-trivial** conjugacy classes are divisible by p, then we use 5 to deduce that $p|Z(G)$. This means that $|Z(G)| = p^{n_0} q_0$ with $(n_0, q_0) = 1$. As $Z(G)$ is an Abelian group, the classification implies that we can choose a subgroup Z_1 of order p^{n_0}, and we can apply the induction hypothesis to G/Z_1. So, suppose that $S_0 \subset G/Z_1$ is a maximal p-subgroup. Denoting the canonical map by $\varphi : G \to G/Z_1$, we define

     $$S = \varphi^{-1}(S_0).$$

     This is a subgroup of order $|S_0||Z_1| = p^{n_0} p^{n-n_0} = p^n$.

2. Let S be a Sylow p-subgroup, and let S_1 be a p-subgroup. Let us consider the action of S_1 on the set of left cosets $G/S = X$ via left multiplication.

   Applying 2, we get

   $$|S_1 x| = \frac{|S_1|}{(S_1)_x}.$$

   Therefore, orders of all non-trivial orbits divide p, but $|X|$ does not divide p, as

   $$|X| = \frac{p^n q}{p^n} = q,$$

and q is not divisible by p. Therefore, there are trivial orbits. But what does it mean for an orbit to be trivial? It means that there exists a coset gS such that $x(gS) = gS$ for any $x \in S_1$. In particular,

$$x(gS) = gS \iff g^{-1}xg \in S \iff S_1 \subseteq gSg^{-1}.$$

So, this implies that any p-group is contained in a **conjugate** to a Sylow p-subgroup, but any conjugate subgroup has the same order, so it is also a Sylow p-subgroup. Finally, if S_1 itself is Sylow, this just yields $S_1 = gSg^{-1}$.

3. Let S be a Sylow p-subgroup. Let us denote the set of all subgroups conjugate to S by $\mathrm{Syl}_p(G)$. Let us consider the action $G \curvearrowright \mathrm{Syl}_p(G)$ via conjugation. This is a transitive action, therefore, (2) implies that

$$|\mathrm{Syl}_p(G)| = \frac{|G|}{|\mathrm{Stab}(S)|}.$$

However, $\mathrm{Stab}(S)$ equals $N_G(S)$ be definition, so

$$|\mathrm{Syl}_p(G)| = \frac{|G|}{|N_G(S)|} = [G : N_G(S)].$$

In particular, the number of Sylow subgroups does **not** divide p.

Let us restrict this action to S. Let's use the same idea as in the previous argument again: $\mathrm{Syl}_p(G)$ can be represented as a disjoint union of its orbits: orders of some of them divide p, and there will be some fixed points. We know that S itself is fixed, so it remains to prove that the fixed point is unique.

Any fixed point $S' \in \mathrm{Syl}_p(G)$ would be a subgroup in $N_G(S)$, but this would mean that S and S' are conjugate in $N_G(S)$ itself, as they would be Sylow in this, potentially smaller subgroup. But $S \triangleleft N_G(S)$, so $S' = S$.

Uniqueness of the fixed point implies that

$$|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}.$$

□

Corollary 17.2. Let G be a finite group, and $|G| = p^n q$ for some $n > 0$, prime p with $\gcd(p^n, q) = 1$.

1. If there is only one Sylow p-subgroup, then it is normal.
2. The number of Sylow p-subgroups divides q.

17.4 Applications of Sylow theorems

Proposition 17.2. Any group of order pq where $p < q$ are two distinct primes such that p does not divide $q - 1$ is Abelian.

Proof. Let N_p and N_q denote the number of Sylow p-subgroups and Sylow q-subgroups, respectively. Then

$$N_p \equiv 1 (\mathrm{mod}\ p), \quad N_q \equiv 1 (\mathrm{mod}\ q).$$

However, from Corollary 17.2 we get

$$N_p | q, \quad N_q | p.$$

So, we have to somehow rule out $N_p = q$ and $N_q = p$. However, $p < q$, so q cannot divide $p - 1$. And p cannot divide $q - 1$ due to the assumption we made in the statement of the proposition.

Therefore, these two facts yield $N_p = N_q = 1$, so there are two normal subgroups of orders p and q. Therefore, G is an internal direct product of $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$. □

Theorem 17.2. There exists an outer automorphism of S_6.

First of all, we need to prove the following lemma.

Lemma 17.2. Let $n > 1$ and suppose that there is a subgroup $H \subset S_n$ which acts on $\{1, \dots, n\}$ transitively. Then H cannot be conjugate to any "naive" $S_{n-1} \subset S_n$, in other words, stabilizers of any single element $x \in \{1, \dots, n\}$.

Proof. Let us denote these subgroups by $G_1, \dots G_n$. It is clear that for any $\sigma \in S_n$ the subgroup $\sigma G_i \sigma^{-1}$ leaves $\sigma(i)$ in place. □

Now we can proceed with the proof.

Proof. We start the proof by looking at the set $\mathrm{Syl}_5(S_5) = X$ of Sylow 5-subgroups of S_5. These are precisely the cyclic subgroups generated by 5-cycles. We can find $|X|$ by hand, or we could use the Corollary, which says that

$$|X| \equiv 1 (\mathrm{mod}\ 5), |X| \,|\, 24.$$

This implies $|X| = 6$. As we already saw in the proof of Sylow theorems, S_5 acts on $\mathrm{Syl}_5(S_5)$ via conjugation. This action defines a homomorphism $S_5 \to S_6$. This is a **transitive action** due to all Sylow subgroups being conjugate to each other. Assuming that we know the structure of normal subgroups of S_5, we can conclude that the kernel of this homomorphism is either $\{e\}$, A_5, or S_5. But we know that the image at least contains a 5-group, so the kernel is too small to be A_5 or S_5. Therefore, this homomorphism is injective.

Let us denote the image by H. We don't know if H is normal (it's not), but we can still consider the action of S_6 on S_6/H via left multiplications. Denote the respective mapping by

$$f : S_6 \cong \mathrm{Perm}(\mathrm{Syl}_5(S_5)) \to \mathrm{Perm}(S_6/H).$$

Once again, we will identify the codomain with S_6 as well.

Let $S_5 \cong H' \subset \mathrm{Perm}(S_6/H)$ be the subgroup which fixes the element corresponding to the coset H. Then $f(H) = H'$. Once again, a similar argument shows that $\mathrm{Ker}(f) = \{e\}$.

However, f can't be an inner automorphism, as the naive subgroup $H' \cong S_5 \subset S_6 \cong \mathrm{Perm}(S_6/H)$ cannot be conjugate to $S_5 \cong H \subset \mathrm{Perm}(\mathrm{Syl}_5(S_5))$ due to Lemma 17.2. □

Remark. A "fun" exercise is to compute these actions explicitly and find $f((1\,2))$. I wouldn't hold it against you if you use some CAS that allows you to deal with permutation groups.

Remark. It is known that there are no outer automorphisms of S_n for $n \neq 2, 6$. The same idea for other n fails: first of all, we need $n - 1$ to be prime, and we want to have exactly n Sylow $(n-1)$-subgroups. And, as it turns out, if p is prime, there are $(p-2)!$ Sylow p-subgroups in S_p! A bit too many for $n > 7$...