Algebraic Structures 1

(notes for course taught at HUJI, Fall 2022)

(UNPOLISHED DRAFT)

Alexander Yom Din

June 21, 2022

Contents

1 Preface

I tried to include material, and also to order the material, as in the Hebrew book "Alegbraic Structures" by de Shalit, Lubozky and Puder (as it is a book often-times used for this course at the Hebrew university). But there are some changes.

2 The very basic notions of group theory

2.1 Isomorphisms of mathematical objects

Common objects in mathematics are **sets with extra structure**. We don't want to formalize this here, but rather give some examples:

1. A **field** is a set K with the extra structure of two operations $+ : K \times K \to K$ and $\cdot : K \times K \to K$ satisfying various conditions.

2. Given a field K, a **vector space over** K is a set V with the extra structure of two operations $+ : V \times V \to V$ and $\cdot : K \times V \to V$ satisfying various conditions.

3. A **real inner product space** is a $\mathbb{R}$-vector space V with the additional extra structure of a positive definite symmetric $\mathbb{R}$-bilinear pairing $\langle -, - \rangle : V \times V \to \mathbb{R}$.

4. A **metric space** is a set X with the extra structure of a map $d : X \times X \to \mathbb{R}_{\geq 0}$ satisfying, for all $x_1, x_2, x_3 \in X$: (1) $d(x_1, x_3) \leq d(x_1, x_2) + d(x_2, x_3)$, (2) $d(x_1, x_2) = 0 \iff x_1 = x_2$, (3) $d(x_1, x_2) = d(x_2, x_1)$. Concrete examples can be gotten as follows. Given a subset $X \subset \mathbb{R}^n$, it has naturally the structure of a metric space by considering the distance function $d(x_1, x_2) := ||x_2 - x_1||$.

Given sets X and Y with extra structure of the same kind, we can usually talk about **isomorphism** between them - a bijection $\phi : X \to Y$ which preserves the extra structure. One can think of an isomorphism as exhibiting how the two objects are "two instances of the same idea". In the examples above:

1. Given fields K and L, an **isomorphism of fields** from K to L is a bijection $\phi : K \to L$ such that $\phi(a+b) = \phi(a)+\phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in K$.

2. Given a field K and vector spaces V and W over K, an **isomorphism of K-vector spaces** from V to W is a bijection $\phi : V \to W$ such that $\phi(v_1 + v_2) = \phi(v_1) + \phi(v_2)$ for all $v_1, v_2 \in V$ and $\phi(cv) = c\phi(v)$ for all $v \in V$ and $c \in K$.

3. Given real inner product spaces V and W, an **isomorphism of real inner product spaces** from V to W is a bijection $\phi : V \to W$ which is an isomorphism of $\mathbb{R}$-vector spaces and, additionally, such that $\langle \phi(v_1), \phi(v_2) \rangle = \langle v_1, v_2 \rangle$ for all $v_1, v_2 \in V$.

4. Given metric spaces X and Y, an **isomorphism of metric spaces** from X to Y is a bijection $\phi : X \to Y$ such that $d(\phi(x_1), \phi(x_2)) = d(x_1, x_2)$ for all $x_1, x_2 \in X$.

Notice that we, as a rule, have the following features of isomorphisms: The identity map is an isomorphism from an object to itself, the composition of isomorphisms is an isomorphism, and the inverse of an isomorphism is an isomorphism.

2.2 Automorphisms ("symmetries") of mathematical objects

Given an object, an isomorphism from it to itself is usually called an **automorphism**, we will also call it a **symmetry** of that object. We can think of it as a "reversible process of self-identification". A bit confusingly perhaps, we can think of it as exhibiting how an object is the instance of an idea in two different[1] ways.

Definition 2.1. Let X be a set. We denote by $S(X)$ the set of bijections from X to itself.

Thus, given a set X with extra structure, the set of automorphisms of X is a subset of $S(X)$.

Example 2.2. *Let us abbreviate*

$$e(q) := \begin{pmatrix} \cos(2\pi q) \\ \sin(2\pi q) \end{pmatrix} \in \mathbb{R}^2$$

(i.e. $e(q)$ is the vector of length 1 forming an angle of $2\pi q$ radians with the positive x-axis). Fix $n \in \mathbb{Z}_{\geq 3}$ and consider

$$X_n := \{e(m/n) \ : \ m \in \mathbb{Z}, \ 0 \leq m < n-1\} \subset \mathbb{R}^2.$$

Let us denote by $D_n \subset S(X_n)$ the set of automorphisms of X_n as a metric space. It turns out that $|D_n| = 2n$. Namely, D_n consists of the following elements:

[1] That is, different unless the automorphism is the identity automorphism.

- *Given $k \in \mathbb{Z}$, $0 \leq k < n$, the rotation by $2\pi\frac{k}{n}$, provides an element in D_n.*
- *Given $k \in \mathbb{Z}$, $0 \leq k < n$, the reflection in the axis spanned by $e(k/n)$ if n is odd and by $e(k/2n)$ if n is even, provides an element in D_n.*

2.3 Forgetting what the extra structure was: Subgroups

Let X be a set with extra structure, and let $H \subset S(X)$ be the subset of automorphisms of X. What properties of H we can write down, without knowing what the extra structure in question is?

Definition 2.3. Let X be a set. A subset $H \subset S(X)$ is called a **subgroup** if the following are satisfied:

1. $\mathrm{id}_X \in H$.
2. Given $g_1, g_2 \in H$ we have $g_1 \circ g_2 \in H$.
3. Given $g \in H$ we have $g^{-1} \in H$.

A very bold step is the following reversal: We can, in some sense, think of the extra structure on X as the thing which is preserved by the elements in H (without knowing what it "really" is)[2].

Example 2.4. *We can consider the subgroup $H \subset S(\mathbb{R}^2)$ consisting of $\mathbb{R}$-linear automorphisms with positive determinant (check that this is indeed a subgroup!). It describes the extra structure of orientation on $\mathbb{R}^2$.*

The idea is that notions that survive under the symmetries are "correct", do not depend on the arbitrariness of our current description. For example, if we consider $\mathbb{R}^2$ as an $\mathbb{R}$-vector space, the property of a vector having one of its coordinates equal to 0 is "not correct", because after applying an automorphism (of $\mathbb{R}$-vector spaces) of $\mathbb{R}^2$ this can change. In contrast, the property of a vector of not being the zero vector is "correct", it is preserved under automorphisms of $\mathbb{R}$-vector spaces. Similarly, the property of a subset of $\mathbb{R}^2$ of being an ellipse is "correct" while the property of a subset of $\mathbb{R}^2$ of being a circle is "not correct". However, if we now consider $\mathbb{R}^2$ not only as an $\mathbb{R}$-vector space but also as equipped with the standard inner product, automorphisms become orthogonal $\mathbb{R}$-linear bijective maps $\mathbb{R}^2 \to \mathbb{R}^2$, and the property of a subset of $\mathbb{R}^2$ of being a circle is now "correct". A vague summary is that a pair (X, H) where X is a set and $H \subset S(X)$ is a subgroup describes a "reality", or that H describes a "geometry" in X.

[2] As far as I understand, this is very much related to the "Erlangen program" of Felix Klein, from 1872.

2.4 Forgetting what the set was: Groups

Given a set X with extra structure, we considered the subset $H \subset S(X)$ of its symmetries. We formulated what is still possible to say generally about the subset $H \subset S(X)$ if we "forget" what the extra structure is (that it is a subgroup). Now one has a much more radical turn - we want to ask what is H if we forget about X itself! Then we can't anymore think of H as a subset of $S(X)$, since we don't know what is X. In particular, we can't anymore freely talk about composition of elements in H (which was the main operation we used). To overcome this, one comes to the idea of book-keeping the result of composition, forgetting about the process which led to the result. We then approach the main definition of this course[3]:

Definition 2.5. A **group** is a pair $(G, \star)$ consisting of a set G and a function $\star : G \times G \to G$ (it is customary to write $g_1 \star g_2$ instead of $\star(g_1, g_2)$), such that the following properties are satisfied:

1. Let $g_1, g_2, g_2 \in G$. We have[4] $g_1 \star (g_2 \star g_3) = (g_1 \star g_2) \star g_3$.
2. There exists an element $1_G \in G$ such that for every $g \in G$ we have $1_G \star g = g$ and $g \star 1_G = g$. The element 1_G is called the **identity element of** G.

   (such an element 1_G is unique, if exists - indeed given another element $1'_G \in G$ with the same property, we obtain $1_G = 1_G \star 1'_G = 1'_G$).
3. Let $g \in G$. There exists an element $g^{-1} \in G$ such that $g \star g^{-1} = e$ and $g^{-1} \star g = 1_G$. The element g^{-1} is called the **inverse to** g **in** G.

   (such an element g^{-1} is unique, if exists - indeed given another element $(g^{-1})' \in G$ with the same property, we obtain $g^{-1} = g^{-1} \star 1_G = g^{-1} \star (g \star (g^{-1})') = (g^{-1} \star g) \star (g^{-1})' = 1_G \star (g^{-1})' = (g^{-1})'$).

Exercise 2.1. *Let $(G, \star)$ be a group. We have:*

1. *Given $a, b \in G$ there exists a unique $x \in G$ such that $a \star x = b$, and a unique $y \in G$ such that $y \star a = b$. In other words, given $a \in G$ the map $G \to G$ given by $x \mapsto a \star x$ is bijective, and the map $G \to G$ given by $x \mapsto x \star a$ is bijective.*
2. *Given $a, b \in G$ we have $(a \star b)^{-1} = b^{-1} \star a^{-1}$.*

Remark 2.6. Eventually one abbreviates notation as follows (usually this does not cause confusion). We will write 1 instead of 1_G. We will write $g_1 g_2$, or $g_1 \cdot g_2$, instead of $g_1 \star g_2$. The notation $\star$ itself will be eliminated, or kept implicit, so that we speak of a group G (in the same way as we speak of a vector space V, but of course formally it is a triple $(V, +, \cdot)$ etc.).

[3] Is it correct, that the first appearance of the abstract concept of a group was in an 1882 paper by Dyck?

[4] In the usual functional-theoretic notation one would write this $\star(g_1, \star(g_2, g_3)) = \star(\star(g_1, g_2), g_3)$.

Remark 2.7. The cardinality $|G|$ is usually called the **order** of the group G, especially when G is finite.

Example 2.8. *Let X be a set. Then $(S(X), \circ)$ is a group (here $\circ : S(X) \times S(X) \to S(X)$ is the composition of maps). In line with Remark 2.6, we write $S(X)$ instead of $(S(X), \circ)$, and given $g_1, g_2 \in S(X)$ we sometimes write $g_1 \circ g_2$ simply $g_1 g_2$, or $g_1 \cdot g_2$. Especially, one writes $S_n := S(\{1, 2, \ldots, n\})$, this is called the **symmetric group on** n **elements**, or the **permutation group on** n **elements**.*

Definition 2.3 naturally generalizes:

Definition 2.9. Let G be a group. A subset $H \subset G$ is called a **subgroup (of G)** if the following conditions are satisfied:

1. Let $g_1, g_2 \in H$. Then $g_1 g_2 \in H$.
2. Let $g \in H$. Then $g^{-1} \in H$.
3. We have $1_G \in H$.

Notice that a subgroup $H \subset G$ can (and always will) be considered as a group itself, restricting the group operation $G \times G \to G$ to a group operation $H \times H \to H$.

Example 2.10. *We obtain examples of groups as subgroups of groups of the form $S(X)$, those preserving some extra structure, as discussed above. Given a vector space V over a field k, we denote by $\mathrm{GL}_k(V)$ the group of automorphisms of V as a k-vector space (the **general linear group**). We denote by $\mathrm{SL}_k(V)$ the group of automorphisms of V as a k-vector space which have determinant 1 (the **special linear group**). We have the group D_n of Example 2.2, called the **dihedral group**. Recall, that the order of D_n is $2n$.*

A very interesting feature of the abstraction of the concept of a group is that it applies to some basic and natural mathematical structures of which we don't think a-priori as collections of symmetries:

Example 2.11. *Let k be a field. There are two standard groups associated to k. One is the **additive group**, which as a set is k and in which the group operation is addition in k. The other is the **multiplicative group**, which as a set is $k^\times := k \smallsetminus \{0\}$ and in which the group operation is multiplication in k.*

Example 2.12. *Let k be a field and let V be a vector space over k. Then V, together with the operation of addition it has as a vector space, is a group.*

Example 2.13. *The set $\mathbb{Z}$ of integers together with the operation of addition is a group.*

Definition 2.14. A group G is called **abelian**, or **commutative**, if for all $g_1, g_2 \in G$ one has $g_1 g_2 = g_2 g_1$.

Notice that the groups in Example 2.11, Example 2.12 and Example 2.13 are abelian.

Remark 2.15. Often, given an abelian group A we use the notation $a_1 + a_2$ for the group operation in A. We use the notation 0_A, or 0, for the identity element in A. We use the notation $-a$ for the inverse to a in A. This is called **additive notation**, as opposed to the **multiplicative notation** of above. But, we don't always use additive notation when dealing with an abelian group. For example, in the example of the multiplicative group of a field above, one always uses multiplicative notation.

Recall the following definition and notation:

Definition 2.16. Given $m, n \in \mathbb{Z}$, we say that m **divides** n, or n is **divisible by** m, if there exists $q \in \mathbb{Z}$ such that $n = qm$. We write in such a case $m|n$.

Remark 2.17. Let us do a refresher on equivalence relations. A **relation** R on a set X is a subset $R \subset X \times X$. One then usually has the following notation: Given $x, y \in X$, one writes xRy if $(x, y) \in R$ (and one writes $x \not R y$ if $(x, y) \notin R$). A relation $\sim$ on a set X is called an **equivalence relation** if the following conditions are satisfied:

1. Given $x \in X$ we have $x \sim x$.
2. Given $x, y \in X$, if $x \sim y$ then $y \sim x$.
3. Given $x, y, z \in X$, if $x \sim y$ and $y \sim z$ then $x \sim z$.

Let $\sim$ be an equivalence relation on a set X. Given $x \in X$, let us denote $E_x^{\sim} := \{y \in X \mid x \sim y\}$. One checks that given $x, y \in X$, if $x \sim y$ then $E_x^{\sim} = E_y^{\sim}$, while if $x \not\sim y$ then $E_x^{\sim} \cap E_y^{\sim} = \emptyset$. A subset $E \subset X$ is called an **equivalence class** with respect to the equivalence relation $\sim$ if $E = E_x^{\sim}$ for some $x \in X$. Recall that a **partition** of a set X is a a set $\mathcal{S}$ of subsets of X, such that for every $x \in X$ there is precisely one $E \in \mathcal{S}$ such that $x \in E$. Notice then that our equivalence relation $\sim$ yields a partition of X - the set of equivalence classes with respect to the equivalence relation $\sim$ is a partition of X. We denote by $X/\sim$ the set of equivalence classes with respect to the equivalence relation $\sim$, and call it the **quotient set** (of X by the equivalence relation $\sim$). We have a **"canonical projection"**, or **"quotient map"** map $\pi : E \to E/\sim$ given by sending x to $E_x^{\sim}$. This map is surjective. For $x, y \in X$, one has $\pi(x) = \pi(y)$ if and only if $x \sim y$. For $\xi \in E/\sim$ and $x \in X$, if $x \in \pi^{-1}(\xi)$ then $\pi^{-1}(\xi) = E_x^{\sim}$.

Example 2.18. *Let $n \in \mathbb{Z}_{\geq 1}$. We will define an abelian group $\mathbb{Z}_n$; we use additive notation. Let us define an equivalence relation $\equiv_n$ on $\mathbb{Z}$, by writing $m_1 \equiv_n m_2$ if $n|m_2 - m_1$. We let $\mathbb{Z}_n$ be the set of equivalence classes. Let us denote by $[-]_n : \mathbb{Z} \to \mathbb{Z}_n$ the corresponding surjective quotient map. To define the addition, given $\mu_1, \mu_2 \in \mathbb{Z}_n$ let us choose $m_1, m_2 \in \mathbb{Z}$ such that $\mu_1 = [m_1]_n$ and $\mu_2 = [m_2]_n$, and define $\mu_1 + \mu_2 := [m_1 + m_2]_n$. As an exercise (it is important to do it!) check that this definition does not depend on the choices. As a further exercise, this provides $\mathbb{Z}_n$ with the structure of a (commutative) group. We call $\mathbb{Z}_n$ the* ***group of integers modulo*** *n.*

Example 2.19. *The group $\mathbb{Z}_{12}$ is often called the* ***clock arithmetic*** *group. We have, for example $[11]_n + [3]_n = [14]_n = [2]_n$, and we can imagine this calculation on a clock (I will illustrate in person).*

2.5 From old groups to new - the example of a product of groups

One of the powers of the abstraction of the concept of a group is that now we can produce "industrially" new groups of old groups (without the need to care what are they symmetries of). Let us illustrate this on a simple example.

Definition 2.20. Let G and H be groups. The **product group** $G \times H$ is defined as follows. As a set, it is the Cartesian product $G \times H$ (consisting of ordered pairs (g, h), where $g \in G$ and $h \in h$). The group operation is given by: $(g_1, h_1)(g_2, h_2) := (g_1 g_2, h_1 h_2)$.

Exercise 2.2. *Check that the thus-defined operation indeed satisfies all the axioms, and gives $G \times H$ the structure of a group.*

2.6 Homomorphisms of groups

Definition 2.21. Let G and H be groups. A **homomorphism** from G to H is a map $\phi : G \to H$ satisfying $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$.

Exercise 2.3. *Let G and H be groups and let $\phi : G \to H$ be a group homomorphism. Then $\phi(1_G) = 1_H$ and $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$.*

Example 2.22. *Let $n \in \mathbb{Z}_{\geq 1}$. We have a homomorphism of groups $\mathbb{Z} \to \mathbb{Z}_n$ given by sending m to $[m]_n$.*

Example 2.23. *Let V be a finite-dimensional vector space over a field k. We have a homomorphism $\det : \mathrm{GL}_k(V) \to k^\times$ given by sending a k-linear automorphism of V to its determinant.*

Example 2.24. *Let G be a group and let $H \subset G$ be a subgroup. Then the tautological inclusion map $i : H \to G$ is a group homomorphism.*

Exercise 2.4. *Let G , H and K be groups. Let $\phi : G \to H$ be a group homomorphism and let $\psi : H \to K$ be a group homomorphism. Then $\psi \circ \phi : G \to K$ is a group homomorphism.*

Remark 2.25. We will discuss group homomorphisms much more extensively later on.

2.7 Group actions

We now want to reconcile the abstract concept of a group, to which we arrived, with the concrete concept of a subgroup of symmetries, from which we started.

Definition 2.26. Let G be a group and X a set. An (left) **action** of G on X is a group homomorphism $\rho : G \to S(X)$.

Remark 2.27. It might seem that one would like the homomorphism ρ to be injective, but the flexibility of not requiring that turns out to be "correct".

Example 2.28. *Let X be a set and let $H \subset S(X)$ be a subgroup. Then the tautological inclusion homomorphism $H \to S(X)$ gives an action of H on X. In other words, our general definition generalizes the concrete situation we had in the beginning.*

Remark 2.29. We will discuss group actions much more extensively later on.

2.8 Isomorphism of groups

Notice that a group is a set with extra structure. Thus we can be interested in isomorphism of groups.

Definition 2.30. Let G and H be groups. An **isomorphism** of G and H (or from G to H) is a bijection $\phi : G \to H$ which satisfies the following condition. Let $g_1, g_2 \in G$. We have $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$. In other words, an isomorphism is a bijective homomorphism.

Exercise 2.5. *Let G, H and K be groups.*

1. *Show that the identity map $\mathrm{id}_G : G \to G$ is an isomorphism of groups.*
2. *Let $\phi : G \to H$ and $\psi : H \to K$ be isomorphism of groups. Show that $\psi \circ \phi$ is an isomorphism of groups.*
3. *Let $\phi : G \to H$ be an isomorphism of groups. Show that the inverse map $\phi^{-1} : H \to G$ is an isomorphism of groups.*

Definition 2.31. Let G and H be groups. One says that G is **isomorphic** to H if there exists an isomorphism from G to H. If G is isomorphic to H, one often[5] writes $G \cong H$.

Exercise 2.6. *Let G, H and K be groups.*

1. *Show that G is isomorphic to G.*
2. *Show that if G is isomorphic to H then H is isomorphic to G.*
3. *Show that if G is isomorphic to H and H is isomorphic to K then G is isomorphic to K.*

Example 2.32. *A "boring", or straight-forward, example is as follows. Let X and Y be sets and let $\psi : X \to Y$ be a bijection. Then we can construct an isomorphism of groups $\phi : S(X) \to S(Y)$ as follows. We set $\phi(\sigma)(y) := \psi(\sigma(\psi^{-1}(y)))$.*

[5] Although some people prefer to write $G \cong H$ only if there is a canonical isomorphism from G to H at hand.

Example 2.33. *Let k be a field and let $n \in \mathbb{Z}_{\geq 0}$. Denote by $\mathrm{GL}_n(k)$ the following group. As a set, $\mathrm{GL}_n(k)$ is the set of invertible matrices in $\mathrm{M}_n(k)$ (the set of $n \times n$-matrices over the field k). The group operation is multiplication of matrices. Check, as an exercise, that this is indeed a group. Now, let V be an n-dimensional vector space over k. Let $e_1, \ldots, e_n$ be a basis for V. We then obtain an isomorphism $\phi : \mathrm{GL}_k(V) \to \mathrm{GL}_n(k)$ as follows. Given $g \in \mathrm{GL}_k(V)$, there exists a unique $A = (A_{ij}) \in \mathrm{GL}_n(k)$ such that $ge_i = \sum_j A_{ji} e_j$ for all i. We then let $\phi(g)$ be this A.*

Example 2.34. *Let us show that the groups S_3 and $\mathrm{GL}_2(\mathbb{F}_2)$ are isomorphic. Here $\mathbb{F}_2$ denotes the field with two elements. First, let V be a two-dimensional $\mathbb{F}_2$-vector space. By choosing a basis of V we obtain an isomorphism of $\mathrm{GL}_2(\mathbb{F}_2)$ with $\mathrm{GL}_{\mathbb{F}_2}(V)$. Let us denote $X := V \setminus \{0\}$. By choosing a bijection between $\{1, 2, 3\}$ and X we obtain an isomorphism of S_3 and $S(X)$. Therefore, it is enough to establish an isomorphism of $S(X)$ and $\mathrm{GL}_{\mathbb{F}_2}(V)$. We construct a map $\phi : \mathrm{GL}_{\mathbb{F}_2}(V) \to S(X)$ by restricting $g \in \mathrm{GL}_{\mathbb{F}_2}(V)$, which is a bijection $V \to V$, to a bijection $X \to X$ (since 0 maps to 0 under g). It is easy to see that ϕ is injective and that ϕ satisfies $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in \mathrm{GL}_{\mathbb{F}_2}(V)$. It is left to see that ϕ is surjective. Since ϕ is injective, it is enough to see that $|\mathrm{GL}_{\mathbb{F}_2}(V)| = |S(X)|$. Both cardinalities are easily seen to be equal to 6.*

Example 2.35. *The groups $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are not isomorphic. Indeed, using multiplicative notation, notice that the latter group G has the property that every $g \in G$ satisfies $gg = 1_G$. While for the former group G there exists $g \in G$ such that $gg \neq 1_G$. Understand why this shows that these groups can not be isomorphic.*

Somewhat self-referentially, we have the group of symmetries of a group:

Definition 2.36. Let G be a group. We denote by $\mathrm{Aut}(G)$ the set of automorphisms of G. Composition gives it a group structure. It is called the **automorphism group of** G.

2.9 The powers of an element in a group

Let G be a group. Given $g \in G$ and $n \in \mathbb{Z}$ we define $g^n \in G$ as follows. For $n \in \mathbb{Z}_{\geq 1}$ we define g^n inductively: We define $g^1 := g$ and $g^{n+1} := gg^n$. Next, we define $g^0 := 1_G$. Finally, if $n \in \mathbb{Z}_{\leq -1}$ we define $g^n := (g^{-1})^{-n}$. Notice that g^{-1} now has seemingly two interpretations, but they coincide, so everything is fine. One can see that the following holds:

Claim 2.37. *Let G be a group. We have:*

1. *Let $g \in G$ and let $n, m \in \mathbb{Z}$. We have $g^{n+m} = g^n g^m$.*
2. *Let $g \in G$ and let $n, m \in \mathbb{Z}$. We have $(g^n)^m = g^{nm}$.*
3. *Suppose that G is abelian. Let $g, h \in G$ and let $n \in \mathbb{Z}$. Then $(gh)^n = g^n h^n$.*

Exercise 2.7. *Show that the last property in the claim does not necessarily hold if G is not abelian.*

Remark 2.38. Let A be an abelian group, and use additive notation. Then given $a \in A$ and $n \in \mathbb{Z}$ one write na instead of what we denoted generally a^n.

Remark 2.39. Given $m, k \in \mathbb{Z}$, notice that the two possible interpretations of $mk \in \mathbb{Z}$ - one as multiplication of integers and one as the m-th power of k in the group of integers with the operation of addition - coincide. As regarding the group $\mathbb{Z}_n$, we have $m[k]_n = [mk]_n$ for all $m, k \in \mathbb{Z}$.

Exercise 2.8. *Let H and G be groups and let $\phi : H \to G$ be a group homomorphism. Show (using induction) that $\phi(h^n) = \phi(h)^n$ for $h \in H$ and $n \in \mathbb{Z}$.*

Remark 2.40. A particular case of Exercise 2.8 is when we are given a group G and a subgroup $H \subset G$. To prevent confusion, let us denote by $\text{power}(G, g, n)$ the n-th power of g in the group G. Then we get that, for $h \in H$ and $n \in \mathbb{Z}$, we have $\text{power}(G, h, n) \in H$ and in fact $\text{power}(G, h, n) = \text{power}(H, h, n)$. Thus, in particular, there is no ambiguity in such a setting when using our more ambiguous notation for powers (the notation g^n in which we don't specify in which group we take the power).

2.10 Basic constructions of subgroups

Lemma 2.41. *Let G be a group.*

1. *Let $H_1, H_2 \subset G$ be subgroups. Then $H_1 \cap H_2 \subset G$ is a subgroup.*
2. *More generally, let $(H_i)_{i \in I}$ be a family of subgroups of G. Then $\cap_{i \in I} H_i$ is a subgroup of G.*

Proof. Left as an exercise. □

Lemma-Definition 2.42. *Let G be a group. Let $S \subset G$ be a subset. There exists a unique subgroup $H \subset G$ with the following properties:*

1. *$S \subset H$.*
2. *Let $K \subset G$ be a subgroup such that $S \subset K$. Then $H \subset K$.*

*We call this H **the subgroup of** G **generated by** S, and we denote it by $\langle S \rangle$. Given $g \in G$, we also abbreviate $\langle g \rangle := \langle \{g\} \rangle$, and more generally $\langle g_1, \ldots, g_n \rangle := \langle \{g_1, \ldots, g_n\} \rangle$.*

Proof. Let us consider the set $\mathcal{F}$ of all subgroups K in G which contain S. Let us consider then the intersection of them all

$$H := \bigcap_{K \in \mathcal{F}} K$$

(which is a subgroup of G by Lemma 2.41). We claim that this H is as desired - we leave it as an easy exercise. □

Lemma 2.43. *Let G be a group. Let $g \in G$. Then $\langle g \rangle = \{g^n \ : \ n \in \mathbb{Z}\}$.*

Proof. It is immediate to check that $\{g^n \ : \ n \in \mathbb{Z}\}$ is a subgroup of G, it contains g, and by Remark 2.40 it is contained in any subgroup of G which contains g. Hence it is equal to $\langle g \rangle$ by the definition of $\langle g \rangle$. □

Exercise 2.9. *Given a group G and a subset $S \subset G$, let us provide another description of $\langle S \rangle$. Namely, consider the subset $H \subset G$ consisting of elements $g \in G$ for which we can find $r \in \mathbb{Z}_{\geq 0}$ and $(g_1, \ldots, g_r) \in G^r$ such that for each $1 \leq i \leq r$ we have either $g_i \in S$ or $g_i^{-1} \in S$, and $g = g_1 \cdot g_2 \ldots \cdot g_r$. In other words, H is the subset of G consisting of elements which can be written as a product of elements in S or their inverses. We allow $r = 0$, corresponding to taking the empty product of elements in G, which is equal to the identity element of G. Show that in fact $H = \langle S \rangle$.*

Lemma 2.44. *Let A be an abelian group, and use additive notation in it. Let $B, C \subset A$ be two subgroups. Then*

$$\langle B \cup C \rangle = B + C := \{b + c \ : \ b \in B, c \in C\}.$$

In particular, $\langle b, c \rangle = \langle b \rangle + \langle c \rangle$ for $b, c \in A$.

Proof. The proof of the lemma is left as an exercise: Check that $B + C$ is a subgroup of A, that it contains $B \cup C$, and that every subgroup of A which contains $B \cup C$ also contains $B + C$. □

2.11 Subgroups of the group of integers, the lcm and gcd

We will now discuss subgroups of $\mathbb{Z}$. Notice that, given $n \in \mathbb{Z}$, the subgroup $\langle n \rangle$ of $\mathbb{Z}$ consists of integers which are divisible by n (I will draw how these look like in person).

Remark 2.45. For the subgroup $\langle n \rangle$ of $\mathbb{Z}$, one also uses the notation $n\mathbb{Z}$.

Theorem 2.46. *Let us consider the group $\mathbb{Z}$.*

1. *Given $n_1, n_2 \in \mathbb{Z}_{\geq 0}$, if $n_1 \neq n_2$ then $\langle n_1 \rangle \neq \langle n_2 \rangle$.*
2. *Every subgroup of $\mathbb{Z}$ is equal to $\langle n \rangle$ for some $n \in \mathbb{Z}_{\geq 0}$. More precisely, if $A \cap \mathbb{Z}_{\geq 1}$ is empty then $A = \langle 0 \rangle$. Otherwise, denoting by n the smallest element[6] in $A \cap \mathbb{Z}_{\geq 1}$, we have $A = \langle n \rangle$.*

Proof.

1. Suppose, without loss of generality, that $n_1 < n_2$. If $n_1 = 0$, then $\langle n_1 \rangle = \{0\}$ while $\langle n_2 \rangle$ contains $n_2 \neq 0$, and therefore we certainly have $\langle n_1 \rangle \neq \langle n_2 \rangle$. So let us assume that $n_1 \neq 0$. We claim that $n_1 \notin \langle n_2 \rangle$. Since $n_1 \in \langle n_1 \rangle$, this will then show that $\langle n_1 \rangle \neq \langle n_2 \rangle$, as desired. To that end,

[6] Such an element exists by a basic principle, equivalent to the principle of mathematical induction.

let us see what $n_1 \in \langle n_2 \rangle$ would mean. It means that there exists $m \in \mathbb{Z}$ such that $n_1 = mn_2$. Since $n_1, n_2 \in \mathbb{Z}_{>0}$, we must have $m \in \mathbb{Z}_{>0}$. But then $n_1 < n_2 \leq mn_2$, which is incompatible with the equality $n_1 = mn_2$.

2. Let $A \subset \mathbb{Z}$ be a subgroup. Suppose first that $A \cap \mathbb{Z}_{\geq 1}$ is empty. Then also $A \cap \mathbb{Z}_{\leq -1}$ is empty, because if $n \in A$ then also $-n \in A$. Hence we must have $A = \{0\} = \langle 0 \rangle$. Suppose now that $A \cap \mathbb{Z}_{\geq 1}$ is not empty. Let n be the smallest element in $A \cap \mathbb{Z}_{\geq 1}$. We want to show that $A = \langle n \rangle$. Clearly $\langle n \rangle \subset A$, and therefore it remains to see that $A \subset \langle n \rangle$. To that end, let $k \in A$. By division with reminder, we can write $k = qn + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Notice that $r = k - qn \in A$. Therefore we can not have $r \neq 0$ because this would contradict the minimality of n. Hence $r = 0$ and $k = qn$. This shows that $k \in \langle n \rangle$ and thus we have shown that $A \subset \langle n \rangle$, as desired.

□

Definition 2.47. Let $n_1, n_2 \in \mathbb{Z}$. Consider the subgroup $A := \langle n_1 \rangle \cap \langle n_2 \rangle$ of $\mathbb{Z}$. By Theorem 2.46, there exists a unique $n \in \mathbb{Z}_{\geq 0}$ such that $A = \langle n \rangle$. This n is called the **least common multiple** of n_1 and n_2, denoted $\mathrm{lcm}(n_1, n_2)$.

Remark 2.48 (The "characterizing property", or "universal property", of the least common multiple)**.** Let $n_1, n_2 \in \mathbb{Z}$. Let us abbreviate $n := \mathrm{lcm}(n_1, n_2)$. Notice that for every $m \in \mathbb{Z}$ we have:

$$n_1 | m \text{ and } n_2 | m \iff m \in \langle n_1 \rangle \cap \langle n_2 \rangle \iff m \in \langle n \rangle \iff n | m.$$

In words, we got that the least common multiple of two integers is divisible by them both, and divides any other integer which is divisible by them both.

Definition 2.49. Let $n_1, n_2 \in \mathbb{Z}$. Consider the subgroup $A := \langle n_1, n_2 \rangle = \langle n_1 \rangle + \langle n_2 \rangle$ of $\mathbb{Z}$. By Theorem 2.46, there exists a unique $n \in \mathbb{Z}_{\geq 0}$ such that $A = \langle n \rangle$. This n is called the **greatest common divisor** of n_1 and n_2, denoted $\gcd(n_1, n_2)$.

Remark 2.50 (The "characterizing property", or "universal property", of the greatest common divisor)**.** Let $n_1, n_2 \in \mathbb{Z}$. Let us abbreviate $n := \gcd(n_1, n_2)$. Notice that $n_1 \in \langle n_1 \rangle \subset \langle n_1, n_2 \rangle = \langle n \rangle$, and therefore n divides n_1. Analogously, n divides n_2. If now we are given $m \in \mathbb{Z}$ which divides both n_1 and n_2, then we have $n_1 \in \langle m \rangle$ and $n_2 \in \langle m \rangle$ and so $\langle n \rangle = \langle n_1, n_2 \rangle \subset \langle m \rangle$, and thus $n \in \langle m \rangle$, meaning that m divides n. In words, we got that the greatest common divisor of two integers divides them both, and is divisible by any other integer which divides them both.

Remark 2.51 (very important property of the gcd)**.** Let $n_1, n_2 \in \mathbb{Z}$. Let us abbreviate $n := \gcd(n_1, n_2)$. Since $\langle n \rangle = \langle n_1, n_2 \rangle = \langle n_1 \rangle + \langle n_2 \rangle$, we have $n \in \langle n_1 \rangle + \langle n_2 \rangle$, which means that there exist $m_1 \in \langle n_1 \rangle$ and $m_2 \in \langle n_2 \rangle$ such that $n = m_1 + m_2$. Furthermore, there exist $k_1 \in \mathbb{Z}$ and $k_2 \in \mathbb{Z}$ such that $m_1 = k_1 n_1$ and $m_2 = k_2 n_2$, and we then obtain $n = k_1 n_1 + k_2 n_2$. In words, the greatest

common divisor of two integers can be expressed as a "linear combination with integer coefficients" of these two integers.

Remark 2.52. Given $n, m \in \mathbb{Z}$, we have $n|m$ and $m|n$ if and only if $m = n$ or $m = -n$. In particular, given $n, m \in \mathbb{Z}_{\geq 0}$, if we have $n|m$ and $m|n$ then $m = n$. This supports the naming above, of the properties being "characterizing". For example, given $n_1, n_2 \in \mathbb{Z}$, a number $m \in \mathbb{Z}_{\geq 0}$ having the following property - m divides n_1 and n_2 and is divisible by any other number $m' \in \mathbb{Z}$ which divides n_1 and n_2 - must be equal to $\gcd(n_1, n_2)$. Indeed, we know that $\gcd(n_1, n_2)$ has this property, so it is enough to show that there exists at most one $m \in \mathbb{Z}_{\geq 0}$ having this property. And indeed, if we have $m, m' \in \mathbb{Z}_{\geq 0}$ which both have this property, then $m|m'$ by the property of m' and $m'|m$ by the property of m and therefore by our current remark we have $m = m'$.

2.12 An example of an isomorphism of groups - the Chinese remainder theorem

Claim 2.53. *Let $n, m \in \mathbb{Z}$. If $\gcd(n, m) = 1$ then, given $k \in \mathbb{Z}$, $n|k$ and $m|k$ imply $nm|k$.*

Proof. By Remark 2.51 we can find $a, b \in \mathbb{Z}$ such that $an + bm = 1$. Since $n|k$ and $m|k$, we can find $p, q \in \mathbb{Z}$ such that $k = mp$ and $k = nq$. Then we obtain

$$k = 1 \cdot k = (an + bm)k = ank + bmk = anmp + bmnq = (ap + bq)mn,$$

and so $mn|k$. □

Exercise 2.10. *Show the following generalization of Claim 2.53: Given $n, m \in \mathbb{Z}_{\geq 1}$,*

$$\operatorname{lcm}(m, n) = \frac{mn}{\gcd(m, n)}.$$

Lemma-Definition 2.54. *Let $n, m \in \mathbb{Z}_{\geq 1}$. Suppose that $m|n$. Then the following is a well-defined group homomorphism:*

$$\operatorname{frgt}_m^n : \mathbb{Z}_n \xrightarrow{[k]_n \mapsto [k]_m} \mathbb{Z}_m.$$

Proof. We need to check independence on choice of representative. In other words, we need to check that if $k_1, k_2 \in \mathbb{Z}$ satisfy $[k_1]_n = [k_2]_n$, then $[k_1]_m = [k_1]_m$. By definition, the former means that $n|k_1 - k_2$. Since $m|n$, we then obtain $m|k_1 - k_2$, i.e. $[k_1]_m = [k_2]_m$, as desired. The homomorphism property is then immediate to verify. □

Theorem 2.55 (Chinese remainder theorem)**.** *Let $n, m \in \mathbb{Z}_{\geq 1}$. Suppose that $\gcd(n, m) = 1$. Then the group homomorphism*

$$\mathbb{Z}_{mn} \xrightarrow{\alpha \mapsto (\operatorname{frgt}_m^{mn}(\alpha), \operatorname{frgt}_n^{mn}(\alpha))} \mathbb{Z}_m \times \mathbb{Z}_n$$

is an isomorphism.

Proof. We need to check that this homomorphism is bijective. Since the source and target have the same order (nm), it is enough to check that this homomorphism is injective. For this, we need to check that given $k_1, k_2 \in \mathbb{Z}$, if $[k_1]_m = [k_2]_m$ and $[k_2]_m = [k_2]_n$ then $[k_1]_{mn} = [k_2]_{mn}$. By definition, we have $m|k_1 - k_2$ and $n|k_1 - k_2$. Then Claim 2.53 gives $mn|k_1 - k_2$, i.e. $[k_1]_{mn} = [k_2]_{mn}$, as desired. □

Corollary 2.56. *Let $n, m \in \mathbb{Z}_{\geq 1}$. Suppose that $\gcd(n, m) = 1$. Then the group homomorphism*

$$\mathbb{Z} \xrightarrow{k \mapsto ([k]_m, [k]_n)} \mathbb{Z}_m \times \mathbb{Z}_n$$

is surjective.

Proof. Notice that this factors as

$$\mathbb{Z} \xrightarrow{k \mapsto [k]_{mn}} \mathbb{Z}_{mn} \xrightarrow{\alpha \mapsto (\mathrm{frgt}_m^{mn}(\alpha), \mathrm{frgt}_n^{mn}(\alpha))} \mathbb{Z}_m \times \mathbb{Z}_n,$$

and the second map here is surjective by Theorem 2.55. □

Remark 2.57. Let us also prove the surjectivity above directly, because this is instructive. Thus, we are given $k_1, k_2 \in \mathbb{Z}$, and we want to show that there exists $k \in \mathbb{Z}$ such that $[k]_m = [k_1]_m$ and $[k]_n = [k_2]_n$. Let us find $p_1, p_2 \in \mathbb{Z}$ such that $p_1 m + p_2 n = 1$. Consider now

$$k := k_2 p_1 m + k_1 p_2 n.$$

Then

$$k = k_2 p_1 m + k_1 p_2 n = k_2 p_1 m + k_1(1 - p_1 m) = k_1 + (k_2 p_1 - k_1 p_1) m$$

and so $[k]_m = [k_1]_m$. Analogously, $[k]_n = [k_2]_n$, as desired.

Remark 2.58. This means that if we want an amount of apples such that when divided among 3 children it leaves 2 apples with us, while when divided among 10 children it leaves 7 with us - such an amount can be found.

2.13 Subgroups of the group of integers modulo n and Euler's function

Exercise 2.11. *Let G and H be groups and let $\phi : G \to H$ be a group homomorphism. Let $K \subset H$ be a subgroup of H. Then*

$$\phi^{-1}(K) := \{g \in G \mid \phi(g) \in K\} \subset G$$

is a subgroup of G.

Let us, in this subsection, denote by $\mathrm{pr}_n : \mathbb{Z} \to \mathbb{Z}_n$ the group homomorphism sending k to $[k]_n$.

Lemma 2.59. *Let $n \in \mathbb{Z}_{\geq 1}$. Let $m \in \mathbb{Z}$. Then*

$$\mathrm{pr}_n^{-1}(\langle [m]_n \rangle) = \langle \gcd(m,n) \rangle.$$

Proof. We have $k \in \mathrm{pr}_n^{-1}(\langle [m]_n \rangle)$ if and only if $[k]_n \in \langle [m]_n \rangle$, if and only if $[k]_n = d[m]_n = [dm]_n$ for some $d \in \mathbb{Z}$, if and only if $k - dm = en$ for some $d, e \in \mathbb{Z}$, i.e. if and only if $k \in \langle m \rangle + \langle n \rangle$. Since $\langle m \rangle + \langle n \rangle = \langle \gcd(m,n) \rangle$, we get that $k \in \mathrm{pr}_n^{-1}(\langle [m]_n \rangle)$ if and only if $k \in \langle \gcd(m,n) \rangle$, i.e. $\mathrm{pr}_n^{-1}(\langle [m]_n \rangle) = \langle \gcd(m,n) \rangle$, as desired. □

Claim 2.60. *Let $n \in \mathbb{Z}_{\geq 1}$.*

1. *Given $m \in \mathbb{Z}$, we have $\langle [m]_n \rangle = \langle [\gcd(n,m)]_n \rangle$.*
2. *Given $d_1, d_2 \in \mathbb{Z}_{\geq 1}$ such that $d_1 | n$ and $d_2 | n$, if $d_1 \neq d_2$ then $\langle [d_1]_n \rangle \neq \langle [d_2]_n \rangle$.*
3. *Every subgroup of $\mathbb{Z}_n$ is equal to $\langle [d]_n \rangle$ for some $d \in \mathbb{Z}_{\geq 1}$ satisfying $d | n$.*

Proof.

1. Let us abbreviate $d := \gcd(m,n)$. Since pr_n is surjective, we have $\langle [m]_n \rangle = \langle [d]_n \rangle$ if and only if $\mathrm{pr}_n^{-1}(\langle [m]_n \rangle) = \mathrm{pr}_n^{-1}(\langle [d]_n \rangle)$. By Lemma 2.59 we therefore need to check that

   $$\langle \gcd(m,n) \rangle = \langle \gcd(d,n) \rangle.$$

   By definition $\gcd(m,n) = d$, while $\gcd(d,n) = d$ also, since $d | n$ (check, as an exercise, that you understand this). Thus the equality holds.

2. Suppose that $\langle [d_1]_n \rangle = \langle [d_2]_n \rangle$; we want to show that $d_1 = d_2$. We have $\mathrm{pr}^{-1}(\langle [d_1]_n \rangle) = \mathrm{pr}^{-1}(\langle [d_2]_n \rangle)$ and by Lemma 2.59 we thus have $\langle \gcd(d_1,n) \rangle = \langle \gcd(d_2,n) \rangle$. However, since $d_i | n$, we have $\gcd(d_i, n) = d_i$, for $i \in \{1,2\}$. Thus we obtain $\langle d_1 \rangle = \langle d_2 \rangle$. By Theorem 2.46 we obtain $d_1 = d_2$.

3. Let $A \subset \mathbb{Z}_n$ be a subgroup. Consider $B := \mathrm{pr}_n^{-1}(A) \subset \mathbb{Z}$. Then, by Theorem 2.46, there exists $m \in \mathbb{Z}$ such that $B = \langle m \rangle$. Thus

   $$A = \mathrm{pr}_n(\mathrm{pr}_n^{-1}(A)) = \mathrm{pr}_n(B) = \mathrm{pr}_n\left(\{qm \ : \ q \in \mathbb{Z}\}\right) = \{[qm]_n \ : \ q \in \mathbb{Z}\} =$$

   $$= \{q[m]_n \ : \ q \in \mathbb{Z}\} = \langle [m]_n \rangle.$$

   By part 1 of the current claim, denoting $d := \gcd(m,n)$ we have $A = \langle [m]_n \rangle = \langle [d]_n \rangle$. Notice that $d \in \mathbb{Z}_{\geq 1}$ and satisfies $d | n$.

□

Exercise 2.12. *Let $n \in \mathbb{Z}_{\geq 1}$. Let $d \in \mathbb{Z}_{\geq 1}$ be such that $d | n$. Show that $|\langle [d]_n \rangle| = n/d$. Let $d_1, d_2 \in \mathbb{Z}_{\geq 1}$ be such that $d_1 | n$ and $d_2 | n$. Show that $\langle [d_1]_n \rangle \subset \langle [d_2]_n \rangle$ if and only if $d_2 | d_1$.*

Corollary 2.61. *Let $n \in \mathbb{Z}_{\geq 1}$. Let $m \in \mathbb{Z}$. Then $\mathbb{Z}_n = \langle [m]_n \rangle$ if and only if* $\gcd(m, n) = 1$.

Proof. Let us abbreviate $r := \gcd(m, n)$ (so $r \in \mathbb{Z}_{\geq 1}$ and $r|n$). By part 1 of Claim 2.60 we have $\langle [m]_n \rangle = \langle [r]_n \rangle$. Clearly, if $r = 1$ then $\langle [m]_n \rangle = \mathbb{Z}_n$ as desired. So we are left to show the converse - assume $\langle [m]_n \rangle = \mathbb{Z}_n$. Since also $\langle [1]_n \rangle = \mathbb{Z}_n$, by part 2 of Claim 2.60 we have $[r]_n = [1]_n$. Since $1 \leq 1, r \leq n$, this equality implies $r = 1$, as desired. □

Remark 2.62. Let us repeat the proof of Corollary 2.61 independently (in case we want to skip the more general material above). Our condition $\mathbb{Z}_n = \langle [m]_n \rangle$ is satisfied if and only if $\mathbb{Z} = \mathrm{pr}_n^{-1}(\langle [m]_n \rangle)$. However, we see easily that $\mathrm{pr}_n^{-1}(\langle [m]_n \rangle) = \langle m, n \rangle$. Therefore our condition is satisfied if and only if $\langle m, n \rangle = \mathbb{Z} = \langle 1 \rangle$, which means by definition $\gcd(m, n) = 1$.

Definition 2.63. Let $n \in \mathbb{Z}_{\geq 1}$. The number

$$|\{r \in \mathbb{Z},\ 1 \leq r \leq n \mid \gcd(r, n) = 1\}| = |\{\alpha \in \mathbb{Z}_n \mid \langle \alpha \rangle = \mathbb{Z}_n\}|$$

is denoted by $\phi(n)$. The function $n \mapsto \phi(n)$ is called **Euler's function**.

Remark 2.64. Given a group G and an element $g \in G$, we say that g is a **generator** of G if $G = \langle g \rangle$. We say that G is **cyclic** if it admits a generator (we will discuss cyclic groups later).

Example 2.65. *Let $p \in \mathbb{Z}_{\geq 1}$ be a prime number. Then given $r \in \mathbb{Z}$ we have* $\gcd(r, p) = 1$ *if and only if $p \nmid r$. Indeed, abbreviating $d := \gcd(r, p)$, we have $d|p$ and therefore $d = 1$ or $d = p$. But $d = p$ would mean $p|r$. So, in particular, we see that for $1 \leq r < p$ we have* $\gcd(r, p) = 1$ *and therefore $\phi(p) = p - 1$.*

2.14 The group $\mathbb{Z}_n^\times$

Let us fix $n \in \mathbb{Z}_{\geq 1}$ throughout this subsection.

Let us notice that $\mathbb{Z}_n$ has another natural operation $\mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, multiplication (in addition to the operation already discussed, addition). To define it, given $\alpha, \beta \in \mathbb{Z}_n$ we choose $a, b \in \mathbb{Z}$ such that $[a]_n = \alpha$ and $[b]_n = \beta$, and define $\alpha \cdot \beta := [ab]_n$ (one checks then that this is well-defined, i.e. does not depend on the choice of representatives). This operation does <u>not</u> provide $\mathbb{Z}_n$ with a group structure (unless we are in the trivial case $n = 1$) - the multiplication is associative, and there exists an identity element (namely $[1]_n$), but the element $[0]_n$, for example, does not have an inverse with respect to this multiplication. Here, an element $\beta \in \mathbb{Z}_n$ is said to be an **inverse** to an element $\alpha \in \mathbb{Z}_n$ if $\beta\alpha = [1]_n$ (and $\alpha\beta = [1]_n$, which is the same since the multiplication is commutative). If $\alpha \in \mathbb{Z}_n$ has an inverse then we say it is **invertible**. So, when talking about inverses and invertible elements in $\mathbb{Z}_n$ we always mean with respect to the multiplication - with respect to addition we use additive language, so we talk about the negative instead of the inverse.

Remark 2.66. The set $\mathbb{Z}_n$ with the operations of addition and multiplication forms what is known as a **commutative ring** - it satisfies all the axioms of a field except from, possibly, the axiom that every non-zero element has an inverse. There are various simple consequences which we don't specify in full detail. For example (we will use this in a moment), the distributive law $(\beta+\gamma)\alpha = \beta\alpha+\gamma\alpha$ for $\alpha, \beta, \gamma \in \mathbb{Z}_n$ implies that for $\alpha, \beta \in \mathbb{Z}_n$ and $m \in \mathbb{Z}$ we have $(m\beta)\alpha = m(\beta\alpha)$.

Lemma 2.67. *Let $\alpha \in \mathbb{Z}_n$. Then α admits an inverse if and only if $\langle\alpha\rangle = \mathbb{Z}_n$. Equivalently, if when writing $\alpha = [a]_n$ for $a \in \mathbb{Z}$ we have $\gcd(a, n) = 1$.*

Proof. We saw that $\langle\alpha\rangle = \mathbb{Z}_n$ is equivalent to $\gcd(a, n) = 1$ (in the notations in the formulation of the lemma) in Corollary 2.61.

We have $\langle\alpha\rangle = \mathbb{Z}_n$ if and only if $[1]_n \in \langle\alpha\rangle$. This happens if and only if $[1]_n = m\alpha$ for some $m \in \mathbb{Z}$. But $m\alpha = m([1]_n\alpha) = (m[1]_n)\alpha = [m]_n\alpha$. Thus this happens if and only if $\beta\alpha = [1]_n$ for some $\beta \in \mathbb{Z}_n$, i.e. if and only if α admits an inverse.

□

We denote by $\mathbb{Z}_n^\times \subset \mathbb{Z}_n$ the subset consisting of α for which α admits an inverse. By Lemma 2.67 the subset $\mathbb{Z}_n^\times$ of $\mathbb{Z}_n$ consists precisely of all the generators of $\mathbb{Z}_n$ (as an additive group). We have $|\mathbb{Z}_n^\times| = \phi(n)$. Notice that $\mathbb{Z}_n^\times$ is closed under multiplication in $\mathbb{Z}_n$ (because it is clear that if two elements have an inverse, then their product also has an inverse). If we restrict the multiplication on $\mathbb{Z}_n$ to $\mathbb{Z}_n^\times$, we obtain a group structure on $\mathbb{Z}_n^\times$ (because now, in addition to the multiplication being associative and admitting an identity element $[1]_n$, every element has an inverse). We always consider $\mathbb{Z}_n^\times$ with this group structure, and call it the **multiplicative group of integers modulo** n.

2.15 The order of an element in a group, cyclic groups

Definition 2.68. Let G be a group and let $g \in G$. If there exists $n \in \mathbb{Z}_{\geq 1}$ such that $g^n = 1_G$, the minimal such n will be denoted o_g and called the **order** of g. If there is no such n, we will write $o_g := \infty$ and say that the order of g is **infinite**.

Remark 2.69. Let G be a group. Clearly, for $g \in G$ we have $o_g = 1$ if and only if $g = 1_G$.

Exercise 2.13. *Show that $A \in \mathrm{GL}_n(\mathbb{C})$ has finite order if and only if A is diagonalizable and all the eigenvalues of A are roots of unity.*

Proposition 2.70. *Let G be a group and let $g \in G$.*

1. *Suppose that $o_g \neq \infty$. Then we have a unique isomorphism of groups $\mathbb{Z}_{o_g} \to \langle g\rangle$ which sends $[1]_{o_g}$ to g.*
2. *Suppose that $o_g = \infty$. Then we have a unique isomorphism of groups $\mathbb{Z} \to \langle g\rangle$ which sends 1 to g.*

In particular, we have[7] $|\langle g\rangle| = o_g$.

Proof.

1. Let us consider
$$A_g := \{m \in \mathbb{Z} \mid g^m = 1_G\} \subset \mathbb{Z}.$$
It is easy to check that A_g is a subgroup of $\mathbb{Z}$. By definition, o_g is the minimal element in $A_g \cap \mathbb{Z}_{\geq 1}$ and therefore by Theorem 2.46 we have $A_g = \langle o_g\rangle$. Let us now notice that the uniqueness of an isomorphism as desired is clear - given $m \in \mathbb{Z}$, since $[m]_{o_g} = m[1]_{o_g}$, such an isomorphism must send $[m]_{o_g}$ to g^m, and thus its values on all elements in $\mathbb{Z}_{o_g}$ are determined. To show existence, let us define a map $\phi : \mathbb{Z}_{o_g} \to \langle g\rangle$ by sending $[m]_{o_g}$ to g^m, for any $m \in \mathbb{Z}$. First we need to check that this map is well-defined. To that end, given $m_1, m_2 \in \mathbb{Z}$ such that $[m_1]_{o_g} = [m_2]_{o_g}$, we need to check that $g^{m_1} = g^{m_2}$. But $[m_1]_{o_g} = [m_2]_{o_g}$ amounts to $m_1 - m_2$ being divisible by o_g, i.e. to $m_1 - m_2 \in \langle o_g\rangle = A_g$, and so we get $g^{m_1-m_2} = 1_G$, and from here $g^{m_1} = g^{m_2}$, as desired. Now we want to check that ϕ is bijective. It is surjective since every element of $\langle g\rangle$ has the form g^m for some $m \in \mathbb{Z}$, and $\phi([m]_{o_g}) = g^m$. It is injective since, given $m_1, m_2 \in \mathbb{Z}$, $\phi([m_1]_{o_g}) = \phi([m_2]_{o_g})$ means $g^{m_1} = g^{m_2}$, which gives $g^{m_1-m_2} = 1_G$, meaning $m_1 - m_2 \in A_g = \langle o_g\rangle$, and so $[m_1]_{o_g} = [m_2]_{o_g}$. Finally, we check that ϕ is a homomorphism of groups:
$$\phi([m_1]_{o_g}+[m_2]_{o_g}) = \phi([m_1+m_2]_{o_g}) = g^{m_1+m_2} = g^{m_1}g^{m_2} = \phi([m_1]_{o_g})\phi([m_2]_{o_g}).$$

2. This is left to the reader (one proceeds similarly to the previous item, but perhaps easier).

□

Corollary 2.71. *Let G be a finite group. Then the order of every element in G is finite.*

Corollary 2.72. *Let G be a group and let $g \in G$. Suppose that the order if g is finite. Then, given $m \in \mathbb{Z}$, we have $g^m = 1_G$ if and only if o_g divides m.*

Definition 2.73. A group G is called **cyclic** if it is generated by one element, i.e. there exists $g \in G$ such that $G = \langle g\rangle$.

Corollary 2.74 (of Proposition 2.70)**.** *An infinite cyclic group is isomorphic to $\mathbb{Z}$, while a finite cyclic group is isomorphic to $\mathbb{Z}_n$, where n is its order.*

Exercise 2.14. *See that you understand the following summary. Let G be a cyclic group of order n. Let $g \in G$ be a generator of G. Given $m \in \mathbb{Z}$, the element g^m is a generator of G if and only if* $\gcd(m, n) = 1$. *We have $\phi(n)$ generators of G, we can parametrize them as the elements g^m, where m runs*

[7] To interpret this equality optimally when $o_g = \infty$, we should think of this infinite value as $\aleph_0$.

over integers satisfying $1 \leq m \leq n$ *and* $\gcd(m,n) = 1$. *More generally, given an integer* $1 \leq d \leq n$ *satisfying* $d|n$, *there is a unique subgroup* G_d *of* G *of order* d, *and for an integer* m, *the element* g^m *is a generator of* G_d *if and only if* $\gcd(m,n) = n/d$ *(while the element* g^m *lies in* G_d *if and only if* n/d *divides* $\gcd(m,n)$*).*

Remark 2.75. An interesting example of a cyclic group is $\mathbb{Z}_p^\times$ for a prime number $p \in \mathbb{Z}_{\geq 1}$. It is not immediate that this group is cyclic (maybe we will prove it later). Let $\alpha \in \mathbb{Z}_p^\times$ be a generator. Then by Proposition 2.70 there exists a unique isomorphism $\mathcal{E}xp : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^\times$ sending $[1]_{p-1}$ to α. It sends $[m]_{p-1}$ to α^m for every $m \in \mathbb{Z}$. Given $0 \leq m < p-1$, one can compute $\mathcal{E}xp([m]_{p-1})$ with computational complexity $O(\log p)$, so reasonably. However, let us denote by $\mathcal{L}og : \mathbb{Z}_p^\times \to \mathbb{Z}_{p-1}$ the map inverse to $\mathcal{E}xp$. For the computation of $\mathcal{L}og$ there is no known efficient classical algorithm[8]. This is called the **discrete logarithm problem**. A function such as $\mathcal{E}xp$, which is "easy" to compute but whose inverse is "hard" to compute is called a **one-way function** (we don't want to formalize this now). This stuff is the basis for public-key cryptography, among other things.

Example 2.76. *Let* $n \in \mathbb{Z}_{\geq 1}$. *We claim that we have an isomorphism of groups* $\phi : \mathrm{Aut}(\mathbb{Z}_n) \xrightarrow{\sim} \mathbb{Z}_n^\times$ *given by sending* σ *to* $\sigma([1]_n)$. *Clearly* ϕ *is well-defined, as an isomorphism of groups must send a generator to a generator, and* $\mathbb{Z}_n^\times$ *consists of the generators of* $\mathbb{Z}_n$. *In fact,* ϕ *is bijective - given* $\alpha \in \mathbb{Z}_n^\times$, *by part (1) Proposition 2.70 there exists a unique automorphism of* $\mathbb{Z}_n$ *which sends* $[1]_n$ *to* α. *Finally, one would like to check that* ϕ *is a homomorphism of groups. Given* $\sigma, \tau \in \mathrm{Aut}(\mathbb{Z}_n)$, *let us choose* $m, k \in \mathbb{Z}$ *such that* $\sigma([1]_n) = [m]_n$ *and* $\tau([1]_n) = [k]_n$. *Then*

$$\phi(\sigma \circ \tau) = (\sigma \circ \tau)([1]_n) = \sigma(\tau([1]_n) = \sigma([k]_n) = \sigma(k[1]_n) = k\sigma([1]_n) = k[m]_n =$$

$$= k([1]_n[m]_n) = (k[1]_n)[m]_n = [k]_n[m]_n = [m]_n[k]_n = \phi(\sigma)\phi(\tau).$$

2.16 Cosets

Recall how we constructed $\mathbb{Z}_n$. We defined an equivalence relation on $\mathbb{Z}$, by declaring $m_1 \sim m_2$ if $m_1 - m_2 \in \langle n \rangle$. We can think of it as saying that the difference between m_1 and m_2 is "neglegible", if we decide that to belong to $\langle n \rangle$ is neglegible. Generalizing this, let G be a group and let $H \subset G$ be a subgroup. We can define an equivalence relation on G, by setting $g_1 \sim g_2$ if $g_2^{-1} g_1 \in H$. As a small exercise, check that indeed this is an equivalence relation. The equivalence classes are called **left cosets of** H **in** G. Similarly, we can consider the equivalence relation on G given by $g_1 \sim g_2$ if $g_1 g_2^{-1} \in H$, and the equivalence classes for that equivalence relation are called **right cosets of** H **in** G. Notice that if G is abelian (as we had in the case of $\mathbb{Z}$) then there is no

[8] Wikipedia says that there is an efficient quantum algorithm due to P. Shor.

difference between those, so that we can simply talk about cosets. How does a left coset look like? Given $g \in G$, the unique left coset which contains g is

$$\{g' \in G \mid g^{-1}g' \in H\} = \{g' \in G \mid \exists h \in H : g^{-1}g' = h\} =$$

$$= \{g' \in G \mid \exists h \in H : g' = gh\} = \{gh \ : \ h \in H\} =: gH.$$

In other words, the left coset that contains g is the set of elements in G which can be obtained from g by multiplying by some element in H on the right. Or, "dually", it is the left shift by g of the subset H. We denote by G/H the set of left cosets of H in G, and we denote by $H\backslash G$ the set of right cosets of H in G.

Example 2.77. *Probably the most pictorially-satisfying example is as follows. Let us consider the abelian group $\mathbb{R}^2$ (with the addition of vectors as group operation). Let us consider $L \subset \mathbb{R}^2$ given by*

$$L := \{(x, y) \in \mathbb{R}^2 \mid x + 2y = 0\}.$$

Then L is an $\mathbb{R}$-vector subspace of $\mathbb{R}^2$, and in particular a subgroup of $\mathbb{R}^2$. I will draw in person the illustration of what cosets of L in $\mathbb{R}^2$ look like. In formulas, those are given by

$$C_a := \{(x, y) \in \mathbb{R}^2 \mid x + 2y = a\} = (a, 0) + L$$

for $a \in \mathbb{R}$, i.e. those are the lines in $\mathbb{R}^2$ which are parallel to the line L.

Example 2.78. *Of course, generalizing the previous example one can imagine the example of a vector space V over a field k, a k-vector subspace $W \subset V$, and the set of cosets V/W consists of subsets in V of the form*

$$v + W := \{v + w \ : \ w \in W\}.$$

Example 2.79. *Let us consider the group S_n. Consider the subgroup $H \subset S_n$ given by*

$$H := \{\sigma \in S_n \mid \sigma(1) = 1\}.$$

Then a left coset of H is of the form

$$L_r := \{\sigma \in S_n \mid \sigma(1) = r\}$$

(where $r \in \{1, \ldots, n\}$) and a right coset of H is of the form

$$R_r := \{\sigma \in S_n \mid \sigma(r) = 1\}.$$

2.17 The index and Lagrange's theorem

Given a group G and a subset $S \subset G$, we denote $S^{-1} := \{g^{-1} \ : \ g \in S\}$.

Exercise 2.15. *Let G be a group and let $H \subset G$ be a subgroup. Then we have a bijection between G/H and $H\backslash G$, given by sending S to S^{-1}.*

Definition 2.80. Let G be a group and let $H \subset G$ be a subgroup. We define the **index of H in G**, denoted $[G : H]$, as $|G/H|$, which is the same as $|H\backslash G|$ by the exercise above.

Claim 2.81 (Lagrange's theorem)**.** *Let G be a group and let $H \subset G$ be a subgroup. Then*

$$|G| = |H| \cdot [G : H].$$

Proof. Notice first that for every $S \in G/H$ we have $|S| = |H|$. Indeed, let $g \in S$. Then we obtain a bijection $H \to S$ by sending $h \mapsto gh$. Thus, we can now compute:

$$|G| = \left| \coprod_{S \in G/H} S \right| = \sum_{S \in G/H} |S| = \sum_{S \in G/H} |H| = |H| \cdot [G : H].$$

□

Corollary 2.82 (also called Lagrange's theorem)**.** *Let G be a finite group and let $H \subset G$ be a subgroup. Then $|H|$ divides $|G|$.*

Corollary 2.83. *Let G be a finite group and let $g \in G$. Then o_g (which is finite by Corollary 2.71) divides $|G|$.*

Proof. By Proposition 2.70 we have $o_g = |\langle g \rangle|$ and, by Corollary 2.82, $|\langle g \rangle|$ divides $|G|$. □

Corollary 2.84. *Let G be a finite group and let $g \in G$. Then $g^{|G|} = 1$.*

Example 2.85. *Let $n \in \mathbb{Z}_{\geq 1}$. Given $\alpha \in \mathbb{Z}_n^\times$, we have $\alpha^{\phi(n)} = [1]_n$. This is called **Euler's theorem**. Put differently, given $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$ we have $a^{\phi(n)} \equiv_n 1$. As a special case, given a prime number $p \in \mathbb{Z}_{\geq 1}$ and given $\alpha \in \mathbb{Z}_p^\times$ we have $\alpha^{p-1} = [1]_p$. This is called **Fermat's little theorem**. Put differently, given $a \in \mathbb{Z}$ such that $p \nmid n$ we have $a^p \equiv_p 1$.*

Exercise 2.16. *Let G be a group, let $H, K \subset G$ be subgroups and assume that $H \subset K$. Show that $[G : K] = [G : H] \cdot [H : K]$. Hint: In general, given a group G and a subgroup $H \subset G$, a **family of representatives** in G for left cosets of H is a family $\{g_i\}_{i \in I}$ of elements in G such that for every $C \in G/H$ there exists a unique $i \in I$ satisfying $g_i H = C$ (sometimes it is convenient to take the indexing set I to be equal to G/H and require $g_C H = C$, but sometimes it is convenient to allow it to be more abstract). Of course we then have $|I| = |G/H|$. Back to our exercise, choose a family of representatives $\{g_i\}_{i \in I}$ in G for the left cosets of K. Choose a family of representatives $\{k_j\}_{j \in J}$ in K for the left cosets of H. Show then that $\{g_i k_j\}_{(i,j) \in I \times J}$ is a family of representatives in G for the left cosets of H.*

2.18 Groups of prime order

Claim 2.86. *Every group of prime order is cyclic, and so isomorphic to $\mathbb{Z}_p$, where p is its order.*

Proof. Let G be a finite group such that $p := |G|$ is prime. Let $g \in G$ be any element such that $g \neq 1_G$. Since, by Corollary 2.83, we have $o_g | p$, we must have either $o_g = 1$ or $o_g = p$. Since $g \neq 1_G$, we have $o_g \neq 1$, and so $o_g = p$. By Proposition 2.70 we get $|\langle g \rangle| = o_g = p = |G|$ and so $\langle g \rangle = G$. Thus G is cyclic. □

3 Group action

3.1 The definition of action again

Recall that, given a group G and a set X, an action of G on X is a group homomorphism $\rho : G \to S(X)$, which we can call an **action homomorphism**. There is a standard second way of thinking about the same.

Definition 3.1. Let $(G, \star)$ be a group and let X be a set. A map $\bullet : G \times X \to X$ (it is customary to write $g \bullet x$ instead of $\bullet(g, x)$) is called an **action map** if:

1. Let $g_1, g_2 \in G$ and $x \in X$. We have $g_1 \bullet (g_2 \bullet x) = (g_1 \star g_2) \bullet x$.
2. Let $x \in X$. We have $1_G \bullet x = x$.

We think of $g \bullet x$ as the result of applying g to x.

Exercise 3.1. *Let $(G, \star)$ be a group and let X be a set. We have a bijection between the sets*

$$\{\text{action homomorphisms } \rho : G \to S(X)\}$$

and

$$\{\text{action maps } \bullet : G \times X \to X\}$$

given as follows. Given ρ belonging to the upper set, we construct $\bullet$ in the lower set by defining $g \bullet x := \rho(g)(x)$. Given $\bullet$ in the lower set, we construct ρ in the upper set by defining $\rho(g)(x) := g \bullet x$. One should now check that these two maps between the two sets are well-defined and mutually inverse.

Therefore, we can think of an action of a group G on a set X either as given by an group homomorphism $\rho : G \to S(X)$ or as given by an action map $a : G \times X \to X$. We get used to this, and use these as convenient.

Remark 3.2. Similarly to notational conventions before, given a group G and a set X, given an action of G on X, encoded by a group homomorphism $\rho : G \to S(X)$ and an action map $\bullet : G \times X \to X$, we usually keep ρ and a implicit, and write gx instead of $g \bullet x$.

Let us give some basic examples of group actions.

Example 3.3. *Given a set X, we have an action of $S(X)$ on X given by $\sigma \bullet x := \sigma(x)$.*

Example 3.4. *Given a vector space V over a field k, we have an action of $\mathrm{GL}_k(V)$ on V given by $T \bullet v := T(v)$.*

Example 3.5. *Let G be a group and let $H \subset G$ be a subgroup. There is a G-action on G/H, given by $g \bullet g'H := gg'H$.*

Example 3.6. *Let G be a group. There are three standard actions of G on G. The **left regular action** is given by $g \bullet g' := gg'$. The **right regular action** is given by $g \bullet g' := g'g^{-1}$. The **conjugation action** is given by $g \bullet g' := gg'g^{-1}$.*

Example 3.7. *An important example of a group action in mathematics is as follows. Let $G := \mathrm{SL}_2(\mathbb{R})$ and let $\mathbb{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ (the **upper half plane**). Then we have an action of G on $\mathbb{H}$ given by*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \bullet z := \frac{az+b}{cz+d}.$$

3.2 The idea of "induced" symmetry

Roughly speaking, if we have a symmetry of a situation and this situation gives rise to another situation, the new situation has the same symmetry. A bit more precisely, let G be a group acting on a set X which has some extra structure, and the group action preserves the extra structure in a natural sense. Then if from the set X with its extra structure we construct a new set with extra structure, we should expect the new set to also carry an action of the group G, preserving the extra structure. Some examples:

1. Let X be a set equipped with an action of a group G. Let us consider $X \times X$. Then it has an action of G given by $g \cdot (x_1, x_2) := (g \cdot x_1, g \cdot x_2)$.

2. Let X be a set equipped with an action of a group G. Let us consider a set S, and the set $\mathrm{Fun}(S, X)$ of functions from S to X. Then it has an action of G given by $(g \cdot f)(s) := g \cdot f(s)$.

3. Let X be a set equipped with an action of a group G. Let us consider a set S, and the set $\mathrm{Fun}(X, S)$ of functions from X to S. Then it has an action of G given by $(g \cdot f)(x) := f(g^{-1} \cdot s)$. Notice the inverse here! A formal justification of it is that without it, we don't get an action (we get a right action, but our convention is that we only consider left actions). One can also understand this by imagining an element $f \in \mathrm{Fun}(X, S)$ as a collection of things sticking out of X, and then imagine what happens to it when we rotate X - I will explain in person.

4. Let V be a vector space over a field k. Let $\mathcal{L}$ denote the set of 1-dimensional k-vector subspaces in V. Then $\mathrm{GL}_k(V)$ naturally acts on $\mathcal{L}$, by $g \cdot L := \{g(v) \ : \ v \in L\}$.

5. Let G be group, and let Sgrp_G be the set of subgroups of G. The conjugation action of G on itself induces an action of G on Sgrp_G, explicitly given as follows:

$$g \bullet H := gHg^{-1} := \{ghg^{-1} \ : \ h \in H\}.$$

3.3 Stabilizers, transporters, orbits

Definition 3.8. Let G be a group, X a set, and let us be given an action of G on X.

1. Given $x, y \in X$, we define the **transporter**

$$\mathrm{Trans}_G(x, y) := \{g \in G \mid gx = y\}.$$

2. Given $x \in X$, we define the **stabilizer**

$$\mathrm{Stab}_G(x) := \mathrm{Trans}_G(x, x) = \{g \in G \mid gx = x\}.$$

Exercise 3.2. *Let G be a group, X a set, and let us be given an action of G on X.*

1. *Let $x \in X$. Then $\mathrm{Stab}_G(x)$ is a subgroup of G.*
2. *Let $x, y \in X$. Then $\mathrm{Trans}_G(x, y)$ is either empty, or it is a left coset of $\mathrm{Stab}_G(x)$ and a right coset of $\mathrm{Stab}_G(y)$.*

Example 3.9. *Let us consider the action of G on itself by conjugation. Given $g \in G$, its stabilizer under this action is denoted by $C_G(g)$ and called the **centralizer** of g in G. Explicitly:*

$$C_G(g) := \{g' \in G \mid g'g = gg'\}.$$

*Similarly, if we consider the action of G on the set Sgrp_G of subgroups of G by conjugation, given a subgroup $H \subset G$, its stabilizer under this action is denoted by $N_G(H)$ and called the **normalizer** of H in G. Explicitly:*

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

where the notation gHg^{-1} is as in example 5 of §3.2.

Example 3.10. *Let $T \subset \mathrm{GL}_n(k)$ be the subgroup of diagonal matrices. Show that the normalizer of T in $\mathrm{GL}_n(k)$ is the subgroup of invertible matrices A for which each column has precisely one non-zero entry (i.e. "permutation matrices").*

Example 3.11. *Usually, one can interpret groups of symmetries that preserve some extra structure as stabilizers. For example, Let (E, Φ) be a finite-dimensional inner product space over $\mathbb{R}$ (Φ denotes the inner product we have on E). We have the group $\mathrm{GL}_{\mathbb{R}}(E)$ and the subgorup $\mathrm{O}(E, \Phi) \subset \mathrm{GL}_{\mathbb{R}}(E)$ consisting of*

transformations T which are orthogonal with respect to the inner product Φ, i.e. satisfying $\langle T(v), T(w)\rangle = \langle v, w\rangle$ for all $v, w \in E$. How to interpret $\mathrm{O}(E, \Phi)$ as a stabilizer? Let us consider the set $\mathrm{IP}(E)$ of inner products on E. Then $\Phi \in \mathrm{IP}(E)$. We have an action of $\mathrm{GL}_{\mathbb{R}}(E)$ on $\mathrm{IP}(E)$, given by $(T \bullet \Psi)(v, w) := \Psi(T^{-1}(v), T^{-1}(w))$ for all $v, w \in E$. Then $\mathrm{O}(E, \Phi)$ is the stabilizer of Φ under this action of $\mathrm{GL}_{\mathbb{R}}(E)$ on $\mathrm{IP}(E)$.

Lemma-Definition 3.12. *Let G be a group, X a set, and let us be given an action of G on X. The relation on X given by setting $x \sim y$ if there exists $g \in G$ such that $gx = y$, i.e. if $\mathrm{Trans}_G(x, y) \neq \emptyset$, is an equivalence relation. The equivalence classes are called the **G-orbits in** X. Given $x \in X$, we denote by $\mathrm{Orb}_G(x) \subset X$ the orbit which contains x, i.e.*

$$\mathrm{Orb}_G(x) := \{y \in X \mid \exists g \in G \text{ s.t. } gx = y\}.$$

Let us also denote by $\mathrm{Orb}_G(X)$ the sets of G-orbits in X.

Remark 3.13. Let G be a group, X a set, and let us be given an action of G on X. A subset $Y \subset X$ is said to be **G-invariant**, or **invariant under the G-action**, if $gy \in Y$ for all $g \in G$ and $y \in Y$. Thus, G-orbits in X can be thought of as minimal (non-empty) G-invariant subsets of X. Notice that on a G-invariant subset we naturally have an action of G, simply by restricting the action on X.

Example 3.14. *Let G be a group and let $H \subset G$ be a subgroup. By restricting to H the right regular action of G on itself, we obtain an action of H on G, given by $h \bullet g := gh^{-1}$. Then, notice, that the H-orbits on G for that action are precisely the left H-cosets in G. Notice then that $\mathrm{Orb}_G(X)$ is precisely G/H.*

Example 3.15. *Let G be a group and let us consider the conjugation action of G on itself. The orbits of this action are called **conjugacy classes** in G. Explicitly, given $g \in G$ the conjugacy class containing g is given by $\{hgh^{-1} : h \in G\}$. The **center** of G, denoted $Z(G)$, is the defined as the subset*

$$Z(G) := \{g \in G \mid gh = hg \ \forall h \in G\} \subset G.$$

Notice tha $Z(G)$ consists precisely of those $g \in G$ whose centralizer is the whole G or, equivalently, for which the orbit under the conjugation action is the singleton $\{g\}$. Check that $Z(G)$ is a subgroup of G.

Example 3.16. *Let us consider the subgroup $\mathrm{SO}(2) \subset \mathrm{GL}_2(\mathbb{R})$ consisting of orthogonal matrices of determinant 1 (i.e. the group of linear rotations of the plane). The orbits of the action of $\mathrm{SO}(2)$ on $\mathbb{R}^2 \smallsetminus \left\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}\right\}$ given by multiplication of a vector by a matrix are circles whose center is $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$.*

3.4 Free and transitive actions

Lemma-Definition 3.17. *Let G be a group, X a set, and let us be given an action of G on X. The following are equivalent:*

1. *For every $x \in X$, $\mathrm{Stab}_G(x) = \{1_G\}$.*
2. *For every $x, y \in X$, $|\mathrm{Trans}_G(x, y)| \in \{0, 1\}$.*

*If these equivalent conditions are satisfied, we say that the given action of G on X is **free**.*

Example 3.18. *The actions we considered in Example 3.14 and Example 3.16 are free.*

Lemma-Definition 3.19. *Let G be a group, X a set, and let us be given an action of G on X. The following are equivalent:*

1. *X is non-empty and for every $x, y \in X$ the set $\mathrm{Trans}_G(x, y)$ is non-empty.*
2. *$|\mathrm{Orb}_G(X)| = 1$.*

*If these equivalent conditions are satisfied, we say that the given action of G on X is **transitive**.*

Example 3.20. *Given a group G and a subgroup $H \subset G$, the action of G on G/H from Example 3.5 is transitive. The action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}$ from Example 3.7 is also transitive.*

Remark 3.21. Given a group G, a set X and an action $a : G \times X \to X$ of G on X, we can consider the map $\widetilde{a} : G \times X \to X \times X$ given by $\widetilde{a}(g, x) := (x, a(g, x))$. Check that given $x, y \in X$ we have a natural bijection between $\widetilde{a}^{-1}(x, y)$ and $\mathrm{Trans}_G(x, y)$. Deduce that the action a is free if and only if the map $\widetilde{a}$ is injective, while the action a is transitive if and only if the map $\widetilde{a}$ is surjective.

3.5 The orbit-stabilizer formula

Proposition 3.22. *Let G be a group, X a set, and let us be given an action of G on X. Let $x_0 \in X$ and denote $H := \mathrm{Stab}_G(x_0)$. Then the following map is well-defined, and is a bijection:*

$$G/H \xrightarrow{gH \mapsto gx_0} \mathrm{Orb}_G(x_0).$$

Proof. First, one needs to check that the map is well-defined. Namely, given $g_1, g_2 \in G$ such that $g_1 H = g_2 H$, we want to check that $g_1 x_0 = g_2 x_0$. However, the former means that $g_2 = g_1 h$ for some $h \in H$, and then $g_2 x_0 = g_1 h x_0 = g_1 x_0$, as desired. Let us check that the map is injective. Given $g_1, g_2 \in G$, we want to check that $g_1 x_0 = g_2 x_0$ implies $g_1 H = g_2 H$. Indeed, the former implies that $g_1^{-1} g_2 x_0 = x_0$, i.e. $g_1^{-1} g_2 \in H$, and thus $g_1 H = g_2 H$, as we know from our discussion about cosets. Next, notice that the map is surjective - this is clear by the definition of a G-orbit. □

Corollary 3.23 (Orbit-Stabilizer formula)**.** *Let G be a group, X a set, and let us be given an action of G on X. Suppose that G is finite. Let $x_0 \in X$. We have:*

$$|\mathrm{Orb}_G(x)| = \frac{|G|}{|\mathrm{Stab_G(x_0)}|}.$$

Proof. We use Proposition 3.22 and Lagrange's theorem. □

Corollary 3.24. *Let G be a group, X a set, and let us be given an action of G on X. Suppose that G is finite. Let $x_0 \in X$. Then $|\mathrm{Orb}_G(x)|$ divides $|G|$.*

Example 3.25. *Let G be a finite group and let $C \subset G$ be a conjugacy class. Then $|C|$ divides $|G|$.*

3.6 Digression: G-sets

A natural point of view on actions is to fix a group G and consider sets equipped with a G-action, as our objects-with-extra-structure to study.

Definition 3.26. Let G be a group.

1. A **G-set** is a pair consisting of a set X and a action map $G \times X \to X$. Again, in terms of notation, one usually speaks of a G-set X, without making the notation of the action map implicit.

2. Let X and Y be G-sets. A **homomorphism of G-sets** from X to Y is a map $\phi : X \to Y$ satisfying $\phi(gx) = g\phi(x)$ for all $x \in X$ and $g \in G$. An **isomorphism of G-sets** is a homomorphism of G-sets $\phi : X \to Y$ which is invertible, i.e. for which there exists a homomorphism of G-sets $\psi : Y \to X$ such that $\phi \circ \psi = \mathrm{id}_Y$ and $\psi \circ \phi = \mathrm{id}_X$.

Exercise 3.3. *Let G be group and let X and Y be G-sets. Show that a map $\phi : X \to Y$ is a isomorphism of G-sets if and only if it is a bijective homomorphism of G-sets.*

Remark 3.27. We could also define a G-set as consisting of a set X and an action group homomorphism $G \to S(X)$. As we said, we get used to the equivalence between the action homomorphism and action map and will not see a difference between the datum of one or the other.

Remark 3.28. One can precise slightly Proposition 3.22, by saying that the map considered there is not only a bijection, but in fact an isomorphism of G-sets, where G/H is considered a G-set using the action of Example 3.5. One deduces that every transitive G-set is isomorphic to a G-set of the form G/H, for some subgroup $H \subset G$. This relates "how G can act there in the world" (its "foreign affairs") with "what is G built form" (its "domestic affairs").

3.7 Digression: G-torsors

Definition 3.29. Let G be a group. A G-set is called a **G-torsor** if it is free and transitive.

Example 3.30. *Let V be an n-dimensional vector space over a field k. Let us consider the set $\mathcal{B}$ of ordered bases of V. We have an action of $\mathrm{GL}_k(V)$ on $\mathcal{B}$, given by $T \cdot (e_1, \dots, e_n) := (T(e_1), \dots, T(e_n))$. Then $\mathcal{B}$ becomes a $\mathrm{GL}_k(V)$-torsor.*

Example 3.31. *Let G be a group and let $H \subset G$ be a subgroup. Let $C \subset G$ be a right H-coset in G. Then we can consider C as an H-set via $h \bullet c := hc$. It is an H-torsor.*

Remark 3.32. Let G be a group and let X be a G-torsor. Given $x_0 \in X$, we get a bijection $G \to X$ given by $g \mapsto gx_0$. So in some sense X "looks like" G. However, this bijection is not canonical, since varying x_0 will change it. So one sometimes thinks of a G-torsor as "G with the origin 1_G forgotten". For example, one can formalize in this way what an affine space is - given a field k, an **affine space** over k can be defined as a pair (V, A) consisting of a vector space V over k and a V-torsor A, where V is considered as a group for vector addition.

3.8 Burnside's lemma

Claim 3.33 (Burnside's lemma)**.** [9] *Let G be a group, X a set, and let us be given an action of G on X. Suppose that G and X are finite. For $g \in G$, let us denote*

$$\mathrm{Fix}_X(g) := \{x \in X \mid gx = x\}.$$

Then

$$|\mathrm{Orb}_G(X)| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_X(g)|.$$

Proof. As usual, let us denote by $\delta_{a,b}$ the number 1 if $a = b$ and the number 0 if $a \neq b$. We have

$$\sum_{g \in G} |\mathrm{Fix}_X(g)| = \sum_{g \in G} |\{x \in X \mid gx = x\}| = \sum_{g \in G} \sum_{x \in X} \delta_{gx,x} = \sum_{x \in X} \sum_{g \in G} \delta_{gx,x} =$$

$$= \sum_{x \in X} |\{g \in G \mid gx = x\}| = \sum_{x \in X} |\mathrm{Stab}_G(x)| = \sum_{x \in X} \frac{|G|}{|\mathrm{Orb_G(x)}|} =$$

$$= |G| \sum_{G\text{-orbit } O \text{ in } X} \sum_{x \in O} \frac{1}{|\mathrm{Orb}_G(x)|} = |G| \sum_{G\text{-orbit } O \text{ in } X} \frac{1}{|O|} \sum_{x \in O} 1 =$$

$$= |G| \sum_{G\text{-orbit } O \text{ in } X} 1 = |G| \cdot |\mathrm{Orb_G(X)}|,$$

and this is clearly as desired. □

[9] Also known as "the lemma that is not Burnside's".

Let us illustrate the use of Burnside's lemma. Imagine that we have a jewelry in the form of a regular hexagon, thus with six vertices, and we want to color the vertices in $k \in \mathbb{Z}_{\geq 1}$ colors. Here, the jewelry is symmetric, so that colorings are considered the same if we can move our jewelry in space to make them the same (should illustrate in person). How many different colorings are there? We can imagine the jewelry's vertices as X_6 from Example 2.2. Recall the action of the group D_6 on X_6. If we denote by C the set of k colors, we can think of $\mathrm{Fun}(X_6, C)$ (the set of functions from X_6 to C) as the set of colorings. Recall the action of D_6 on $\mathrm{Fun}(X_6, C)$, as in §3.2. Then, in fact, we are interested in

$$|\mathrm{Orb}_{D_6}(\mathrm{Fun}(X_6, C))|,$$

the reader should understand this. We want to use Burnside's lemma in order to compute this. We count fixed points:

1. The identity element: k^6.
2. Rotation by $2\pi \cdot (1/6)$ radians and by $2\pi \cdot (5/6)$ radians: k.
3. Rotation by $2\pi \cdot (2/6)$ radians and rotation by $2\pi \cdot (4/6)$ radians: k^2.
4. Rotation by $2\pi \cdot (3/6)$ radians: k^3.
5. Reflection via an axis passing through a vertex: k^4.
6. Reflection via an axis not passing through a vertex: k^3.

Overall, we obtain by Burnside's lemma:

$$|\mathrm{Orb}_{D_6}(\mathrm{Fun}(X_6, C))| = \frac{1}{12}\left(k^6 + 2 \cdot k + 2 \cdot k^2 + 4 \cdot k^3 + 3 \cdot k^4\right).$$

In particular, we learn that the right hand side is an integer for all $k \in \mathbb{Z}_{\geq 1}$!

3.9 Application: Cauchy's theorem

Theorem 3.34 (Cauchy's theorem)**.** *Let G be a finite group. Let $p \in \mathbb{Z}_{\geq 1}$ be a prime number dividing $|G|$. Then there exists $g \in G$ such that $o_g = p$.*

Proof. Let us consider an auxiliary cyclic group H of order p (we can think of it as $\mathbb{Z}_p$, but I will use for convenience multiplicative notation), and let $h \in H$ be a generator, i.e. $H = \langle h \rangle$. Let us consider the set X of functions from H to G. We consider the action of H on X given by

$$(k \cdot f)(\ell) := f(k^{-1}\ell).$$

Now, let us consider the subset $X_1 \subset X$ consisting of those f for which

$$f(1) \cdot f(h) \cdot f(h^2) \cdot \ldots \cdot f(h^{p-1}) = 1.$$

Notice that $|X_1| = |G|^{p-1}$.

We claim that X_1 is invariant under our action of H. Indeed, first notice that it is enough to check that $h \cdot X_1 \subset X_1$. This is because $\{k \in H \mid k \cdot X_1 \subset X_1\}$ is clearly closed under the group operation and therefore if it contains h then it contains $h \cdot h = h^2$, and $h \cdot h^2 = h^3$, and so on; by induction it will contain h^n for every $n \in \mathbb{Z}_{\geq 1}$, and thus all elements in H. Let us thus show that $h \cdot X_1 \subset X_1$. Let $f \in X_1$. Recall that, in a group, if $ab = 1$ then also $ba = 1$. Therefore, we have:

$$(h \cdot f)(1) \cdot (h \cdot f)(h) \cdot (h \cdot f)(h^2) \cdot \ldots \cdot (h \cdot f)(h^{p-1}) = f(h^{p-1}) \cdot f(1) \cdot f(h) \cdot \ldots \cdot f(h^{p-2}) = 1,$$

as desired.

Thus, we have an action of H on X_1. Notice that each H-orbit in X_1 has either 1 or p elements, by the orbit-stabilizer formula. We thus get:

$$|G|^{p-1} = |X_1| = \sum_{O \in \mathrm{Orb}_H(X_1)} |O| = \sum_{\substack{O \in \mathrm{Orb}_H(X) \\ |O|=1}} |O| + \sum_{\substack{O \in \mathrm{Orb}_H(X_1) \\ |O|=p}} |O| =$$

$$= |\{f \in X_1 \mid \mathrm{Stab}_H(f) = H\}| + (\text{a number divisible by } p)\,.$$

Since $|G|$ is divisible by p, we obtain from this equation that, denoting $X_2 := \{f \in X_1 \mid \mathrm{Stab}_H(f) = H\}$, p divides $|X_2|$. Notice that the constant function with value 1 belongs to X_2, and therefore we must have $|X_2| \geq p$, so X_2 contains some function f which is not the constant function with value 1. Now, notice that in fact X_2 consists precisely of the constant functions with value $g \in G$ satisfying $g^p = 1$ (let us leave this as a very easy exercise). Hence, there exists $g \in G$ such that $g \neq 1$ and $g^p = 1$, implying $o_g = p$, as desired.

□

4 Isomorphism theorems etc.

4.1 Kernel and image

Definition 4.1. Let G and H be groups and let $\phi : G \to H$ be a homomorphism of groups. The **kernel** of ϕ is the subgroup of G defined as follows:

$$\mathrm{Ker}(\phi) := \phi^{-1}(1) = \{g \in G \mid \phi(g) = 1\} \subset G.$$

The **image** of ϕ is the subgroup of H defined as follows:

$$\mathrm{Im}(\phi) := \{\phi(g) \ : \ g \in G\} = \{h \in H \mid \exists g \in G \text{ s.t. } \phi(g) = h\} \subset H.$$

Exercise 4.1. *Check that indeed the kernel and image as defined above are subgroups as claimed.*

Definition 4.2. An injective homomoprhism is called a **monomorphism** and a surjective homomorphism is called an **epimorphism**.

Lemma 4.3. *Let G and H be groups and let $\phi : G \to H$ be a homomorphism of groups.*

1. *ϕ is surjective if and only if $\mathrm{Im}(\phi) = H$.*
2. *ϕ is injective if and only if $\mathrm{Ker}(\phi) = \{1\}$.*

Proof. Property 1 is a general property of the image of a map between sets. Let us show property 2. If ϕ is injective then by definition $|\phi^{-1}(1)| \leq 1$ and since $1 \in \phi^{-1}(1)$ we obtain $\phi^{-1}(1) = \{1\}$. Notice now that $\mathrm{Ker}(\phi) = \phi^{-1}(1)$. In the other direction, suppose that $\mathrm{Ker}(\phi) = \{1\}$. Let $g_1, g_2 \in G$ be such that $\phi(g_1) = \phi(g_2)$; we want to see that $g_1 = g_2$). We have

$$\phi(g_1 g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1} = 1$$

i.e. $g_1 g_2^{-1} \in \mathrm{Ker}(\phi)$ and so $g_1 g_2^{-1} = 1$, i.e. $g_1 = g_2$. □

4.2 Quotient groups

Given a mathematical structure, one can try to study substructures of it, as well as quotient structures of it. There are different ways of talking about these things. Roughly, we can say that there is an **internal** way and an **external** way. For example, let us consider the simplest mathematical structures - sets. A substructure of a set S, in the internal interpretation, is a subset of S. In the external interpretation, it is a pair (T, i) consisting of a set T and an injective map $i : T \to S$. One can explain the precise relation between these two approaches. What about quotient structures for sets? In the internal approach, it will be an equivalence relation on S. In the external approach, it will be a pair (T, p) consisting of a set T and a surjective map $p : S \to T$. Again, one can explain the precise relation between these two approaches.

Remark 4.4. So what is the precise relation alluded to above? For the example of substructures of sets, given (T, i) as above, we can consider the image of i, which is a subset of S. In the opposite direction, given a subset T of S we can consider (T, i) where $i : T \to S$ is simply the inclusion of the subset T in the set S. To understand in what sense these two procedures are inverse to each other, we need to understand the following: Given two pairs $(T, i), (T', i')$ as above, we need to identify those pairs if there exists a bijection $\alpha : T \to T'$ such that $i' \circ \alpha = i$. Then the two procedures which were described indeed become inverse to each other. Regarding the example of quotient structures of sets, given (T, p) as above, we can consider the equivalence relation on S given by defining $s_1 \sim s_2$ if $p(s_1) = p(s_2)$. Conversely, given an equivalence relation $\sim$ on S, we can consider the pair $(S/\sim, p)$ where p is the quotient map, associating to an element of S its equivalence class. Again, in order to have these procedures inverse to each other, we have to identify two pairs $(T, p), (T', p')$ if there exists a bijection $\alpha : T \to T'$ satisfying $p' \circ \alpha = p$.

Substructures for groups are simple to talk about - those are subgroups (that is, in the internal approach; injective group homomorphisms in the external

approach), which we have already considered. We want now to talk about quotient structures.

Proposition 4.5. *Let G and H be groups and let $\phi : G \to H$ be an epimorphism of groups. Let K be another group and let $\psi : G \to K$ be a homomorphism of groups. If $\mathrm{Ker}(\phi) \subset \mathrm{Ker}(\psi)$ then there exists a unique homomorphism of groups $\psi' : H \to K$ such that $\psi = \psi' \circ \phi$.*

Proof. It is clear that ψ' is unique, if exists, because ϕ is surjective. To show existence of ψ', we do the only thing we can do. Namely, given $h \in H$ let us define $\psi'(h)$ by choosing $g \in G$ such that $\phi(g) = h$ and setting $\psi'(h) := \psi(g)$. We need to check that this is well-defined, i.e. the construction does not depend on the choices made within. Thus, given $h \in H$, suppose that $g, g' \in G$ are such that $\phi(g) = h$ and $\phi(g') = h$. We want to check that $\psi(g) = \psi(g')$ in such a case. But since $\phi(g) = \phi(g')$ we have $\phi(g^{-1}g') = 1$ so $g^{-1}g' \in \mathrm{Ker}(\phi)$ and so $g^{-1}g' \in \mathrm{Ker}(\psi)$. Thus $\psi(g^{-1}g') = 1$ so $\psi(g)^{-1}\psi(g') = \psi(g^{-1}g') = 1$ so $\psi(g) = \psi(g')$, as desired. Now, clearly $\psi = \psi' \circ \phi$ by construction, and it is left to check that ψ' is a homomorphism of groups. Let $h_1, h_2 \in H$; we want to check that $\psi'(h_1h_2) = \psi'(h_1)\psi'(h_2)$. Choose $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Then $\psi'(h_1) = \psi(g_1)$ and $\psi'(h_2) = \psi(g_2)$. Moreover, since $\phi(g_1g_2) = h_1h_2$, we have also $\psi'(h_1h_2) = \psi(g_1g_2)$. Hence

$$\psi'(h_1h_2) = \psi(g_1g_2) = \psi(g_1)\psi(g_2) = \psi'(h_1)\psi'(h_2),$$

as desired. □

Corollary 4.6. *Let G, H and K be groups and let $\phi : G \to H$ and $\psi : G \to K$ be epimorphism of groups. Suppose that $\mathrm{Ker}(\phi) = \mathrm{Ker}(\psi)$. Then there exists a unique isomorphism of groups $\alpha : H \to K$ such that $\psi = \alpha \circ \phi$.*

Proof. By Proposition 4.5, there exists a unique homomorphism of groups $\alpha : H \to K$ such that $\psi = \alpha \circ \phi$. The question is whether this α is an isomorphism of groups. Notice, however, that by reversing the roles of H and K, we also obtain that there exists a unique homomorphism of groups $\beta : K \to H$ such that $\phi = \beta \circ \psi$. We claim that α and β are mutually inverse, which will show that α is an isomorphism of groups. To that end, notice that $(\alpha \circ \beta) \circ \psi = \psi$. Since ψ is surjective, this implies $\alpha \circ \beta = \mathrm{id}_K$. Completely analogously we obtain $\beta \circ \alpha = \mathrm{id}_H$, as desired. □

Corollary 4.6 explains that if we study groups equipped with epimorphisms from G, those with the same kernel are "the same", in the sense that there exists a unique isomorphism between them which is compatible with the epimorphisms. It is natural now to ask whether given a subgroup of G, there exists an epimorphism from G whose kernel is that subgroup. The answer, in general, is no, because we notice the following:

Lemma 4.7. *Let G and H be groups, and let $\phi : G \to H$ be a homomorphism of groups. Then given $g \in G$ and $k \in \mathrm{Ker}(\phi)$, we have $gkg^{-1} \in \mathrm{Ker}(\phi)$.*

Proof. We have $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g)^{-1} = \phi(g)1\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = 1$. □

Definition 4.8. Let G be a group and let $K \subset G$ be a subgroup. We say that K is a **normal subgroup** in G if for all $g \in G$ and $k \in K$ we have $gkg^{-1} \in K$.

Exercise 4.2. *Let G be a group and let $K \subset G$ be a subgroup. Show that K is a normal subgroup in G if and only if $gKg^{-1} = K$ for all $g \in G$.*

Exercise 4.3. *Let G be a group and let $K \subset G$ be a subgroup. Show that K is a normal subgroup in G if and only if $gK = Kg$ for all $g \in G$.*

Remark 4.9. One should be a little careful. For example, we can have situations when $gKg^{-1} \subset K$ but $gKg^{-1} \neq K$. An example is given as follows. Let $G := S(\mathbb{Z})$ and let $K := \{g \in G \mid g(x) = x \ \forall x \in \mathbb{Z}_{\geq 0}\}$. Let $g \in G$ be given by $g(x) := x - 1$. Then $gKg^{-1} \subset K$ and $gKg^{-1} \neq K$.

Remark 4.10. In an abelian group, all subgroups are normal.

Example 4.11. *If in S_n we consider the subgroups $H_i := \{\sigma \in S_n \mid \sigma(i) = i\}$. Given $\tau \in S_n$, notice that $\tau H_i \tau^{-1} = H_{\tau(i)}$. In particular, each H_i is not normal in G.*

Let now G be a group and let $K \subset G$ be a normal subgroup. We ask whether there exists a surjective homomorphism of groups from G whose kernel is K. The answer this time is yes. To understand what should be the target group, let us imagine we have such a homomorphism $\phi : G \to H$. If we define an equivalence relation on G by $g_1 \sim g_2$ if $\phi(g_1) = \phi(g_2)$, then we have a bijection $G/\sim \to H$ given by sending the equivalence class of g to $\phi(g)$. Now, notice that $g_1 \sim g_2$, i.e. $\phi(g_1) = \phi(g_2)$, happens if and only if $\phi(g_2^{-1}g_1) = 1$, i.e. $g_2^{-1}g_1 \in K$, or $g_1K = g_2K$. Therefore, the equivalence classes of $\sim$ are in fact left cosets of K in G (or right cosets of K in G - these are the same as K is a normal subgroup in G). Therefore, we have a bijection between G/K and H, given by sending gK to $\phi(g)$. If we use this bijection to construct a binary operation on G/K using that on H, we see that this binary operation is simply the one sending (g_1K, g_2K) to g_1g_2K. We come to the following definition:

Definition 4.12. Let G be a group and let $K \subset G$ be a normal subgroup. Define an operation $G/K \times G/K \to G/K$ by sending $(g_1K, g_2K) \mapsto g_1g_2K$ for $g_1, g_2 \in G$. Notice that this is well-defined; if for $g_1', g_2' \in G$ we have $g_1'K = g_1K$ and $g_2'K = g_2K$, then

$$g_1'g_2'K = g_1'g_2K = g_1'Kg_2 = g_1Kg_2 = g_1g_2K.$$

One checks easily that G/K together with this operation forms a group. This group is called the **quotient group of G by K**. We have an epimorphism $G \to G/K$ given by $g \mapsto gK$, called the **canonical quotient map**. The kernel of this epimorphism is equal to K.

Remark 4.13. Thus, given a group G and a subgroup $H \subset G$, we have the set G/H, and if H is normal in G then this set has in addition a natural structure of a group.

Remark 4.14. Given a group G and subsets $S, T \subset G$, let us denote by $S \cdot T \subset G$ the subset

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

Then if $K \subset G$ is a normal subgroup, we easily see that $(g_1K) \cdot (g_2K) = g_1g_2K$. In other words, the multiplication of cosets in the definition of the quotient group can be thought of using this operation of term-wise multiplication of subsets.

Example 4.15. *In fact, one of our first examples of a group, $\mathbb{Z}_n$, was precisely constructed as a quotient group! Namely, we have the subgroup $\langle n \rangle \subset \mathbb{Z}$ (which is normal since all subgroups in an abelian group are normal), and - go over the definitions and verify! - $\mathbb{Z}_n$ was defined as the quotient group $\mathbb{Z}/\langle n \rangle$.*

Example 4.16. *Another simple example of a quotient group is $\mathbb{R}/\mathbb{Z}$. It is the group of "real numbers modulo 1". Namely, informally, we identify two real numbers if their difference is an integer.*

Remark 4.17. Let us repeat yet differently. Let G be a group, let X be a set and let $\phi : G \to X$ be a surjective map. Then (a very easy exercise!) there exists at most one structure of a group on X (i.e. a binary operation satisfying the group axioms) for which ϕ is a group homomorphism. Let us temporarily say that ϕ is good if such a structure exists. Let now $H \subset G$ be a subgroup. Then (an exercise) the map $\phi : G \to G/H$ given by $g \mapsto gH$ is good if and only if H is normal in G.

Theorem 4.18 (The first isomorphism theorem)**.** *Let G and H be groups and let $\phi : G \to H$ be a homomorphism of groups. Then we have an isomorphism of groups*

$$G/\mathrm{Ker}(\phi) \xrightarrow{\sim} \mathrm{Im}(\phi)$$

given by sending $g\mathrm{Ker}(\phi) \mapsto \phi(g)$.

Proof. We consider the surjective homomorphism of groups $\phi' : G \to \mathrm{Im}(\phi)$ which is simply gotten from ϕ by restricting the codomain. The kernel of this homomorphism is $\mathrm{Ker}(\phi)$. On other hand, we have the surjective homomorphism of groups $p : G \to G/\mathrm{Ker}(\phi)$ which is the canonical projection. The kernel of p is also $\mathrm{Ker}(\phi)$. By Corollary 4.6 there exists a unique isomorphism of groups $\alpha : G/\mathrm{Ker}(\phi) \xrightarrow{\sim} \mathrm{Im}(\phi)$ satisfying $\alpha \circ p = \phi'$. In other words, for every $g \in G$ we have $\alpha(g\mathrm{Ker}(\phi)) = (\alpha \circ p)(g) = \phi'(g) = \phi(g)$, as claimed. □

Example 4.19. *We can reformulate the proof of the main proposition on cyclic groups. Let G be a cyclic group, and let $g \in G$ be a generator, i.e. $G = \langle g \rangle$. We have a homomorphism $\phi : \mathbb{Z} \to G$ given by $n \mapsto g^n$. Notice that ϕ is surjective since g is a generator of G. There exists a unique $m \in \mathbb{Z}_{\geq 0}$ such that $\mathrm{Ker}(\phi) = \langle m \rangle$. Then by the first isomorphism theorem we obtain an*

isomorphism $\mathbb{Z}/\langle m\rangle \xrightarrow{\sim} G$*, given by sending* $n + \langle m\rangle$ *to* g^n*. One can notice now that* $m = 0$ *means that* g *has infinite order, and then, composing with the isomorphism* $\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/\langle 0\rangle$ *given by sending* $n \mapsto n + \langle 0\rangle$*, we obtain an isomorphism* $\mathbb{Z} \xrightarrow{\sim} G$ *given by sending* $n \mapsto g^n$*. If* $m \neq 0$*, then* m *is the order of* g*.*

Example 4.20. *Next, we can define the "angle isomorphism". We have a homomorphism* $\mathbb{R} \to \mathrm{SO}(2)$ *given by sending*

$$x \mapsto \begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix}.$$

This homomorphism is surjective, and its kernel is $2\pi\mathbb{Z}$*. Hence, we obtain an isomorphism*

$$\mathbb{R}/2\pi\mathbb{Z} \xrightarrow{\sim} \mathrm{SO}(2)$$

given by sending

$$x + 2\pi\mathbb{Z} \mapsto \begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix}.$$

In other words, rotations in the plane can be identified, as a group, with real numbers up to addition of an integer multiple of 2π*.*

Example 4.21. *Let* G *be a group. Given* $g \in G$*, let us denote by* $\alpha_g : G \to G$ *the map given by* $\alpha_g(g') := gg'g^{-1}$*. Check that* α_g *is an automorphism of* G*, i.e.* $\alpha_g \in \mathrm{Aut}(G)$*. Then, check that the map* $\mathrm{inn} : G \to \mathrm{Aut}(G)$ *given by* $g \mapsto \alpha_g$ *is a homomorphism. Let us denote by* $\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$ *the image of* inn*. Automorphisms of* G *which lie in* $\mathrm{Inn}(G)$ *are called* ***inner automorphisms*** *of* G*. Show that the kernel of* inn *is* $Z(G)$*, the center of* G*. We obtain an isomorphism* $G/Z(G) \xrightarrow{\sim} \mathrm{Inn}(G)$*, sending* $gZ(G)$ *to* α_g*.*

4.3 The correspondence theorem

Informally, all the information about a quotient group is contained inside the original group - of course, as it was constructed from it. Thus, we should be able to answer questions such as "what subgroups does our quotient group has" in terms of the original group. We will now formalize a claim along those lines.

Recall that given sets X, Y and a map $\phi : X \to Y$ we have two operations. Given a subset $S \subset X$, we define a subset $\phi(S) \subset Y$ by $\phi(S) := \{\phi(x) \,:\, x \in S\}$. Given a susbet $T \subset Y$ we define a subset $\phi^{-1}(T) \subset X$ by $\phi^{-1}(T) := \{x \in X \mid \phi(x) \in Y\}$. Given groups G, H and a homomorphism of groups $\phi : G \to H$, a very simple exercise shows that if $L \subset G$ is a subgroup then $\phi(L) \subset H$ is a subgroup and if $M \subset H$ is a subgroup then $\phi^{-1}(M) \subset G$ is a subgroup.

Given a group G, let us denote by Sgrp_G the set of subgroups of G.

Theorem 4.22 (The correspondence thoerem)**.** *Let* G *and* H *be groups and let* $\phi : G \to H$ *be an epimorphism.*

1. *We have mutually inverse bijections*

$$\phi^{-1}(-) : \mathrm{Sgrp}_H \rightleftarrows \{L \in \mathrm{Sgrp}_G \mid \mathrm{Ker}(\phi) \subset L\} : \phi(-).$$

2. *Given $M_1, M_2 \in \mathrm{Sgrp}_H$, we have $\phi^{-1}(M_1) \subset \phi^{-1}(M_2)$ if and only if $M_1 \subset M_2$.*

3. *Given $M \in \mathrm{Sgrp}_H$, we have a bijection*

$$\gamma_M : G/\phi^{-1}(M) \to H/M$$

given by sending $g\phi^{-1}(M) \mapsto \phi(g)M$. In particular,

$$[G : \phi^{-1}(M)] = [H : M].$$

4. *Given $M \in \mathrm{Sgrp}_H$, M is a normal subgroup in H if and only if $\phi^{-1}(M)$ is a normal subgroup in G.*

5. *(Third isomorphism theorem) Given $M \in \mathrm{Sgrp}_H$, and assuming that M is normal in H, the bijection γ_M of the previous item is in fact an isomorphism of groups.*

Proof.

1. Notice that clearly, given $M \in \mathrm{Sgrp}_H$, we have $\mathrm{Ker}(\phi) = \phi^{-1}(1) \subset \phi^{-1}(M)$. Therefore the map from left to right is well-defined. Now we want to check that the two maps are mutually inverse. Given $M \in \mathrm{Sgrp}_H$, we want to check that $\phi(\phi^{-1}(M)) = M$. This is immediate from ϕ being surjective. Also, given $L \in \mathrm{Sgrp}_G$ satisfying $\mathrm{Ker}(\phi) \subset L$, we want to check that $\phi^{-1}(\phi(L)) = L$. Clearly $L \subset \phi^{-1}(\phi(L))$. Let us see that $\phi^{-1}(\phi(L)) \subset L$. Let $g \in \phi^{-1}(\phi(L))$. Then $\phi(g) = \phi(l)$ for some $l \in L$. Hence $\phi(gl^{-1}) = 1$, i.e. $gl^{-1} \in \mathrm{Ker}(\phi)$ and hence $g \in \mathrm{Ker}(\phi)l \subset L$.

2. This is clear since ϕ is surjective.

3. First, we need to check that the map γ_M is well-defined. In other words, given $g_1, g_2 \in G$ such that $g_1\phi^{-1}(M) = g_2\phi^{-1}(M)$, we want to check that $\phi(g_1)M = \phi(g_2)M$. The former is equivalent to $g_2^{-1}g_1 \in \phi^{-1}(M)$, implying $\phi(g_2^{-1}g_1) \in M$, i.e. $\phi(g_2)^{-1}\phi(g_1) \in M$, which is equivalent to the latter. Next, we want to check that γ_M is injective; given $g_1, g_2 \in G$ such that $\phi(g_1)M = \phi(g_2)M$, we want to see that $g_1M = g_2M$. Again, the former is equivalent to $\phi(g_2^{-1}g_1) \in M$, which is the same as $g_2^{-1}g_1 \in \phi^{-1}(M)$, which is equivalent to the latter. Finally, we want to see that γ_M is surjective; this is immediate.

4. Suppose that M is normal in H. Let $g \in G$ and $l \in \phi^{-1}(M)$. Then

$$\phi(glg^{-1}) = \phi(g)\phi(l)\phi(g)^{-1} \in \phi(g)M\phi(g)^{-1} = M$$

so $glg^{-1} \in \phi^{-1}(m)$, showing that $\phi^{-1}(M)$ is normal in G. Conversely, suppose that $\phi^{-1}(M)$ is normal in G. Let $h \in H$ and $m \in M$. Fix $g \in G$ such that $\phi(g) = h$ and fix $l \in \phi^{-1}(M)$ such that $\phi(l) = m$ (which are possible since ϕ is surjective). Then $hmh^{-1} = \phi(g)\phi(l)\phi(g)^{-1} = \phi(glg^{-1}) \in \phi(\phi^{-1}(M)) = M$, showing that M is normal in H.

5. We just need to see that γ_M is a homomorphism of groups. Given $g_1, g_2 \in G$, we want to check that

$$\gamma_M(g_1\phi^{-1}(M) \cdot g_2\phi^{-1}(M)) = \gamma_M(g_1\phi^{-1}(M)) \cdot \gamma_M(g_2\phi^{-1}(M)).$$

The left hand side is equal to $\gamma_M(g_1g_2\phi^{-1}(M)) = \phi(g_1g_2)M$ and the right hand side is $\phi(g_1)M \cdot \phi(g_2)M = \phi(g_1)\phi(g_2)M$, so these are indeed equal.

□

Remark 4.23. Usually one formulates the previous theorem taking H to be G/K for some normal subgroup $K \subset G$ (and $\phi : G \to G/K$ the canonical quotient map). Then, denoting by $\phi : G \to G/K$ the canonical quotient map, given a subgroup $L \subset G$, we have $\phi(L) = L/K$. Then, if L is normal in G, item 5 gets the suggestive form

$$G/L \cong (G/K)/(L/K)$$

(i.e. K "cancels out").

Example 4.24. *Given $n \in \mathbb{Z}_{\geq 1}$, we found previously what subgroups $\mathbb{Z}_n$ has. Let us re-establish it using the correspondence theorem (by recalling that $\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$). We obtain that there is a bijection between the set of subgroups of $\mathbb{Z}_n$ and the set of subgroups of $\mathbb{Z}$ containing $\langle n \rangle$. Given $m \in \mathbb{Z}_{\geq 0}$, we notice that $\langle n \rangle \subset \langle m \rangle$ if and only if $m|n$. Thus, the subgroups of $\mathbb{Z}_n$ are in correspondence with number $m \in \mathbb{Z}_{\geq 1}$ which divide n. Given such m, the subgroup of $\mathbb{Z}_n$ corresponding to m is $\mathrm{pr}_n(\langle m \rangle) = \langle \mathrm{pr}_n(m) \rangle = \langle [m]_n \rangle$, where we again denote by $\mathrm{pr}_n : \mathbb{Z} \to \mathbb{Z}_n$ the canonical quotient map.*

4.4 The second isomorphism theorem

Let us recall that given a group G and subset $S, T \subset G$, we denote

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

Claim 4.25 (Second isomorphism theorem)**.** *Let G be a group, let $K \subset G$ be a normal subgroup and let $H \subset G$ be a subgroup. Then $HK = KH$, and HK is a subgroup in G, K is normal in HK, $K \cap H$ is normal in H, and we have an isomorphism of groups*

$$H/(K \cap H) \to HK/K$$

given by $h(K \cap H) \mapsto hK$.

Proof. Left as an exercise. □

Example 4.26. *Let us denote by $E_n \subset \mathrm{GL}_n(\mathbb{C})$ the subgroup of scalar matrices. We have an isomorphism*

$$\mathbb{C}^\times \xrightarrow{\sim} E_n,$$

given by sending c to the diagonal matrix all of whose entries are equal to c. One sets

$$\mathrm{PGL}_n(\mathbb{C}) := \mathrm{GL}_n(\mathbb{C})/E_n$$

*(it is called the **projective general linear group**). We have the normal subgroup $\mathrm{SL}_n(\mathbb{C}) \subset \mathrm{GL}_n(\mathbb{C})$ (it is the kernel of the determinant homomorphism). Notice that $E_n\mathrm{SL}_n(\mathbb{C}) = \mathrm{GL}_n(\mathbb{C})$ (i.e. every invertible matrix can be written as a matrix with determinant 1 multiplied by a scalar matrix (here it is essential that $\mathbb{C}$ is algebraically closed). Therefore, by the second isomorphism theorem we obtain an isomorphism of groups*

$$\mathrm{SL}_n(\mathbb{C})/(E_n \cap \mathrm{SL}_n(\mathbb{C})) \xrightarrow{\sim} \mathrm{PGL}_n(\mathbb{C}).$$

Notice also that, denoting by $\mu_n \subset \mathbb{C}^\times$ the subgroup consisting of n-th roots of unity, i.e. of $c \in \mathbb{C}^\times$ satisfying $c^n = 1$, we have an isomorphism

$$\mu_n \xrightarrow{\sim} E_n \cap \mathrm{SL}_n(\mathbb{C}),$$

given by sending c to the diagonal matrix all of whose entries are equal to c.

4.5 The strategy of classifying groups

How to find all possible groups? One approach is "divide and conquer". Namely, let us say that a group G is "glued" from a pair of groups (H, K) if there exist a normal subgroup $K' \subset G$ and isomorphisms of K' with K and of G/K' with H. One can then hope to break the question of what groups are there into two questions: What groups are there that can not be "glued" non-trivially, and given a pair of groups (H, K), what ways are there to "glue" them.

The precise formulation of the first question is as follows. We say that a group is trivial if it consists of only one element. Of course, there is a unique isomorphism between any two trivial groups, so that one can effectively talk about the trivial group. Notice that, in the above notation, if H is the trivial group, then $K' = G$ so that G is isomorphic to K, while if K is the trivial group then $K = \{1\}$ so that G is isomorphic to H. Hence, a "non-trivial" gluing should mean that neither H nor K are the trivial group. We come to the following basic definition:

Definition 4.27. A group G is called **simple** if G is not the trivial group and there are no normal subgroups in G except $\{1\}$ and G.

Thus, informally, simple groups are the groups which can not be "glued" non-trivially from smaller groups.

Question 4.28. Can we classify all simple finite groups?

According to Wikipedia, the classification of simple finite groups was obtained by more than 100 authors, across tens of thousands of pages, mostly between the years 1955 and 2004.

Example 4.29. *Given a prime $p \in \mathbb{Z}_{\geq 1}$, the cyclic group of order p (i.e., up to isomorphism, $\mathbb{Z}_p$) is simple.*

Example 4.30. *We will later learn that S_n, for $n \in \mathbb{Z}_{\geq 5}$, has a unique subgroup of index 2, denoted A_n (the **alternating group**), and A_n is simple.*

Example 4.31. *Let $q \in \mathbb{Z}_{\geq 4}$ be the power of a prime number. Let F be a field with q elements. Let $n \in \mathbb{Z}_{\geq 2}$. We have the group $\mathrm{SL}_n(F)$ of n by n matrices over F with determinant 1 (where the group operation is multiplication of matrices). It is called the **special linear group**. One can see that $Z(\mathrm{SL}_n(F))$ consists of scalar matrices with entry $\alpha \in F^\times$, with $\alpha^n = 1$. One defines $\mathrm{PSL}_n(F) := \mathrm{SL}_n(F)/Z(\mathrm{SL}_n(F))$. This is called the **projective special linear group**. One can see that $\mathrm{PSL}_n(F)$ is simple.*

Example 4.32. *There are other finite simple groups which come in families, similarly to the previous example, i.e. as, roughly, groups of matrices over finite fields satisfying various conditions (such groups are called **finite groups of Lie type**).*

Example 4.33. *Except the above (roughly) mentioned examples, there are 26 more finite simple groups, known as the **sproadic groups**. The one with the highest order is known as the **monster group**. It has order*

$$808017424794512875886459904961710757005754368000000000.$$

4.6 Semi-direct products

Let us now provide a way of gluing a group from two smaller groups, i.e. trying to say something in the direction of the second question above. So let K and H be two groups.

First, the simplest option for "gluing" is that of the **direct product**. Consider $G := K \times H$. We can denote

$$K' := \{(k, 1) \ : \ k \in K\} \subset K \times H.$$

Then of course we have an isomorphism $K \xrightarrow{\sim} K'$ given by $k \mapsto (k, 1)$. And we have an epimorphism $K \times H \to H$ given by $(k, h) \mapsto h$ which has kernel K', and therefore we obtain an isomorphism $(K \times H)/K' \xrightarrow{\sim} H$. In other words, indeed $K \times H$ is "glued" from (H, K). That was an "outer" construction of direct products. There is also an "inner" description of what direct products are:

Lemma-Definition 4.34. *Let G be a group. Let $H, K \subset G$ be two subgroups. We say that G is the **direct product** of H and K if (here conditions 3 and 3' are equivalent, given conditions 1 and 2):*

1. *$H \cap K = \{1\}$.*
2. *$KH = G$.*
3. *$hk = kh$ for all $h \in H$ and $k \in K$.*
3' *H is normal in G and K is normal in G.*

In such a case, we have an isomorphism of groups $K \times H \xrightarrow{\sim} G$ given by $(k, h) \mapsto kh$.

Proof. Given 1 and 2, let us suppose that 3 holds and show that 3' holds. Let $h \in H$ and $g \in G$; we want to show that $ghg^{-1} \in H$ - this will show that H is normal in G, and the proof that K is normal in G is analogous. Since $G = KH$ we can write $g = kh'$ for some $k \in K$ and $h' \in H$. Then

$$ghg^{-1} = (kh')h(kh')^{-1} = kh'h(h')^{-1}k^{-1} = h'h(h')^{-1}kk^{-1} = h'h(h')^{-1} \in H.$$

Conversely, given 1 and 2, let us suppose that 3' holds and show that 3 holds. Let $h \in H$ and $k \in K$. The equality $hk = kh$ is equivalent to the equality $h^{-1}k^{-1}hk = 1$. Notice that $k^{-1}hk \in H$ and therefore $h^{-1}k^{-1}hk \in H$. On the other hand, we also have $h^{-1}k^{-1}h \in K$ and therefore $h^{-1}k^{-1}hk \in K$. Therefore $h^{-1}k^{-1}hk \in H \cap K = \{1\}$ i.e. $h^{-1}k^{-1}hk = 1$, as desired. Finally, that the map $K \times H \to G$ described is an isomorphism is straight-forward, we leave it to the reader. □

However, there is a more sophisticated way of "gluing", the **semi-direct product** (it is more sophisticated than the direct product, but still it does not describe the general case). Its "inner" description is as follows:

Lemma-Definition 4.35. *Let G be a group. Let $H, K \subset G$ be two subgroups. We say that G is the **semi-direct product** of H and K if:*

1. *$H \cap K = \{1\}$.*
2. *$KH = G$.*
3. *K is normal in G.*

In such a case, the composite homomorphism $H \xrightarrow{i} G \xrightarrow{p} G/K$ is an isomorphism, where i is the inclusion of H in G and p is the canonical projection map. So, G is "glued" from (H, K).

Proof. It is straight-forward to see that condition 1 shows that $p \circ i$ is injective, while condition 2 shows that $p \circ i$ is surjective, and so $p \circ i$ is an isomorphism. □

Example 4.36. *Let us consider D_n, denoting by $r \in D_n$ an element generating the subgroup of rotations and by $s \in D_n$ an element not in $\langle r \rangle$. Then D_n is the semi-direct product of $\langle s \rangle = \{1, s\}$ and $\langle r \rangle = \{1, r, \ldots, r^{n-1}\}$.*

What will be an "outer" description of semi-direct products? Given G which is the semi-direct product of its two subgroups H and K, notice that every element in G can be written uniquely as kh for $k \in K$ and $h \in H$. What happens if we want to multiply two such elements? We have

$$(k_1h_1)(k_2h_2) = (k_1h_1k_2h_1^{-1})(h_1h_2)$$

(recall that $h_1k_2h_1^{-1} \in K$ as K is normal in G). Thus, if we want some "outer" description, we need to artificially introduce the information of $\alpha : H \times K \to K$ given by $(h, k) \mapsto hkh^{-1}$. In fact, one checks that this map has the following properties: It is an action of H on K and, moreover, for every $h \in H$, the map $K \to K$ given by $k \mapsto \alpha(h, k)$ is a group automorphism of K.

Definition 4.37. Let H and K be groups. An action $\alpha : H \times K \to K$ of H on K is said to be an **action by group automorphisms** if for every $h \in H$, the map $K \to K$ given by $k \mapsto \alpha(h, k)$ is a group automorphism of K.

Now we can describe the "outer" notion of semi-direct products:

Lemma-Definition 4.38. *Let H and K be groups and let $\alpha : H \times K \to K$ be an action of H on K by group automorphisms. We define a group $K \rtimes_\alpha H$ as follows. As a set, it is $K \times H$. The group operation is:*

$$(k_1, h_1)(k_2, h_2) := (k_1\alpha(h_1, k_2), h_1h_2).$$

If we denote by $K' \subset K \rtimes_\alpha H$ the subgroup given by

$$K' := \{(k, 1) \ : \ k \in K\}$$

then we have an isomorphism $K \xrightarrow{\sim} K'$ given by $k \mapsto (k, 1)$, the map $p : K \rtimes_\alpha H \to H$ given by $(k, h) \mapsto h$ is an epimorphism, the map $H \to K \rtimes_\alpha H$ given by $h \mapsto (1, h)$ is a monomorphism, and the composite $p \circ i : H \to (K \rtimes_\alpha H)/K'$ is an isomrophism, so that $K \rtimes_\alpha H$ is "glued" from (H, K).

Example 4.39. *Let k be a field. There is an action α of $k^\times$ on k by group automorphisms, given by $a * b := ab$. The corresponding semi-direct product $k \rtimes_\alpha k^\times$ is called the **affine group**, or **ax+b** group. Why the latter name? Let us associate to $(b, a) \in k \rtimes_\alpha k^\times$ the function $f_{(b,a)} : k \to k$ given by $x \mapsto ax + b$. Then given another pair $(b', a') \in k \rtimes_\alpha k^\times$ we have*

$$(b, a)(b', a') = (b + ab', aa')$$

and so we have

$$(f_{(b,a)} \circ f_{(b',a')})(x) = f_{(b,a)}(f_{(b',a')}(x)) = f_{(b,a)}(a'x + b') = a(a'x + b') + b =$$

$$= aa'x + ab' + b = f_{(b+ab',aa')}(x) = f_{(b,a)(b',a')}(x),$$

i.e. $k \rtimes_\alpha k^\times$ *is an abstract incarnation of the totality of affine-linear maps* $k \to k$. *There is another realization of this group. Let us consider*

$$H_k := \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \ : \ a \in k^\times, b \in k \right\} \subset \mathrm{GL}_2(k).$$

Then the map

$$k \rtimes_\alpha k^\times$$

given by

$$(b, a) \mapsto \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

is in fact a group isomorphism.

Example 4.40. *Let us denote by* $C_2 := \{1, s\}$ *a group with two elements. Given an abelian group* K *(we use multiplicative notation in* K*), we can consider the action* α *of* C_2 *on* K *by group automorphisms, determined by* $\alpha(s, k) := k^{-1}$. *Let us (just for the sake of this example) denote by* $D(H)$ *the semi-direct product* $K \rtimes_\alpha C_2$. *Then, see if you understand, that we have an isomorphism of* $D(\mathbb{Z}_n)$ *with the dihedral group* D_n.

Remark 4.41. Given an action of a group G on a set X, recall that it is encoded as a map $a : G \times X \to X$ satisfying some properties, but it can also be encoded as a group homomorphism $\rho : G \to S(X)$. Given groups G and H, we notice that given an action $a : G \times H \to H$ of G on H, and denoting by $\rho : G \to S(H)$ the corresponding group homomorphism, the action is by group automorphisms if and only if $\rho(g) \in \mathrm{Aut}(H)$ for all $g \in G$, i.e. if and only if the image of ρ lies in the subgorup $\mathrm{Aut}(H) \subset S(H)$. In other words, we have a bijection between actions of G on H by group automorphisms and group homomorphisms $G \to \mathrm{Aut}(H)$.

5 The symmetric group

Throughout this section, $n \in \mathbb{Z}_{\geq 1}$ is a fixed number. Let us also denote $[n] := \{1, \ldots, n\}$. There is the following notation for permutations: Given $\sigma \in S_n$, one denotes

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

5.1 Cycles

Definition 5.1. Given $1 \leq p \leq n$ and $(i_1, \ldots, i_p) \in [n]^p$ such that $i_r \neq i_s$ whenever $r \neq s$. One denotes by

$$(i_1, i_2, \cdots, i_p) \in S_n$$

the permutation which sends i_r to i_{r+1} for $1 \leq r \leq p-1$, sends i_p to i_1, and sends j to j for every $j \in [n]$ such that $j \neq i_r$ for all $1 \leq r \leq p$. Such a permutation is called a **cycle** (**of length** p).

Exercise 5.1. *Show that the order of a cycle of length p is p.*

Definition 5.2. Let $\sigma, \tau \in S_n$. We say that σ and τ are **disjoint** if for every $1 \leq p \leq n$, if $\sigma(p) \neq p$ then $\tau(p) = p$ and if $\tau(p) \neq p$ then $\sigma(p) = p$.

Example 5.3. *Two cycles $(i_1, i_2, \cdots, i_p)$ and $(j_1, j_2, \cdots, j_q)$ are disjoint if and only if $i_r \neq j_s$ for all $1 \leq r \leq p$ and $1 \leq s \leq q$.*

Definition 5.4. Elements g_1, g_2 in a group are said to **commute** if $g_1 g_2 = g_2 g_1$.

Lemma 5.5. *Let $\sigma, \tau \in S_n$ be disjoint. Then σ and τ commute.*

Proof. Let $i \in [n]$, we want to show that $(\sigma \circ \tau)(i) = (\tau \circ \sigma)(i)$. Suppose that $\sigma(i) \neq i$. Then $\tau(i) = i$. Also, $\sigma(\sigma(i)) \neq \sigma(i)$ and hence $\tau(\sigma(i)) = \sigma(i)$. Therefore, $(\sigma \circ \tau)(i) = \sigma(i)$ and $(\tau \circ \sigma)(i) = \sigma(i)$, and so $(\sigma \circ \tau)(i) = (\tau \circ \sigma)(i)$. Another case is when $\tau(i) \neq i$, and one shows in this case analogously that $(\sigma \circ \tau)(i) = (\tau \circ \sigma)(i)$. Finally, if both of these cases do not hold, so $\sigma(i) = i$ and $\tau(i)$, then clearly $(\sigma \circ \tau)(i) = i$ and $(\tau \circ \sigma)(i) = i$, so also in this case we have $(\sigma \circ \tau)(i) = (\tau \circ \sigma)(i)$. □

Definition 5.6. Let G be a group and let $S \subset G$ be a finite set of elements, such that every two elements in S commute. Then given any two orderings $g_1, \ldots, g_m$ and $g'_1, \ldots, g'_m$ of the elements of S, we have $g_1 \cdot \ldots \cdot g_m = g'_1 \cdot \ldots \cdot g'_m$. We denote the resulting common value by $\prod_{g \in S} g$.

Proposition-Definition 5.7 (Cycle decomposition)**.** *Let $\sigma \in S_n$. There exists a unique subset $C(\sigma) \subset S_n$ consisting of pairwise disjoint cycles such that $\sigma = \prod_{\tau \in C(\sigma)} \tau$.*

Proof. We omit the proof, it is a straight-forward generalization of the illustration in the next example (which I will explain in person). □

Example 5.8. *We have*

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

5.2 Conjugacy in the symmetric group

Exercise 5.2. *Let us consider a transposition $(i_1, \ldots, i_p) \in S_n$ and a permutation $\sigma \in S_n$. Then*

$$\sigma(i_1, \ldots, i_p)\sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_p)).$$

Proposition 5.9. *Let $\sigma, \tau \in S_n$. Then σ and τ are conjugate in S_n if and only if for every $p \in \mathbb{Z}_{\geq 2}$, the number of cycles in $C(\sigma)$ of length p is equal to the number of cycles in $C(\tau)$ of length p (let us say in such a case that σ and τ have the same cycle structure).*

Proof. If we write $\sigma \in S_n$ as a product of cycles $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_m$ and $\omega \in S_n$, then $\omega\sigma\omega^{-1} = (\omega\sigma_1\omega^{-1}) \cdot \ldots \cdot (\omega\sigma_m\omega^{-1})$ and Exercise 5.2 shows that $\omega\sigma_i\omega^{-1}$ is a cycle which has the same length as the cycle σ_i. Furthermore, it is immediate from Exercise 5.2 that for $i \neq j$ the cycles $\omega\sigma_i\omega^{-1}$ and $\omega\sigma_j\omega^{-1}$ are disjoint. Hence we showed one direction - that conjugate permutations have the same cycle structure. For the converse, let us just give an example (the proof in general is a straight-forward generalization of the illustration provided by that example, which I will explain in person). In S_7, let us consider $\sigma = (126)(37)$ and $\tau = (274)(56)$. Then we match terms, and define

$$\omega := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 5 & 1 & 3 & 4 & 6 \end{pmatrix}.$$

Then $\omega\sigma\omega^{-1} = \tau$. □

Remark 5.10. For example, what are the conjugacy classes in S_5? We can parametrize them as follows:

$$(\bullet\bullet\bullet\bullet\bullet),\ (\bullet\bullet\bullet\bullet\bullet),\ (\bullet\bullet\bullet)(\bullet\bullet),\ (\bullet\bullet\bullet),\ (\bullet\bullet)(\bullet\bullet),\ (\bullet\bullet),\ \mathrm{id}.$$

For example, some of the permutations that belong to the conjugacy class depicted as $(\bullet\bullet\bullet)(\bullet\bullet)$ are:

$$(123)(45),\ (234)(15),\ (152)(34),\ \ldots$$

Remark 5.11. A **partition** of n is a sequence $(n_1, n_2, \ldots,)$ of numbers in $\mathbb{Z}_{\geq 0}$ such that

$$1 \cdot n_1 + 2 \cdot n_2 + \ldots = n.$$

Let us denote by $p(n)$ the number of partitions of n. Then a corollary of the above proposition is that the number of conjugacy classes in S_n is $p(n)$. This function of n was studied by number theorists. For example, one knows that

$$p(n) \sim \frac{1}{4\sqrt{3}} \frac{e^{\pi\sqrt{2/3}\cdot\sqrt{n}}}{n} \quad \text{as } n \to \infty.$$

5.3 Transpositions

Definition 5.12. A cycle of length 2 is called a **transposition**.

Exercise 5.3. *Notice that every cycle can be expressed as a product of transpositions:*

$$(i_1, \ldots, i_p) = (i_1, i_p) \cdot \cdots \cdot (i_1, i_3) \cdot (i_1, i_2).$$

Corollary 5.13 (Of Exercise 5.3 and Proposition 5.7)**.** *Every permutation in S_n can be written as a product of transpositions. In particular, the group S_n is generated by its subset of transpositions.*

5.4 The sign homomorphism

Let us denote by μ_2 the group consisting of elements 1 and -1, with the group operation being multiplication.

Theorem-Definition 5.14. *For $n \geq 2$, there exists a unique group epimorphism*

$$\mathrm{sgn} : S_n \to \mu_2.$$

It sends transpositions to -1. It is called the ***sign homomorphism****.*

Proof. Let us first establish that given an epimorphism $\mathrm{sgn} : S_n \to \mu_2$, we must have $\mathrm{sgn}(\sigma) = -1$ for every transposition $\sigma \in S_n$. Indeed, if for some transposition $\sigma \in S_n$ we have $\mathrm{sgn}(\sigma) = 1$, then for every $\omega \in S_n$ we have $\mathrm{sgn}(\omega\sigma\omega^{-1}) = 1$ (why?), and so, since every transposition is conjugate to σ we obtain that $\mathrm{sgn}(\tau) = 1$ for every transposition $\tau \in S_n$. From Corollary 5.13 it then follows that $\mathrm{sgn}(\tau) = 1$ for all $\tau \in S_n$, contradicting sgn being surjective.

Let us now establish the uniqueness. In fact, from Corollary 5.13 it is clear in view of the epimorphisms in question taking values -1 on transpositions.

Finally, one needs to establish existence. Let us denote by F the set of functions from $\mathbb{R}^n$ to $\mathbb{R}$. We have an action of S_n on F:

$$(\sigma \bullet f)(x_1, \ldots, x_n) := f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Let us consider the function $D : \mathbb{R}^n \to \mathbb{R}$ given by

$$D(x_1, \ldots, x_n) := \prod_{1 \leq i < j \leq n} (x_j - x_i).$$

Given a subset $S \subset [n]$ such that $|S| = 2$, let us denote by $a(S)$ the minimal element in S and by $z(S)$ the maximal element in S. We can then rewrite

$$D(x_1, \ldots, x_n) = \prod_{S \subset [n], |S|=2} (x_{z(S)} - x_{a(S)}).$$

Let us also, given $S \subset [n]$ such that $|S| = 2$ and $\sigma \in S_n$, denote by $\epsilon_{\sigma,S}$ the number 1 if $\sigma(a(S)) < \sigma(z(S))$ and the number -1 otherwise. Let us notice that, given $\sigma \in S_n$, we have

$$(\sigma \bullet D)(x_1, \ldots, x_n) = \prod_{S \subset [n], |S|=2} (x_{\sigma(z(S))} - x_{\sigma(a(S))}) = \prod_{S \subset [n], |S|=2} \epsilon_{\sigma,S}(x_{z(\sigma(S))} - x_{a(\sigma(S))}) =$$

$$= \left(\prod_{S \subset [n], |S|=2} \epsilon_{\sigma,S} \right) \cdot \left(\prod_{S \subset [n], |S|=2} (x_{z(S)} - x_{a(S)}) \right) = \left(\prod_{S \subset [n], |S|=2} \epsilon_{\sigma,S} \right) \cdot D(x_1, \ldots, x_n).$$

Thus, given $\sigma \in S_n$, we have $\sigma \bullet D \in \{D, -D\}$. Let us define $\mathrm{sgn}(\sigma) \in \mu_2$ to be such that $\sigma \bullet D = \mathrm{sgn}(\sigma) \cdot D$. Then sgn is a group homomorphism: Given $\sigma, \tau \in S_n$ we have

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

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

and therefore

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

A final point to check is that there exists $\sigma \in S_n$ for which $\mathrm{sgn}(\sigma) = -1$. Namely, let us see that $\mathrm{sgn}((1,2)) = -1$. For that, we need to check that, denoting $\sigma := (1,2)$,

$$\prod_{S \subset [n], |S|=2} \epsilon_{\sigma,S} = -1.$$

This is equivalent to

$$\left|\{(i,j) \in [n]^2 \mid \imath < j,\ \sigma(i) > \sigma(j)\}\right|$$

being odd. But we see that the set in question contains precisely one element - the element $(1,2)$. □

Remark 5.15. Thus, a description of $\mathrm{sgn}(\sigma)$ is as follows: Write σ as a product of transpositions $\sigma = \tau_1 \cdot \ldots \cdot \tau_m$. Then $\mathrm{sgn}(\sigma)$ is equal to 1 if m is even and to -1 if m is odd.

Remark 5.16. We see from the proof of Theorem-Definition 5.14 that another description of $\mathrm{sgn}(\sigma)$ is as follows. Consider the number of pairs (i,j) with $i,j \in [n]$ and $i < j$ and $\sigma(i) > \sigma(j)$. Then $\mathrm{sgn}(\sigma)$ is equal to 1 if this number is even and to -1 if this number is odd.

Exercise 5.4. *Here is another description of the sign homomorphism. Consider the group homomorphism*

$$\iota : S_n \to \mathrm{GL}_n(\mathbb{C})$$

defined as follows. Denoting by $\{e_i\}_{1 \le i \le n}$ the standard basis of the space $\mathbb{C}^n$ of column vectors, we set $\iota(\sigma)$ to be the unique matrix satisfying $\iota(\sigma)e_i = e_{\sigma(i)}$ for all $1 \le i \le n$. In other words, $\iota(\sigma)_{j,i}$ is equal to 1 if $\sigma(i) = j$ and to 0 otherwise. Then $\mathrm{sgn}(\sigma) = \det(\iota(\sigma))$ for all $\sigma \in S_n$.

5.5 The alternating group

Definition 5.17. For $n \ge 2$, we denote by A_n the kernel of the epimorphism $\mathrm{sgn} : S_n \to \mu_2$. Thus, A_n is a normal subgroup in S_n, of index 2. It consists of the even permutations.

Lemma 5.18. *A_n is generated by its subset of cycles of length 3.*

Proof. Every element in A_n can be written as a product of an even number of transpositions. Thus, it is enough to show that the product of two transpositions can be written as a product of cycles of length 3. To that end, let us consider a product of two transpositions $\sigma := (i_1 i_2)(j_1 j_2)$. Let us divide into cases according to the size of $\{i_1, i_2\} \cap \{j_1, j_2\}$. If this size is 2, then $\sigma = \mathrm{id}$ (so it is the empty product of cycles of length 3). If this size is 1, say $i_2 = j_2$, then $\sigma = (i_1, i_2, j_1)$. If this size is 0, then $\sigma = (i_1, i_2, j_1)(i_2, j_1, j_2)$. □

Lemma 5.19. *If $n \geq 5$, then all cycles of length 3 are conjugate inside A_n.*

Proof. Let us consider two cycles $\sigma, \tau \in A_n$ of length 3. By Proposition 5.9 they are conjugate in S_n, i.e. there exists $\omega \in S_n$ such that $\tau = \omega\sigma\omega^{-1}$. If ω is even then we are done. Otherwise, since $n \geq 5$ there exist $i_1, i_2 \in [n]$ such that $i_1 \neq i_2$ and $\sigma(i_1) = i_1$ and $\sigma(i_2) = i_2$. Then $(i_1, i_2)\sigma(i_1, i_2)^{-1} = \sigma$ and therefore if we denote $\omega' := \omega \circ (i_1, i_2)$ then we obtain $\omega'\sigma(\omega')^{-1} = \sigma$. Notice that ω' is even, and we are done. □

Theorem 5.20. *If $n \geq 5$, then A_n is a simple group.*

Proof. Let $N \subset A_n$ be a normal subgroup, and assume that $N \neq \{\mathrm{id}\}$. We want to show that $N = A_n$. It is enough to see that N contains a cycle of length 3, because then by Lemma 5.19 it will contain all cycles of length 3, and then by Lemma 5.19 it will be equal to A_n.

Let $\mathrm{id} \neq \sigma \in N$ be a permutation with maximal possible number of fixed points (i.e. $i \in [n]$ satisfying $\sigma(i) = i$). It is enough to see that σ is a cycle of length 3. We will consider several options for $C(\sigma)$. Each time, unless σ is a cycle of length 3, we will come up with a 3-cycle $\tau \in A_n$, denote $\sigma' := \tau\sigma\tau^{-1}\sigma^{-1}$, notice that $\sigma' \in N$ since N is normal in A_n, and check that $\sigma' \neq \mathrm{id}$ and σ' has more fixed points than σ, contradicting the choice of σ. This will finish the proof.

(had some inaccuracies in this part, should complete again sometime... look in a book...)

□

Corollary 5.21. *If $n \geq 5$, then S_n has no normal subgroups except $\{\mathrm{id}\}$, S_n and A_n.*

Proof. Let $N \subset S_n$ be a normal subgroup - we want to see that either $N = \{\mathrm{id}\}$ or $N = S_n$. Consider $N' := N \cap A_n$. Then N' is a normal subgroup in A_n. Hence, since A_n is simple, we have either $N' = \{\mathrm{id}\}$ or $N' = A_n$. In the first case, either $N = \{\mathrm{id}\}$ or $|N| = 2$. The first subcase finishes the proof, while the second subcase is impossible since, taking $\mathrm{id} \neq \sigma \in N$ we have that N contains also all permutations with the same cycle structure as σ (in view of Proposition 5.9), and this prevents $|N|$ being equal to just 2. In the second case, we have $A_n \subset N$, and thus (by the correspondence theorem, say) either $N = A_n$ or $N = S_n$, as desired. □

Remark 5.22. The group A_4 is not simple. Indeed, it has a normal subgroup $V \subset A_4$ which is

$$V := \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

6 p-groups and Sylow theorems

6.1 p-groups

Throughout this subsection, let $p \in \mathbb{Z}_{\geq 1}$ be a prime number.

Definition 6.1. A group G is called a **p-group** if the order of G is equal to p^k for some $k \in \mathbb{Z}_{\geq 0}$.

Lemma 6.2. *Let us be given an action of a p-group G on a finite set X. Recall the notation*

$$\mathrm{Fix}_G(X) := \{x \in X \mid gx = x \ \forall g \in G\}$$

*(this is the set of **fixed points** of the given action).*

1. *We have $|\mathrm{Fix}_G(X)| \equiv_p |X|$.*
2. *If p does not divide $|X|$ then our action has at least one fixed point.*

Proof. Clearly 2 follows from 1. To show 1, we simply consider the decomposition into orbits. Notice that the orbits with one element are precisely $\{x\}$ for $x \in \mathrm{Fix}_G(X)$. Recall that given an orbit $O \in \mathrm{Orb}_G(X)$, if $x \in O$ then $|O| = |G|/|\mathrm{Stab}_G(x)|$. Therefore, if $|O| > 1$ then p divides $|O|$. Therefore

$$|X| = \sum_{O \in \mathrm{Orb}_G(X)} |O| = |\mathrm{Fix}_G(X)| + \sum_{\substack{O \in \mathrm{Orb}_G(X) \\ |O|>1}} |O|$$

and the last sum is divisible by p, which gives the desired. □

Claim 6.3. *Let G be a p-group. If $|G| > 1$ then $|Z(G)| > 1$.*

Proof. Let us consider the action of G on itself by conjugation. The fixed points of this action are the elements in $Z(G)$. By the previous lemma we obtain that p divides $|Z(G)|$. Since $|Z(G)| \geq 1$ (as $1 \in Z(G)$, we must have $|Z(G)| \geq p$, so in particular $|Z(G)| > 1$. □

Exercise 6.1. *Let G be a group. Assume that $G/Z(G)$ is cyclic. Then G is abelian.*

Corollary 6.4. *Let G be a group with p^2 elements. Then G is abelian.*

Proof. We saw that $|Z(G)| > 1$ and so either $|Z(G)| = p$ or $|Z(G)| = p^2$ (the latter means that G is abelian, so we want to exclude the former). But $|Z(G)| = p$ would imply that $|G/Z(G)| = p$ and so, as we saw in the past, $G/Z(G)$ would be cyclic, so by the exercise G would be abelian, a contradiction. □

Exercise 6.2. *Let G be a group with p^2 elements. Then G is either isomorphic to $\mathbb{Z}_{p^2}$ or to $\mathbb{Z}_p \times \mathbb{Z}_p$. Hint: If G is not isomorphic to $\mathbb{Z}_{p^2}$ then all non-identity elements in G have order p. Take one such element $g_1 \in G$, and then take some $g_2 \in G \smallsetminus \langle g_1 \rangle$. Show that G is the direct product of $\langle g_1 \rangle$ and $\langle g_2 \rangle$.*

Claim 6.5. *Let G be a p-group. Then for every d dividing $|G|$ there exists in G a subgroup of order d.*

Proof. The proof is by induction on $|G|$ (the case $|G| = 1$ being trivial). Assume $|G| > 1$. Then, as we saw, $|Z(G)| > 1$. By Cauchy's theorem, there exists $z \in Z(G)$ such that $o_z = p$. Let us denote $C := \langle z \rangle$. Then C is normal in G and $|C| = p$. By the induction hypothesis, G/C has subgroups of orders p^e for $0 \leq e \leq k-1$. Therefore, using the correspondence theorem, G has subgroups of orders p^e for $1 \leq e \leq k$. □

6.2 Sylow theorems

Throughout this subsection, let $p \in \mathbb{Z}_{\geq 1}$ be a prime number.

Definition 6.6. Let G be a finite group. Write $|G| = p^k n$ where $n \in \mathbb{Z}_{\geq 1}$ and $k \in \mathbb{Z}_{\geq 0}$ and $\gcd(p, n) = 1$. A subgroup $H \subset G$ is called a **p-Sylow subgroup** if $|H| = p^k$.

Example 6.7. *Recall that $\mathbb{Z}_p$ is a field with p elements. Let us consider the group $G := \mathrm{GL}_n(\mathbb{Z}_p)$. By counting linearly independent vectors, we have:*

$$|G| = (p^n - 1)\cdot(p^n - p)\cdot\ldots\cdot(p^n - p^{n-1}) = p^{1+2+\ldots+(n-1)}\cdot(p^n-1)\cdot(p^{n-1}-1)\cdot\ldots\cdot(p-1).$$

Let us now consider the subgroup $U \subset G$ consisting of upper-triangular matrices whose diagonal entries are equal to 1. We have:

$$|U| = p^{1+2+\ldots+(n-1)}.$$

Therefore U is a p-Sylow subgroup in G.

Proposition 6.8. *Let G be a finite group and let $H \subset G$ be a subgroup. Let P be a p-Sylow subgroup in G. Then there exists $g \in G$ such that $H \cap g^{-1}Pg$ is a p-Sylow subgroup in H.*

Proof. Let us consider the action of H on G/P by $h \bullet gP := hgP$. Since $|G/P| = |G|/|P|$ is not divisible by p, there exists an orbit $O \in \mathrm{Orb}_H(G/P)$ such that $|O|$ is not divisible by p. Fixing such an orbit O, let us also fix some $gP \in O$. Then

$$\mathrm{Stab}_H(gP) = \{h \in H \mid hgP = gP\} = \{h \in H \mid g^{-1}hg \in P\} = H \cap gPg^{-1}.$$

Thus

$$[H : H \cap gPg^{-1}] = |H|/|H \cap gPg^{-1}| = |H|/|\mathrm{Stab}_H(gP)| = |O|$$

and so $H \cap gPg^{-1}$ is a p-group whose index in H is not divisible by p. Clearly, this is equivalent to $H \cap gPg^{-1}$ being a p-Sylow subgroup of H. □

Theorem 6.9 (First Sylow theorem)**.** *Let G be a finite group. Then there exist in G p-Sylow subgroups.*

Proof. By Proposition 6.8, if we can find a monomorphism of groups $G \to G'$ where G' is a finite group which has a p-Sylow subgroup, then G will also have a p-Sylow subgroup, giving the desired. Recall that, denoting $n := |G|$, we can find a monomorphism $G \to S_n$, so that we reduce the claim to $G = S_n$. Also, recall that we can find a monomorphism $S_n \to \mathrm{GL}_n(\mathbb{Z}_p)$, so that we reduce the claim to $G = \mathrm{GL}_n(\mathbb{Z}_p)$. But we saw that this G contains a p-Sylow subgroup, in Example 6.7. □

Remark 6.10. Let us give another proof of the first Sylow theorem, using Cauchy's theorem and induction on $|G|$, instead of using Proposition 6.8. Let us denote $|G| = p^k n$ with $\gcd(p, n) = 1$. If $k = 0$ the claim is trivial, so we assume that $k \geq 1$. Let us argue by induction on $|G|$ (the case $|G| = 1$ being trivial). Let us consider an element $g \in G \setminus Z(G)$, and its centralizer $C_G(g)$. We have $C_G(g) \neq G$ (since $g \notin Z(G)$). If p^k divides $|C_G(g)|$ then by the induction hypothesis $C_G(g)$ contains a subgroup of order p^k and therefore G contains a subgroup of order p^k and we are done. Thus we can assume that (for every $g \in G \setminus Z(G)$) p^k does not divide $|C_G(g)|$, and therefore the size of the conjugacy class of g, which is $|G|/|C_G(g)|$, is divisible by p. In other words, we can assume that all conjugacy classes in G which are not singletons have size divisible by p. Therefore, since G is the union of $Z(G)$ and all the conjugacy classes in G which are not singletons, we get that the size of $Z(G)$ is divisible by p. By Cauchy's theorem, $Z(G)$ then contains an element of order p, denote such an element by z. Denote $C = \langle z \rangle$. Then $|C| = p$ and C is a normal subgroup of G. By the induction hypothesis, G/C has a subgroup of order p^{k-1}, denote such a subgroup by $\overline{H}$. Denote by $H \subset G$ the subgroup which corresponds to $\overline{H}$ under the correspondence theorem (i.e. the inverse image of $\overline{H}$ under the canonical projection map $G \to G/C$). Then $|H| = |C| \cdot |\overline{H}| = p \cdot p^{k-1} = p^k$, and we found a p-Sylow subgroup in G as desired.

Let us next give some corollaries of Proposition 6.8.

Corollary 6.11 (Second Sylow theorem)**.** *Let G be a finite group. Every two p-Sylow subgroups in G are conjugate, i.e. given p-Sylow subgroups $P_1, P_2 \subset G$ there exists $g \in G$ such that $gP_1g^{-1} = P_2$.*

Proof. Applying Proposition 6.8, there exists $g \in G$ such that $P_2 \cap gP_1g^{-1}$ is a p-Sylow subgroup in P_2. Since P_2 is a p-group, this simply means that $P_2 = P_2 \cap gP_1g^{-1}$, i.e. $P_2 \subset gP_1g^{-1}$. Since P_2 and gP_1g^{-1} have the same order, we must have an equality $P_2 = gP_1g^{-1}$. □

Corollary 6.12 (Also sometimes called a part of the second Sylow theorem)**.** *Let G be a finite group. Every p-subgroup of G is contained in a p-Sylow subgroup of G, i.e. given a p-subgroup $Q \subset G$ there exists a p-Sylow subgroup $P \subset G$ such that $Q \subset P$.*

Proof. In fact we more or less repeat the previous proof (one can unify if one wants to "save argumentation raw material"). Namely, let $R \subset G$ be some p-Sylow subgroup. By Proposition 6.8, there exists $g \in G$ such that $Q \cap gRg^{-1}$

is a p-Sylow subgroup in Q. Since Q is a p-group this simply means that $Q \cap gRg^{-1} = Q$ i.e. $Q \subset gRg^{-1}$. Notice that gRg^{-1} is a p-Sylow subgroup of G, and we are done. □

Corollary 6.13. *Let G be a finite group and let $P \subset G$ be a p-Sylow subgroup. Then P is normal in G if and only if P is the only p-Sylow subgroup in G.*

Proof. The set $\{gPg^{-1} \ : \ g \in G\}$ is the set of p-Sylow subgroups in G (by the second Sylow theorem). It is equal to the singleton $\{P\}$ if and only if $gPg^{-1} = P$ for all $g \in G$, i.e. if and only if P is normal in G. □

Theorem 6.14 (Third Sylow theorem)**.** *Let G be a finite group. Denote $|G| = p^k n$ for $k \in \mathbb{Z}_{\geq 0}$ and $m \in \mathbb{Z}_{\geq 1}$ with m not divisible by p. Denote by $s_p \in \mathbb{Z}_{\geq 1}$ the number of p-Sylow subgroups in G. Then:*

1. *$s_p | n$.*
2. *$s_p \equiv_p 1$.*

Proof. Let S denote the set of p-Sylow subgroups of G (so $s_p = |S|$). We have an action of G on S by conjugation: $g \bullet P := gPg^{-1}$. This action is transitive by the second Sylow theorem. Thus, fixing some $P_0 \in S$, and denoting by H the stabilizer of P_0 with respect to our action, i.e. $H = N_G(P_0)$, we have $|G|/|H| = s_p$. Notice that $P_0 \subset H$, so $|P_0| = p^k$ divides H. Hence $s_p = |G|/|H|$ divides n, giving the first desired fact. To show the second fact, let us restrict our action of G on S by conjugation to an action of P_0 on S. Since P_0 is a p-group, by Lemma 6.2 the number of fixed points of this action is congruent modulo p to $|S| = s_p$. It is enough therefore to check that there is precisely one fixed point. A fixed point of this action is a p-Sylow subgroup $P \subset G$ satisfying $gPg^{-1} = P$ for all $g \in P_0$, i.e. satisfying $P_0 \subset N_G(P)$. Clearly P_0 is such, and we want to check that is it the only one. In other words, given a p-Sylow subgroup $P \subset G$ satisfying $P_0 \subset N_G(P)$, we want to check that $P = P_0$. But, notice that P and P_0 are p-Sylow subgroups in $N_G(P)$, and thus conjugate in $N_G(P)$ by the second Sylow theorem. But P is normal in $N_G(P)$, and thus we must have $P = P_0$. □

Remark 6.15. As we have implicitly seen above, given a finite group G, using the action by conjugation of G on the set of p-Sylow subgroups in G, we have that the number of p-Sylow subgroups in G is equal to $[G : N_G(P)]$ where P is any p-Sylow subgroup in G.

Example 6.16. *Let us prove the following claim using Sylow theory: Let G be a finite group of order pq where p and q are primes with $p < q$. Assume in addition that $q \not\equiv_p 1$. Then we claim that G is cyclic. Indeed, let $P \subset G$ be a p-Sylow subgroup. We have $[G : P] = q$, and therefore $N_G(P)$, being a subgroup of G which contains P, must be either equal to P or to G. In the first case we have that the number of p-Sylow subgroups in G is $[G : N_G(P)] = q$. But this is impossible since $q \not\equiv_p 1$, in view of the third Sylow theorem. Hence we must have $N_G(P) = G$, i.e. P is normal in G. Let also $Q \subset G$ be a q-Sylow subgroup*

in G. Reasoning similarly, since we clearly have $p \not\equiv_q 1$, we also see that Q is normal in G. Notice that $P \cap Q = \{1\}$ (why?), and therefore $|PQ| = pq$, and so $PQ = G$. Thus, we have all the conditions to deduce that G is the direct product of P and Q, so isomorphic to $P \times Q$. By the Chinese reminder theorem, since $\gcd(p, q) = 1$,

$$G \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq},$$

i.e. G is cyclic.

Example 6.17. *The condition in the previous example is necessary, in general, for the conclusion. Indeed, suppose that p and q are primes numbers, with $p < q$ and $q \equiv_p 1$. Since p divides $q - 1$, there exists $s \in \mathbb{Z}_q^\times$ with order p. Recall that we have an isomorphism*

$$\alpha : \mathbb{Z}_q^\times \xrightarrow{\sim} \mathrm{Aut}(\mathbb{Z}_q)$$

given by sending $e \in \mathbb{Z}_q^\times$ to the automorphism of $\mathbb{Z}_q$ given by $x \mapsto ex$. We have a homomorphism

$$\beta : \mathbb{Z}_p \to \mathbb{Z}_q^\times$$

given by sending $[m]_p$ to a^m. Taking the composition

$$\gamma := \alpha \circ \beta : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q)$$

we obtain an action $a_\gamma : \mathbb{Z}_p \times \mathbb{Z}_q \to \mathbb{Z}_q$ of $\mathbb{Z}_p$ on $\mathbb{Z}_q$ by group automorphisms (defined by $a_\gamma([m]_p, x) := s^m x$ - recall Remark 4.41). Then the corresponding semidirect product $\mathbb{Z}_q \rtimes_{a_\gamma} \mathbb{Z}_p$ is not abelian (and so not cyclic).

Exercise 6.3. *Repeat the above analysis again - given primes $p < q$ and a group G of order pq, show that G is isomorphic to some semidirect product $\mathbb{Z}_q \rtimes \mathbb{Z}_p$. The piece of data of the action of $\mathbb{Z}_p$ on $\mathbb{Z}_q$ is encoded by an element $s \in \mathbb{Z}_q^\times$ of order dividing p, and one can understand things completely...*

7 Normal series etc.

7.1 Normal series

Definition 7.1. Let G be a group. A **normal series** for G is a series $(G_0, G_1, \ldots, G_n)$ consisting of subgroups of G, with the properties:

- $G_0 = \{1\}$.
- $G_n = G$.
- G_i is a normal subgroup of G_{i+1} for all $0 \leq i \leq n - 1$.

We call the sequence $(G_1/G_0, \ldots, G_n/G_{n-1})$ the corresponding sequence of **factors**.

Lemma 7.2. *Let G be a group and let $H \subset G$ be a subgroup. Let*

$$(G_0, \ldots, G_n) \tag{7.1}$$

be a normal series for G.

1. *The sequence*
$$(G_0 \cap H, \ldots, G_n \cap H) \tag{7.2}$$
is a normal series for H, whose factors are isomorphic to subgroups of factors of (7.1). If H is normal in G then the factors of (7.2) are isomorphic to normal subgroups of factors of (7.1).

2. *Suppose that H is normal in G, and denote by $p : G \to G/H$ the canonical projection map. Then the sequence*
$$(p(G_0), \ldots, p(G_n)) \tag{7.3}$$
is a normal series for G/H, whose factors are isomorphic to quotient groups of factors of (7.1).

Proof. 1. It is immediate to see that the sequence is a normal series for H. Notice that we have a monomorphism $(G_{i+1} \cap H)/(G_i \cap H) \to G_{i+1}/G_i$ given by $h(G_i \cap H) \mapsto hG_i$, and that its image is normal in the target if H is normal in G, giving the desired.

2. It is immediate to see that the sequence is a normal series for G/H. Notice that we have an epimorphism $G_{i+1}/G_i \to p(G_{i+1})/p(G_i)$ given by $gG_i \mapsto p(g)p(G_i)$, giving the desired. □

Lemma 7.3. *Let G be a group, let $H \subset G$ be a normal subgroup and denote by $p : G \to G/H$ the canonical quotient map. Let*

$$(H_0, \ldots, H_m) \tag{7.4}$$

be a normal series for H and let

$$(L_0, \ldots, L_k) \tag{7.5}$$

be a normal series for G/H. Then

$$(H_0, \ldots, H_m = p^{-1}(L_0), \ldots, p^{-1}(L_k))$$

is a normal series for G, whose sequence of factors is isomorphic to the concatenation of the sequences of factors of (7.4) and (7.5).

Proof. Left as an exercise. □

7.2 Groups of finite length, Jordan-Holder theorem

Definition 7.4. Let G be a group. A normal series for G is called a **composition series** if all its factors are simple groups. In such a case, the sequence of factors is called a sequence of **composition factors**.

Definition 7.5. A group is said to be of **finite length** if it has a composition series.

Remark 7.6. Given a group G and a normal series

$$(G_0, \ldots, G_n)$$

for G, let us say that this series is **without repetitions** if $G_i \neq G_{i+1}$ for all $0 \leq i \leq n-1$. Let us say that this series is **saturated** if for every $0 \leq i \leq n-1$ and every subgroup $G_i \subset H \subset G_{i+1}$ such that H is normal in G_{i+1}, we have either $H = G_i$ and $H = G_{i+1}$. Then the normal series is a composition series if and only if it is without repetitions and saturated. Notice that if a group G has a saturated normal series then it has finite length, since by eliminating repeating elements in the series, we can make it to be without repetitions (while still being saturated).

Example 7.7. *A composition series for the group $\mathbb{Z}_{12}$ is given by*

$$(\{[0]_{12}\}, \langle [6]_{12} \rangle, \langle [3]_{12} \rangle, \mathbb{Z}_{12}).$$

Indeed, the corresponding sequence of factors is isomorphic to

$$(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3).$$

Notice that we can find some other composition series for $\mathbb{Z}_{12}$, such as

$$(\{[0]_{12}\}, \langle [4]_{12} \rangle, \langle [2]_{12} \rangle, \mathbb{Z}_{12}),$$

$$(\{[0]_{12}\}, \langle [6]_{12} \rangle, \langle [2]_{12} \rangle, \mathbb{Z}_{12}),$$

and the sequences of composition factors are isomorphic to a permutation of the sequence of composition factors for the first composition series.

Example 7.8. *The group A_4 has a composition series:*

$$(\{\mathrm{id}\}, \{\mathrm{id}, (12)(34)\}, V, A_4),$$

and the sequence of composition factors is isomorphic to

$$(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3).$$

Remark 7.9. Combining the above two examples, we learn that, first, a group can have several composition series, with different (up to isomorphism) sequences of composition factors, although in the example they happen to be the same if we disregard the order of appearance of the composition factors. Also, it might

be that two non-isomorphic groups can have composition series with isomorphic sequences of composition factors. This is a repetition of the idea that groups can be "glued" in various ways from the same "building blocks". For example, we say that under the right conditions on primes $p < q$, we can find non-abelian semi-direct products $G := \mathbb{Z}_q \rtimes \mathbb{Z}_p$. Such a semi-direct product has a composition series $(\{1\}, \mathbb{Z}_q, G)$ with a sequence of composition factors, up to isomorphism, $(\mathbb{Z}_q, \mathbb{Z}_p)$. But, of course, also the abelian group $\mathbb{Z}_q \times \mathbb{Z}_p$ has a composition series $(\{1\}, \mathbb{Z}_q, H)$ with composition factors $(\mathbb{Z}_q, \mathbb{Z}_p)$.

Example 7.10. *It can be that a group does not have a composition series, i.e. it is of infinite length. The simplest example is of $\mathbb{Z}$. Indeed, if we have a composition series $(G_0, \ldots, G_n)$ in $\mathbb{Z}$, then $G_1 \neq \{0\}$ (otherwise G_1/G_0 is the trivial group, so not simple). But then $G_1 = \langle m \rangle$ for some $m \in \mathbb{Z}_{\geq 1}$ and so $G_1/G_0 \cong H_1 = \langle m \rangle \cong \mathbb{Z}$, but $\mathbb{Z}$ is not simple.*

Lemma 7.11. *Let G be a group and let $N \subset G$ be a normal subgroup. Then G has finite length if and only if both N and G/N have finite length.*

Proof. Suppose first that G has finite length. Pick a composition series for G and construct a normal series for N using Lemma 7.2. By the lemma, the factors of this series for N are isomorphic to normal subgroups of factors of our series for G. Since the latter are simple, the factors of the normal series for N are either trivial or simple, i.e. the normal series is saturated, showing that N has finite length. Now construct a normal series for G/N using Lemma 7.2. By the lemma, the factors of this series for G/N are isomorphic to quotient groups of factors of our series for G. Since the latter are simple, the factors of the normal series for G/N are either trivial or simple, i.e. the normal series is saturated, showing that G/N has finite length.

Suppose now that both N and G/N have finite length. Pick composition series for N and G/N and construct a normal series for G from them using Lemma 7.3. By the lemma, the factors of this normal series are isomorphic to factors of the normal series for N or the normal series for G/N, so that in any case they are simple, showing that the normal series for G is a composition series, and hence G has finite length. □

Lemma 7.12. *A finite group is of finite length.*

Proof. The proof is by induction on $|G|$, where G is the finite group which we want to show is of finite length. If $|G| = 1$ then (G) is a composition series for G (the corresponding sequence of composition factors is empty). Now let $|G| > 1$. If G is simple, then $(\{1\}, G)$ is a composition series for G (with sequence of composition factors isomorphic to (G)). Suppose that G is not simple. Then there exists a normal subgroup $N \subset G$ such that $N \neq \{1\}$ and $N \neq G$. Using the induction hypothesis, both N and G/N are of finite length, and hence by the previous lemma G is of finite length. □

Theorem 7.13 (Jordan-Holder)**.** *Let G be a group and let*

$$(H_0, \ldots, H_n)$$

and

$$(K_0, \ldots, K_m)$$

be two composition series for G. Then the sequences of factors

$$(H_1/H_0, \ldots, H_n/H_{n-1})$$

and

$$(K_1/K_0, \ldots, K_m/K_{m-1})$$

coincide up to isomorphism and permutation.

Proof. We perform induction on $\min(m, n)$ (the case when this is 0 is clear). Let us denote

$$L := H_{n-1} \cap K_{m-1}.$$

If $H_{n-1} \subset K_{m-1}$ then, since G/H_{n-1} is simple, by the correspondence theorem we obtain $K_{m-1} = H_{n-1}$. Similarly, if $K_{m-1} \subset H_{n-1}$ then $K_{m-1} = H_{n-1}$. In this case L has composition series

$$(H_0, \ldots, H_{n-1})$$

and

$$(K_0, \ldots, K_{m-1}),$$

and we can apply the induction hypothesis to see that the sequences

$$(H_1/H_0, \ldots, H_{n-1}/H_{n-2})$$

and

$$(K_1/K_0, \ldots, K_{m-1}/K_{m-2})$$

are the same up to isomorphism and permutation, and therefore appending to them $G/L = G/H_{n-1} = G/K_{m-1}$ yields sequences which are the same up to isomorphism and permutation, giving the desired. Thus, we are left to analyse the case when neither $H_{n-1} \subset K_{m-1}$ nor $K_{m-1} \subset H_{n-1}$. Since L is a normal subgroup of G, L admits a composition series, say

$$(L_0, \ldots, L_k).$$

We have a monomorphism $\alpha : H_{n-1}/L \to G/K_{m-1}$ (given by $hL \mapsto hK_{m-1}$) whose image is a normal subgroup in the target. The image can not be trivial because this would mean that $H_{n-1} \subset K_{m-1}$, which we assume is not the case. Hence (since G/K_{m-1} is a simple group), the image must be the whole G/K_{m-1}, so that in fact α is an isomorphism. Therefore, we have a composition series for H_{n-1} given by

$$(L_0, \ldots, L_k, H_{n-1}).$$

We also have the composition series for H_{n-1} given by

$$(H_0, \ldots, H_{n-1}).$$

We can apply the induction hypothesis, obtaining that the following series are the same up to isomorphism and permutation:

$$(L_1/L_0, \ldots, L_k/L_{k-1}, G/K_{m-1})$$

and

$$(H_1/H_0, \ldots, H_{n-1}/H_{n-2}).$$

Analogously, we obtain that the following series are the same up to isomorphism and permutation:

$$(L_1/L_0, \ldots, L_k/L_{k-1}, G/H_{n-1})$$

and

$$(K_1/K_0, \ldots, K_{m-1}/K_{m-2}).$$

But then

$$(L_1/L_0, \ldots, L_k/L_{k-1}, G/K_{m-1}, G/H_{n-1})$$

is the same up to isomorphism and permutation as both

$$(H_1/H_0, \ldots, H_{n-1}/H_{n-2}, G/H_{n-1})$$

and

$$(K_1/K_0, \ldots, K_{m-1}/K_{m-2}, G/K_{m-1}),$$

so the two latter series are the same up to isomorphism and permutation, as desired. □

Definition 7.14. Let G be a group of finite length. If

$$(G_0, \ldots, G_n)$$

is a composition series for G, the number n is called the **length**, or **composition length**, of G. For a simple group H, the number of $0 \leq i \leq n-1$ for which G_{i+1}/G_i is isomorphic to H can be called the **amount of times H appears in G**. These do not depend on the choice of composition series, by the Jordan-Holder theorem.

Exercise 7.1. *Let G be a group of finite length and let $N \subset G$ be a normal subgroup. Let H be a simple group. Then the amount of times H appears in G is equal to the amount of times H appears in N plus the amount of times H appears in G/N.*

Example 7.15. *Given $n \in \mathbb{Z}_{\geq 1}$, let us write $n = p_1 \cdot \ldots p_k$ where p_i are prime numbers. Then we have a composition series for $\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$ given by*

$$(\mathbb{Z}/\langle 1 \rangle, \mathbb{Z}/\langle p_1 \rangle, \mathbb{Z}/\langle p_1 p_2 \rangle \ldots, \mathbb{Z}/\langle n \rangle),$$

whose sequence of factors is isomorphic to

$$(\mathbb{Z}_{p_1}, \mathbb{Z}_{p_2}, \ldots, \mathbb{Z}_{p_n}).$$

Then the Jordan-Holder theorem shows that for each given prime p, the amount of $1 \leq i \leq n$ for which $p = p_i$ does not depend on our choice of writing n as a product of primes. In other words, it recovers the uniqueness of decomposition into primes, basically.

7.3 Commutator subgroups

Definition 7.16. Let G be a group.

1. Given $g_1, g_2 \in G$ we define the **commutator** $[g_1, g_2] := g_1 g_2 g_1^{-1} g_2^{-1} \in G$.
2. Given subgroups $H_1, H_2 \subset G$ we define $[H_1, H_2]$ to be the subgroup of G generated by the subset

$$\{[h_1, h_2] \ : \ h_1 \in H_1, h_2 \in H_2\} \subset G.$$

In particular, $[G, G]$ is called the **commutator subgroup** of G.

Exercise 7.2. *Let G be a group and let $g_1, g_2 \in G$. Then $[g_1, g_2] = 1$ if and only if $g_1 g_2 = g_2 g_1$, i.e. g_1 and g_2 commute.*

Exercise 7.3. *Let G be a group. Show that $[G, G]$ is a normal subgroup of G. Show that $G/[G, G]$ is abelian. Show that given a normal subgroup K in G such that G/K is abelian, we have $[G, G] \subset K$. One says informally that "$G/[G, G]$ is the largest abelian quotient of G".*

7.4 Solvable groups

Definition 7.17. A group G is called **solvable** if there exists a normal series for G all of whose factors are abelian.

Lemma 7.18. *Let G be a group and let $H \subset G$ be a subgroup. If G is solvable then H is solvable. If H is normal in G and G is solvable then G/H is solvable. If H is normal in G and both H and G/H are solvable then G is solvable.*

Proof. This follows in a straight-forward way from Lemma 7.2 and Lemma 7.3, once we notice that subgroups of abelian groups are abelian and quotient groups of abelian groups are abelian. □

Example 7.19. *Abelian groups are solvable. The semidirect product of two solvable groups is solvable, and so in particular the semidirect product of two abelian groups is solvable.*

Example 7.20. *p-groups are solvable. Indeed, we can prove this by induction on the order of a p-group, because, recall, the center of a non-trivial p-group is non-trivial.*

Remark 7.21. A theorem of Burnside states that if the order of a finite group is divisible by at most two primes, then this group is solvable. The proof is via representation theory of finite groups.

Claim 7.22. *The group S_n is not solvable for $n \geq 5$ (in fact, A_n is not solvable for $n \geq 5$).*

Proof. This is clear, since we saw that A_n is simple (for $n \geq 5$), therefore it has no non-trivial normal series (complete!). □

Remark 7.23. In Galois theory, the previous claim is used to show the non-solvability of equations of degree ≥ 5 in radicals (it is a very virtuoso transition). Hence the term, "solvable".

Definition 7.24. Let G be a group. The **derived series** of G is the sequence of subgroups of G defined recursively as follows: $G^{(0)} := G$ and $G^{(n+1)} := [G^{(n)}, G^{(n)}]$ for $n \geq 0$.

Lemma 7.25. *Let G be a group. For every $n \geq 0$, $G^{(n)}$ is a normal subgroup of G.*

Proof. The proof is by induction on n, the case $n = 0$ being trivial. Suppose that we showed the claim for some n, and let us show it for $n + 1$. Let $g \in G$; we want to see that $gG^{(n+1)}g^{-1} \subset G^{(n+1)}$. Since $G^{(n+1)}$ is generated by elements of the form $[h, k]$ where $h, k \in G^{(n)}$, it is enough to show that for $h, k \in G^{(n)}$ we have $g[h, k]g^{-1} \in G^{(n+1)}$. We have $g[h, k]g^{-1} = [ghg^{-1}, gkg^{-1}]$, and since by the induction hypothesis we have $ghg^{-1}, gkg^{-1} \in G^{(n)}$, we have $[ghg^{-1}, gkg^{-1}] \in G^{(n+1)}$, as desired. □

Claim 7.26. *Let G be a group. The following are equivalent:*

1. *G is solvable.*
2. *There exists $n \geq 0$ such that $G^{(n)} = \{1\}$.*
3. *There exists a normal series for G*

$$(G_0, \ldots, G_n)$$

with abelian factors such that, additionally, G_i is normal in G for all $0 \leq i \leq n$.

Proof. Notice that it is trivial that 3 implies 1. That 2 implies 3 is also clear: If $G^{(n)} = \{1\}$ consider the normal series for G given by

$$(G^{(n)}, G^{(n-1)}, \ldots, G^{(0)})$$

has abelian factors, and each $G^{(i)}$ is normal in G. Thus, we are left to see that 1 implies 2. Let

$$(G_0, \ldots, G_n)$$

be a normal series for G with abelian factors. We claim that $G^{(i)} \subset G_{n-i}$ for all $0 \leq i \leq n$. Then $G^{(n)} \subset G_0 = \{1\}$ showing that $G^{(n)} = \{1\}$ as desired. One proceeds by induction on i, the case $i = 0$ being trivial. Now if the claim is shown for a given i, notice that

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \subset [G_{n-i}, G_{n-i}] \subset G_{n-(i+1)},$$

as desired. □

7.5 Nilpotent groups

Definition 7.27. Let G be a group. A normal series for G

$$(G_0, \ldots, G_n)$$

is called a **central series** if G_i is normal in G for all $0 \leq i \leq n$, and G_{i+1}/G_i lies in the center of G/G_i for all $0 \leq i \leq n-1$. If G admits a central series then G is called **nilpotent**.

Exercise 7.4. *Given a group G and a normal series*

$$(G_0, \ldots, G_n)$$

for G, show that it is a central series if and only if $[G_{i+1}, G] \subset G_i$ for all $0 \leq i \leq n-1$.

Example 7.28. *Abelian groups are nilpotent.*

Remark 7.29. Clearly, nilpotent groups are solvable.

Lemma 7.30. *Let G be a group and let $H \subset G$ be a subgroup. If G is nilpotent then H is nilpotent. If H is normal in G and G is nilpotent, then G/H is nilpotent.*

Proof. The proof repeats the same ideas as the proof of the analogous claim for solvability, we leave it as an exercise. □

Exercise 7.5. *Let G be a nilpotent group. Show that if G is not trivial then $Z(G)$ is not trivial.*

Remark 7.31. Notice, however, that if G is a group and $H \subset G$ is a normal group, then if both H and G/H are nilpotent, it in general does not follow that G is nilpotent. Indeed, the group S_3 has the subgroup A_3, and both A_3 and S_3/A_3, being abelian, are nilpotent. However, we claim that S_3 is not nilpotent. Indeed, one easily checks that $Z(S_3) = \{1\}$ and therefore the previous exercise shows that S_3 is not nilpotent.

Exercise 7.6. *Let k be a field and let $n \in \mathbb{Z}_{\geq 1}$. Let U be the subgroup of $\mathrm{GL}_n(k)$ consisting of upper triangular matrices whose diagonal values are all equal to 1. Show that U is a nilpotent group. Next, denote by B the subgroup of $\mathrm{GL}_n(k)$ consisting of upper triangular matrices and denote by T the subgroup of $\mathrm{GL}_n(k)$ consisting of diagonal matrices. Notice that $T, U \subset B$. Show that $B = U \rtimes T$. Deduce that B is solvable. As an extra exercise (not a must), try to see that, in general, B is not nilpotent (maybe except a few simple cases, like $n = 1$ etc.).*

Definition 7.32. Let G be a group. The **lower central series** of G is the sequence of subgroups of G defined recursively as follows: $L_0(G) := G$, $L_{n+1}(G) := [L_n(G), G]$. The **upper central series** of G is the sequence of subgroups of G defined recursively as follows: $U_0(G) := \{1\}$, $U_{n+1}(G) := p_n^{-1}(Z(G/U_n(G)))$ where $p_n : G \to G/U_n(G)$ denotes the canonical projection.

Claim 7.33. *Let G be a group. The following are equivalent:*

1. *G is nilpotent.*
2. *There exists $n \geq 0$ such that $L_n(G) = \{1\}$.*
3. *There exists $n \geq 0$ such that $U_n(G) = G$.*

Proof. To show that 2 implies 1, notice that it is easy to see that

$$(L_n(G), \ldots, L_0(G))$$

is a central series for G. To show that 3 implies 1, notice that it is easy to see that

$$(U_0(G), \ldots, U_n(G))$$

is a central series for G.

Suppose now that G is nilpotent. Let

$$(G_0, \ldots, G_n)$$

be a central series for G. We claim that $L_i(G) \subset G_{n-i}$ for all $0 \leq i \leq n$. Indeed, we check this by induction. For $i = 0$ the claim is clear. If we checked the claim for some i, then

$$L_{i+1}(G) = [L_i(G), G] \subset [G_{n-i}, G] \subset G_{n-(i+1)},$$

completing the induction step. Therefore, in particular, $L_n(G) \subset G_0 = \{1\}$, and so $L_n(G) = \{1\}$. We claim next that we also have $G_i \subset U_i(G)$ for all $0 \leq i \leq n$. We again check this by induction. For $i = 0$ the claim is clear. If we checked the claim for some i, then we have

$$[G_{i+1}, G] \subset G_i \subset U_i(G)$$

and therefore, denoting by $p : G \to G/U_i(G)$ the canonical quotient map, we have $p(G_{i+1}) \subset Z(G/U_i(G))$, showing that $G_{i+1} \subset U_{i+1}(G)$, completing the induction step. Therefore, in particular, $G = G_n \subset U_n(G)$, and so $U_n(G) = G$. □

Claim 7.34. *p-groups are nilpotent.*

Proof. If G is a p-group, we claim that $U_{i+1}(G) \neq U_i(G)$ unless $U_i(G) = G$. This will show that $U_i(G) = G$ for big enough i, by order consideration. To that end, notice that $G/U_i(G)$ is a p-group, and if it is not trivial then, as we saw, $Z(G/U_i(G)$ is not trivial, i.e. $Z(G/U_i(G)) \neq U_i(G)/U_i(G)$ and therefore $U_{i+1}(G) \neq U_i(G)$ (by the correspondence theorem). □

Lemma 7.35. *The product of two finitely many nilpotent groups is nilpotent.*

Proof. It is enough to show that $G_1 \times G_2$ is nilpotent for two nilpotent groups G_1 and G_2. Given subgroups $H_1, H_1' \subset G_1$ and $H_2, H_2' \subset G_2$ it is easy to see that $[H_1 \times H_2, H_1' \times H_2'] = [H_1, H_1'] \times [H_2, H_2']$ and from this it is easy to see that $L_n(G_1 \times G_2) = L_n(G_1) \times L_n(G_2)$ for all $n \geq 0$. □

Remark 7.36. Let us briefly remark regarding internal finite products. Given a group G and subgroups $H_1, \ldots, H_k \subset G$, we say that G is the **product** of $H_1, \ldots, H_k$ if the map

$$\phi : H_1 \times \ldots \times H_k \to G$$

given by

$$(h_1, \ldots, h_k) \mapsto h_1 \cdot \ldots \cdot h_k$$

is an isomorphism. It is an exercise that this is equivalent to the following conditions:

1. For any $1 \leq i, j \leq k$ and any $h \in H_i$ and $h' \in H_j$ we have $hh' = h'h$. This condition allows us to write, for example, $H_1 H_2 \cdot \ldots \cdot H_k$ as $\prod_{1 \leq i \leq k} H_i$, because it does not matter in which order we take the product (and the product is a subgroup of G).
2. For every $1 \leq i \leq k$ we have $H_i \cap \prod_{1 \leq j \leq k, j \neq i} H_j = \{1\}$.
3. We have $G = \prod_{1 \leq i \leq k} H_i$.

In fact, more precisely, the first conditions is equivalent to ϕ being a group homomorphism. The second condition then is equivalent to ϕ being injective, and the third condition to ϕ being surjective. In particular, if G is finite, the first condition implies that $\left|\prod_{1 \leq i \leq k} H_i\right|$ divides $\prod_{1 \leq i \leq k} |H_i|$. If the second condition is satisfies in addition, then we have $\left|\prod_{1 \leq i \leq k} H_i\right| = \prod_{1 \leq i \leq k} |H_i|$. The third condition is then equivalent, given the first two conditions, to the numerical condition $|G| = |P_1| \cdot \ldots \cdot |P_k|$.

Theorem 7.37. *Let G be a finite group. The following are equivalent:*

1. *G is nilpotent.*
2. *Each Sylow subgroup in G is normal in G.*
3. *G is the direct product of its Sylow subgroups.*
4. *G is isomorphic to a finite product of p-groups (for different p's).*

Proof. Notice that 4 implies 1 since we saw that p-groups are nilpotent and that the finite product of nilpotent groups is nilpotent. Notice also that it is trivial that 3 implies 4.

Let us see that 2 implies 3. Let $p_1, \ldots, p_k$ be the different primes dividing $|G|$. Let P_i be the unique p_i-Sylow subgroup in G, for every $1 \leq i \leq k$. We want to see that G is the product of $P_1, \ldots, P_k$, using the remark above. Since the Sylow

subgroups of G are normal in G, for i and j we have $[P_i, P_j] \subset P_i \cap P_j = \{1\}$, or in other words $gh = hg$ for all $g \in P_i$ and $h \in P_j$, so that condition 1 of the remark above is satisfied. Notice that it is also clear that the numerical condition replacing condition 3 in the remark also obviously holds in our case. Thus, it is left to check condition 2. But, notice that, since condition 1 is satisfied, we have that $\left|\prod_{1\leq j\leq k, j\neq i} P_j\right|$ divides $\prod_{1\leq j\leq k, j\neq i} |P_j|$, and therefore is relatively prime to $|P_i|$. Hence $\left|P_i \cap \prod_{1\leq j\leq k, j\neq i} P_j\right|$ divides two relatively prime numbers, and hence it is equal to 1, so $P_i \cap \prod_{1\leq j\leq k, j\neq i} P_j = \{1\}$, as desired.

Let us now see that 1 implies 2. So let G be nilpotent, let p be a prime and let $P \subset G$ be a p-Sylow subgroup. We want to show that P is normal in G. We will do this by induction on $|G|$. If $|G| = 1$ then the claim is trivial, so assume $|G| > 1$. Then $Z(G) \neq \{1\}$. Let us consider $P' := PZ(G) \subset G$. If $P' = G$ then it is immediate to see that P is normal in G. Hence let us assume that $P' \neq G$. Notice that $P'/Z(G)$ is a p-Sylow subgroup in $G/Z(G)$. Therefore, since $G/Z(G)$ is nilpotent, by the induction hypothesis $P'/Z(G)$ is normal in $G/Z(G)$, and so by the correspondence theorem P' is normal in G. Thus, given $g \in G$, we have p-Sylow subgroups P and gPg^{-1} of P'. But, notice also that P is normal in P'. Hence, by the second Sylow theorem, P is the only p-Sylow subgorup in P', and therefore $gPg^{-1} = P$. Since g was arbitrary, this shows that P is normal in G. □

8 A bit about presentation

8.1 The infinite cyclic group

Definition 8.1. Given groups G and H, let us denote by $\mathrm{Hom}(H, G)$ the set of group homomorphism from H to G.

Exercise 8.1. *Let G be a group. We have a bijection*

$$\mathrm{Hom}(\mathbb{Z}, G) \to G$$

given by sending ϕ to $\phi(1)$.

In words, "to give a homomorphism from $\mathbb{Z}$ is the same as to specify where 1 should go (and this specification is unconstrained).

8.2 Finite cyclic groups

Claim 8.2. *Let G be a group and let $n \in \mathbb{Z}_{\geq 1}$. We have a bijection*

$$\mathrm{Hom}(\mathbb{Z}_n, G) \to \{g \in G \mid g^n = 1\}$$

given by sending ϕ to $\phi([1]_n)$.

Proof. An exercise. □

Let us paraphrase in multiplicative notation for convenience. Let $n \in \mathbb{Z}_{\geq 1}$ and let C be a cyclic group of order n, with generator c. Then for any group G we have a bijection

$$\mathrm{Hom}(C, G) \to \{g \in G \mid g^n = 1\}$$

and we say "to give a homomorphism from C is the same as to specify an element whose n-th power is 1". We say that C is given by **generators and relations** as follows: It has a generator c, satisfying the relation $c^n = 1$.

8.3 Dihedral groups

Let $n \in \mathbb{Z}_{\geq 3}$ and let us consider the dihedral group D_n. Recall that we have elements $r \in D_n$, $s \in D_n$ and they satisfy relations $r^n = 1$, $s^2 = 1$ and $srs^{-1} = r^{-1}$. If we want to say in this case also, that D_n is specified by having generators r, s and relations $r^n = 1$, $s^2 = 1$ and $srs^{-1} = r^{-1}$, we should understand that in some sense these relations are "enough", they already determine D_n. What is the formalization of this? It is precisely given by the idea hinted at before:

Claim 8.3. *Given a group G, we have a bijection*

$$\mathrm{Hom}(D_n, G) \to \{(g, h) \in G^2 \mid g^n = 1, h^2 = 1, hgh^{-1} = g^{-1}\}$$

given by $\phi \mapsto (\phi(r), \phi(s))$.

8.4 Free groups

In this language of generators and relations, $\mathbb{Z}$ is given by generators and relations as follows: it has generator 1 and an empty set of relations. We can ask, whether there a group F_2 which is given by generators and relations as follows: it has two generators x_1, x_2 and an empty set of relations. In other words, we would like to have a group F_2, together with two elements $x_1, x_2 \in F_2$, such that for any group G the map

$$\mathrm{Hom}(F_2, G) \to G^2$$

given by $\phi \mapsto (\phi(x_1), \phi(x_2))$ is a bijection. Such a group exists, it is called the **free group on two generators**. Similarly, we have the free group on n generators for every $n \in \mathbb{Z}_{\geq 0}$ (and, in fact, also free groups on infinitely many generators...).

9 Abelian groups

9.1 Notation

In this section, we discuss abelian groups and use exclusively additive notation (unless stated otherwise). Let us note that a customary notation for the direct product in this setting is, except $A_1 \times A_2$, also $A_1 \oplus A_2$. In this setting elements of finite order are also called **torsion** elements.

9.2 Some general properties

In abelian groups, the subgroup generated by a set has simpler description than in general, in non-abelian groups.

Lemma 9.1. *Let A be an abelian group and let $S \subset A$ be a subset. Then $\langle S \rangle$ consists precisely of elements in A that can be written as $n_1 s_1 + \ldots + n_k s_k$ for some $k \in \mathbb{Z}_{\geq 0}$, $n_i \in \mathbb{Z}$ and $s_i \in S$. In particular, if $(s_1, \ldots, s_k) \in A^k$ is a finite sequence of elements in A, then*

$$\langle s_1, \ldots, s_k \rangle := \langle \{s_1, \ldots, s_k\} \rangle = \{n_1 s_1 + \ldots + n_k s_k \ : \ n_1, \ldots, n_k \in \mathbb{Z}\}.$$

Proof. An exercise. □

Lemma 9.2. *Let A be an abelian group and let $a_1, a_2 \in a$. Denote by n_1 the order of a_1 and denote by n_2 the order of a_2. Then the order of $a_1 + a_2$ divides $\mathrm{lcm}(n_1, n_2)$.*

Proof. Abbreviate $n := \mathrm{lcm}(n_1, n_2)$. Then $n(a_1 + a_2) = na_1 + na_2 = 0 + 0$ and hence the order of $a_1 + a_2$ divides n. □

9.3 Finite abelian groups

Definition 9.3. Let A be an abelian group and let $n \in \mathbb{Z}_{\geq 0}$. Let us denote

$$A_{(n)} := \{a \in A \mid na = 0\}.$$

In other words, $A_{(n)}$ consists of the elements in A whose order divides n.

Lemma 9.4. *Let A be an abelian group and let $n \in \mathbb{Z}_{\geq 0}$. Then $A_{(n)}$ is a subgroup of A.*

Proof. Since A is abelian, we have $n(a_1 + a_2) = na_1 + na_2$ for all $a_1, a_2 \in A$. Therefore the map $A \to A$ given by $a \mapsto na$ is a group homomorphism. Hence its kernel, which is $A_{(n)}$, is a subgroup of A. □

Definition 9.5. Let A be an abelian group and let $p \in \mathbb{Z}_{\geq 1}$ be a prime number. Let us denote

$$A_{((p))} := \bigcup_{k \in \mathbb{Z}_{\geq 0}} A_{(p^k)}.$$

In other words, $A_{((p))}$ consists of the element of A which are killed by high enough power of p or, in other words, the elements whose order is a power of p.

Lemma 9.6. *Let A be an abelian group and let $p \in \mathbb{Z}_{\geq 1}$ be a prime number. Then $A_{((p))}$ is a subgroup of A.*

Proof. This follows from the more general exercise, that if G is a group and for every $k \in \mathbb{Z}_{\geq 0}$ we are given a subgroup $G_k \subset G$, such that $G_k \subset G_{k+1}$ for all $k \in \mathbb{Z}_{\geq 0}$ then

$$\bigcup_{k \in \mathbb{Z}_{\geq 0}} G_k$$

is a subgroup of G. In other words, the "increasing union" of a sequence of subgroups is a subgroup. □

Lemma 9.7. *Let A be a finite abelian group and let $p \in \mathbb{Z}_{\geq 1}$ be a prime number. Then $A_{((p))}$ is the (unique) p-Sylow subgroup of A.*

Proof. Notice that we know that A has a unique p-Sylow subgroup, because we know that if there is a normal p-Sylow subgroup then it is the unique p-Sylow subgroup, and in an abelian group all subgroups are normal. If we denote by $P \subset A$ the p-Sylow subgroup, then on one hand all elements in P have order dividing $|P|$ and hence have an order which is a power of p, showing that $P \subset A_{((p))}$. On other other hand, given $a \in A_{((p))}$, since the order of a is a power of p, the subgroup $\langle a \rangle$ of A is a p-group, and therefore (as we learned) it is contained in a p-Sylow subgroup, so contained in P, showing that $A_{((p))} \subset P$. □

Claim 9.8. *Let A be a finite abelian group and let $p_1, \ldots, p_k$ be the prime numbers dividing $|A|$. Then*

$$A = A_{((p_1))} \times \ldots \times A_{((p_k))}.$$

Proof. Since $A_{((p_i))}$ is the unique p_i-Sylow subgroup of A, this claim is immediate from Theorem 7.37. However, notice that we don't need really to remember anything about nilpotent groups for this claim (it is too much). The argument is simply that

$$A_{((p_i))} \bigcap \sum_{1 \leq j \leq k, j \neq i} A_{((p_j))} = \{0\}$$

because the order of $\sum_{1 \leq j \leq k, j \neq i} A_{((p_j))}$ divides $\prod_{1 \leq j \leq k, j \neq i} |A_{((p_j))}|$ and hence is relatively prime to the order of $A_{((p_i))}$. And also $\prod_{1 \leq i \leq k} |A_{((p_i))}| = |A|$ (just by counting, since each $A_{((p_i))}$ is a p_i-Sylow subgroup of A) and therefore by Remark 7.36 the claim is valid. □

Proposition 9.9. *Let $p \in \mathbb{Z}_{\geq 1}$ be prime and let A be an abelian p-group. Then A is the finite direct product of some cyclic subgroups. In other words, there exists $k_1, \ldots, k_r \in \mathbb{Z}_{\geq 1}$ and an isomorphism*

$$\mathbb{Z}_{p^{k_1}} \times \ldots \times \mathbb{Z}_{p^{k_r}} \xrightarrow{\sim} A.$$

We will have a lemma before proving the proposition:

Lemma 9.10. *Let A be an abelian p-group. Let $a \in A$ be an element with maximal possible order. Let us denote by $\pi : A \to A/\langle a \rangle$ the canonical projection. Let $\overline{b} \in A/\langle a \rangle$. Then there exists $b \in A$ such that $\pi(b) = \overline{b}$ and b has the same order as $\overline{b}$.*

Proof. Let us denote by p^r the order of a and by p^k the order of $\overline{b}$. Let $b \in \pi^{-1}(\overline{b})$ be any element. The order of $\overline{b}$, which is p^k, divides the order of b. We have $\pi(p^k b) = p^k \overline{b} = 0$ and therefore $p^k b \in \mathrm{Ker}(\pi) = \langle a \rangle$, so we can write $p^k b = na$

for some $n \in \mathbb{Z}$ with $0 \leq n < p^r$. If $n = 0$ then $p^k b = 0$ so the order of b divides p^k, and since it is divisible by p^k, we get that the order of b is p^k, as desired. So let us assume $n \neq 0$. Then we can write $n = p^\ell m$ for $\ell \in \mathbb{Z}_{\geq 0}$ and $m \in \mathbb{Z}_{\geq 1}$ with $\gcd(m, p) = 1$. Since $0 < n < p^r$ we have $\ell \leq r$. The order of na is $p^r/\gcd(p^r, p^\ell m) = p^r/p^\ell = p^{r-\ell}$. The order of b is then, it is easy to see, $p^k \cdot p^{r-\ell} = p^{k+r-\ell}$. Since a is assumed to have maximal possible order among the elements of A, we have $r \geq k + r - \ell$, i.e. $\ell \geq k$. Then we can denote $c := p^{\ell-k} ma$ so that we have $na = p^k c$. Now denote $b' := b - c$. Then, since $c \in \langle a \rangle$, we have $\pi(b') = \bar{b}$. Also, we have $p^k b' = 0$ and therefore b' has order p^k (since, as we said, the order of b' is divisible by the order of $\bar{b} = \pi(b')$ which is p^k). Thus we found an element b' as desired. □

Proof (of Proposition 9.9). The proof is by induction on $|A|$. If $|A| = 1$ then the claim is clear, so assume $|A| > 1$. Let $a \in A$ be an element of maximal possible order. Then $|A/\langle a \rangle| < |A|$ and therefore by the induction hypothesis we can find $k_1, \ldots, k_r \in \mathbb{Z}_{\geq 1}$ and an isomorphism

$$\phi : \mathbb{Z}_{p^{k_1}} \times \ldots \times \mathbb{Z}_{p^{k_r}} \xrightarrow{\sim} A/\langle a \rangle.$$

Let us denote $\bar{b}_i := \phi(0, \ldots, [1]_{p^{k_i}}, \ldots, 0)$ where the $[1]_{p^{k_i}}$ is at the i-th place and all the other components are zeros. Let us, using the previous lemma, find $b_i \in A$ such that $b_i + \langle a \rangle = \bar{b}_i$ and the order of b_i is p^{k_i}. Let us consider the group homomorphism

$$\widetilde{\phi} : \mathbb{Z}_{p^{k_1}} \times \ldots \times \mathbb{Z}_{p^{k_r}} \to A$$

given by

$$\widetilde{\phi}([m_1]_{p^{k_1}}, \ldots, [m_r]_{p^{k_r}}) := m_1 b_1 + \ldots + m_r b_r$$

(see that it is well-defined). It is injective, since its composition with the canonical projection $A \to A/\langle a \rangle$ is ϕ, which is injective. Let us denote by $B \subset A$ the image of $\widetilde{\phi}$ (so that $\widetilde{\phi}$ induces an isomorphism of its source with B). Since the composition of $\widetilde{\phi}$ with the canonical projection $A \to A/\langle a \rangle$ is injective, we in fact have $B \cap \langle a \rangle = \{0\}$. Also, since the composition of $\widetilde{\phi}$ with the canonical projection $A \to A/\langle a \rangle$ is surjective, we have $B + \langle a \rangle = A$. Thus we have $A = \langle a \rangle \times B$. Since B is isomorphic to a product of cyclic groups, we get that A is also isomorphic to a product or cyclic groups, as desired. □

We also have uniqueness:

Proposition 9.11. *Let $p \in \mathbb{Z}_{\geq 1}$ be a prime. If we are given sequences of positive integers $(k_1, \ldots, k_r), (d_1, \ldots, d_s)$ such that*

$$\mathbb{Z}_{p^{k_1}} \times \ldots \times \mathbb{Z}_{p^{k_r}}$$

is isomorphic to

$$\mathbb{Z}_{p^{d_1}} \times \ldots \times \mathbb{Z}_{p^{d_s}},$$

then these sequences coincide up to permutation. Equivalently, for every positive integer k, the number

$$|\{1 \leq i \leq r \mid k_i = k\}|$$

is equal to the number

$$|\{1 \leq i \leq s \mid d_i = k\}|.$$

Proof. Let us denote

$$A := \mathbb{Z}_{p^{k_1}} \times \ldots \times \mathbb{Z}_{p^{k_r}}.$$

Let us denote, for $k \in \mathbb{Z}_{\geq 1}$,

$$\alpha(k) = \{1 \leq i \leq r \mid k_i = k\}.$$

We want to determine α from the abelian p-group A (without knowing about the decomposition we have of A) - this will imply the claim (understand why). Notice that, given $d \in \mathbb{Z}_{\geq 1}$ and $k \in \mathbb{Z}_{\geq 0}$, we have

$$\log_p \left|(\mathbb{Z}_{p^d})_{(p^k)}\right| = \min\{k, d\}.$$

Therefore, for every $k \in \mathbb{Z}_{\geq 0}$, we have

$$\log_p \left|A_{(p^k)}\right| = \sum_{1 \leq i \leq r} \min\{k, k_i\}.$$

Hence, if we denote, for every $k \in \mathbb{Z}_{\geq 0}$,

$$\alpha'(k) := \log_p \left|A_{(p^{k+1})}\right| - \log_p \left|A_{(p^k)}\right|,$$

we have, for every $k \in \mathbb{Z}_{\geq 0}$,

$$\alpha'(k) = |\{1 \leq i \leq r \mid k_i > k\}|.$$

Then, we have, for every $k \in \mathbb{Z}_{\geq 1}$,

$$\alpha(k) = \alpha'(k-1) - \alpha'(k).$$

Thus, we recover α completely from A as an abelian p-group (without knowing how it originated), and the claim follows. □

Now, using Claim 9.8, we obtain the basic uniqueness and existence claim for finite abelian groups:

Theorem 9.12. *Let A be a finite abelian group.*

1. *There exists a finite sequence $(n_1, \ldots, n_r)$ where each n_i is a prime power which is not equal to 1, such that A is isomorphic to*

$$\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}.$$

2. *Given two sequences $(n_1, \ldots, n_r)$ and $(m_1, \ldots, m_s)$ as in the previous item, they coincide up to permutation. Put differently, given any k which is a prime power which is not equal to 1, we have*

$$|\{1 \leq i \leq r \mid n_i = k\}| = |\{1 \leq i \leq s \mid m_i = k\}|.$$

Proof. This is immediate from what we seen (exercise). □

9.4 Finitely generated abelian groups

Definition 9.13. An abelian group is a **torsion group** if all its elements are torsion elements. An abelian group is a **torsion-free group** if all its non-zero elements are non-torsion.

Lemma 9.14. *A finitely generated torsion group is finite.*

Definition 9.15. Let A be an abelian group. We denote by $A_{\text{tor}} \subset A$ the subgroup of torsion elements (check that it is a subgroup!).

Lemma 9.16. *Let A be an abelian group. Then A/A_{tor} is torsion-free.*

Proof. Let us denote by $\pi : A \to A/A_{\text{tor}}$ the canonical projection. Let $y \in A/A_{\text{tor}}$, let $d \in \mathbb{Z}_{\geq 1}$ and assume that $dy = 0$ (we want to show that $y = 0$). Let $x \in \pi^{-1}(y)$. We have $\pi(dx) = d\pi(x) = dy = 0$ and therefore $dx \in A_{\text{tor}}$. Therefore there exists $e \in \mathbb{Z}_{\geq 1}$ such that $edx = 0$. Therefore $x \in A_{\text{tor}}$ and so $y = \pi(x) = 0$. □

Thus, in order to understand finitely generated abelian groups, we want to first try to understand torsion-free finitely generated abelian groups. We will next study one kind of such groups, which will turn out to be the only kind.

9.5 Lattices (finitely generated free abelian groups)

Definition 9.17. Let A be an abelian group. A sequence $a_1, \ldots, a_n \in A$ is a **(finite) $\mathbb{Z}$-basis for** A if for every element $a \in A$ there exists a unique $(d_1, \ldots, d_n) \in \mathbb{Z}^n$ such that $a = d_1 a_1 + \ldots + d_n a_n$. Equivalently, if the group homomorphism

$$\mathbb{Z}^n \to A$$

given by

$$(d_1, \ldots, d_n) \mapsto d_1 a_1 + \ldots + d_n a_n$$

is a group isomorphism.

Definition 9.18. An abelian group L is a **lattice** (or a **finitely generated free abelian group**) if it is isomorphic to $\mathbb{Z}^n$ for some $n \in \mathbb{Z}_{\geq 0}$. Equivalently, if it has a finite $\mathbb{Z}$-basis.

Lemma 9.19. *Let $m, n \in \mathbb{Z}_{\geq 0}$ with $m < n$. Then $\mathbb{Z}^n$ can not be generated by m elements.*

Corollary 9.20. *Let $n_1, n_2 \in \mathbb{Z}_{\geq 0}$. If $n_1 \neq n_2$ then $\mathbb{Z}^{n_1}$ is not isomorphic to $\mathbb{Z}^{n_2}$.*

Definition 9.21. Let L be a lattice. The **rank** of L is the number $n \in \mathbb{Z}_{\geq 0}$ such that L is isomorphic to $\mathbb{Z}^n$ (this is well-defined by the corollary).

Proof (of Lemma 9.19). Suppose that $m, n \in \mathbb{Z}_{\geq 0}$ and that $\mathbb{Z}^n$ can be generated by m elements; we will show that $m \geq n$. Let $v_1, \ldots, v_m \in \mathbb{Z}^n$ be such that

$$\mathbb{Z}^n = \langle v_1, \ldots, v_m \rangle.$$

Let us consider

$$\mathbb{Z}^n \subset \mathbb{Q}^n.$$

Given $v \in \mathbb{Q}^n$, there exists $d \in \mathbb{Z}_{\geq 1}$ such that $dv \in \mathbb{Z}^n$. Then, there exist $k_1, \ldots, k_m \in \mathbb{Z}$ such that

$$dv = k_1 v_1 + \ldots + k_m v_m.$$

If we now think about $\mathbb{Q}^n$ as a vector space over the field $\mathbb{Q}$, we can write there

$$v = \frac{d}{k_1} v_1 + \ldots + \frac{d}{k_m} v_m.$$

Thus, since v was arbitrary, we in fact showed that $v_1, \ldots, v_m$ span $\mathbb{Q}^n$ as a vector space over $\mathbb{Q}$. By linear algebra, we know that then necessarily we must have $m \geq n$, as desired. □

Remark 9.22. Let A and B be abelian groups and let $\pi : A \to B$ be an epimorphism of groups. Denote $K := \mathrm{Ker}(\pi)$. If $C \subset A$ is a subgroup such that $A = K \times C$, then $\pi|_C : C \to B$ is an isomorphism. We then have a monomorphism $s : B \to A$ given by $s(b) = (\pi|_C)^{-1}(b)$ and $\pi \circ s = \mathrm{id}_B$. Conversely, if we have a monomorphism $s : B \to A$ such that $\pi \circ s = \mathrm{id}_B$, then setting $C := \mathrm{Im}(s)$ we have $A = K \times C$. When these equivalent conditions hold, we say that π **admits a splitting**. As an exercise, you can also think about this for non-abelian groups, but then one will not have direct products but semi-direct products...

Lemma 9.23. *Let A be an abelian group, let L be a lattice and let $\pi : A \to L$ be an epimorphism. Then π admits a splitting.*

Proof. Let us denote $B := \mathrm{Ker}(\pi)$. Let $y_1, \ldots, y_m \in L$ be a $\mathbb{Z}$-basis for L. For every $1 \leq i \leq m$, let $x_i \in A$ be such that $\pi(x_i) = y_i$. Let $C := \langle x_1, \ldots, x_m \rangle$. We claim that $A = B \times C$. First, let us see that $B \cap C = \{0\}$. Let $a \in B \cap C$. Then, since $a \in C$, we can write $a = d_1 x_1 + \ldots + d_m x_m$ for some $d_1, \ldots, d_m \in \mathbb{Z}$. Then $\pi(a) = d_1 y_1 + \ldots + d_m y_m$. But $\pi(a) = 0$ because $a \in B$, and therefore we obtain $0 = d_1 y_1 + \ldots + d_m y_m$. Since $y_1, \ldots, y_m$ is a $\mathbb{Z}$-basis for L, we obtain $d_i = 0$ for all $1 \leq i \leq m$ and thus $a = 0$. Thus we showed that $B \cap C = \{0\}$. Now, let us see that $B + C = A$. let $a \in A$. There exists $d_1, \ldots, d_m \in \mathbb{Z}$ such that $\pi(a) = d_1 y_1 + \ldots + d_m y_m$. Denote $c := d_1 x_1 + \ldots + d_m x_m$. Then $c \in C$, and we have $\pi(a - c) = 0$, and so $a - c \in B$, showing that $a \in B + C$. □

Lemma 9.24. *Let L be a lattice and let $M \subset L$ be a subgroup. Then M is also a lattice.*

Proof. Denoting by n the rank of L, the proof is by induction on n. If $n = 0$ the claim is clear. If $n = 1$, the claim follows from the fact that all subgroups of $\mathbb{Z}$ are either isomorphic to $\mathbb{Z}$ (and so lattices of rank 1) or trivial (and so lattices of rank 0). Therefore assume $n > 1$ and let us perform the induction step. Let $x_1, \ldots, x_n$ be a $\mathbb{Z}$-basis for L. Denote $L_1 := \langle x_1, \ldots, x_{n-1} \rangle$ and $L_2 := \langle x_n \rangle$. Then $L = L_1 \times L_2$ and so we have the map $\pi : L \to L_2$ given by sending $x \in L$ to $x_2 \in L_2$, where we (uniquely) write $x = x_1 + x_2$ with $x_1 \in L_1$ and $x_2 \in L_2$. Consider now $\pi|_M : M \to L_2$. Then the image of $\pi|_M$ is a subgroup of L_2 and hence a lattice (by the already considered case of rank 1). Therefore, by the previous lemma M is isomorphic to $\mathrm{Ker}(\pi|_M) \times \mathrm{Im}(\pi|_M)$. But $\mathrm{Ker}(\pi|_M)$ is a subgroup of L_1 and hence a lattice by the induction hypothesis. Thus M is isomorphic to a product of two lattices, and hence itself a lattice. □

Corollary 9.25. *Let A be a finitely generated abelian group and let $B \subset A$ be a subgroup. Then B is also finitely generated.*

Proof. Let $a_1, \ldots, a_n \in A$ be such that $A = \langle a_1, \ldots, a_n \rangle$. Let $\pi : \mathbb{Z}^n \to A$ be the group homomorphism given by

$$(d_1, \ldots, d_n) \mapsto d_1 a_1 + \ldots + d_n a_n.$$

Then π is surjective. Denote $B' := \pi^{-1}(B)$. By the lemma, B' is a lattice, and in particular finitely generated. Since we have an epimorphism $\pi|_{B'} : B' \to B$, B is also finitely generated. □

Proposition 9.26. *Let A be a torsion-free finitely generated abelian group. Then A is a lattice.*

Proof. Let $a_1, \ldots, a_n \in A$ be such that $A = \langle a_1, \ldots, a_n \rangle$. Let us fix a maximal subset $S \subset \{1, \ldots, n\}$ such that $\{a_i\}_{i \in S}$ are $\mathbb{Z}$-linearly independent (i.e. if $\{d_i\}_{i \in S}$ are integers such that $\sum_{i \in S} d_i a_i = 0$ then $d_i = 0$ for all $i \in S$). For notational convenience, by reordering we can assume that $S = \{1, \ldots, m\}$ for $0 \leq m \leq n$. Denote $L := \langle a_1, \ldots, a_m \rangle$. Then $a_1, \ldots, a_m$ is a $\mathbb{Z}$-basis for L. Given $m + 1 \leq i \leq n$, there exists $d_i \in \mathbb{Z}_{\geq 1}$ such that $d_i a_i \in L$. Indeed, otherwise it is easy to see that $a_1, \ldots, a_m, a_i$ is also a $\mathbb{Z}$-linearly independent set, contradicting the maximality of S. Let us denote $d := d_{m+1} \cdot \ldots \cdot d_n$. Consider the group homomorphism $M_d : A \to A$ given by $a \mapsto da$. Since A is torsion-free, M_d is injective. Therefore A is isomorphic to $\mathrm{Im}(M_d)$. But $\mathrm{Im}(M_d) \subset L$ and therefore it is a lattice, by the previous lemma. Hence A is a lattice, as desired. □

9.6 Finitely generated abelian groups again

Claim 9.27. *Let A be a finitely generated abelian group. Then there exists a lattice $L \subset A$ such that $A = A_{\mathrm{tor}} \times L$.*

Proof. Clearly, since A is finitely generated so is A/A_{tor}. Since A/A_{tor} is torsion-free, by the proposition we just saw it is a lattice. Therefore, by a lemma we had the canonical projection $\pi : A \to A/A_{\mathrm{tor}}$ admits a splitting, and so there exists

a subgroup $L \subset A$ such that $A = A_{\text{tor}} \times L$. We also know that $\pi|_L : L \to A/A_{\text{tor}}$ is an isomorphism, and so L is a lattice. □

Corollary 9.28 (Existence part of the basic structural theorem on finitely generated abelian groups)**.** *A finitely generated abelian group is isomorphic to a finite product of cyclic groups, of infinite order or an order which is a prime power not equal to* 1*.*

Proof. This is clear from the claim, because a lattice is isomorphic to a finite product of copies of $\mathbb{Z}$, and a finite abelian group is, as we saw, isomorphic to a finite product of cyclic groups of prime power order. □

We also have uniqueness:

Claim 9.29 (Uniqueness)**.** *Suppose we have two data*

$$(r, (m_1, \ldots, m_k))$$

and

$$(s, (n_1, \ldots, n_\ell))$$

where $r, s \in \mathbb{Z}_{\geq 0}$, $k, \ell \in \mathbb{Z}_{\geq 0}$ and the m_i and n_j are prime powers different from 1*. If*

$$\mathbb{Z}^r \times \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}$$

is isomorphic to

$$\mathbb{Z}^s \times \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_\ell},$$

then $r = s$, $k = \ell$ and $(m_1, \ldots, m_k)$ and $(n_1, \ldots, n_\ell)$ are equal after a permutation.

Proof. Denote by A the abelian group which is the first expression in the statement. Notice that

$$A_{\text{tor}} = \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}$$

(embedded in the obvious way in A, by appending zeros at the $\mathbb{Z}$-places). Therefore by the uniqueness theorem we have already seen for finite abelian groups, applied to A_{tor}, we obtain that $(m_1, \ldots, m_k)$, up to permutation, does not depend on the decomposition chosen. Next, $A/A_{\text{tor}} \cong \mathbb{Z}^r$, and therefore r is the rank of the lattice A/A_{tor} and hence it is also independent of the decomposition. □

9.7 The multiplicative group of a finite field

Let us make a small complement here.

Theorem 9.30. *Let k be a finite field. Then $k^\times$ is a cyclic group.*

We will use a lemma:

Lemma 9.31. *Let G be a finite group, denote $n := |G|$. Suppose that for every $d \in \mathbb{Z}_{\geq 1}$ satisfying $d|n$, we have*

$$\left|\left\{g \in G \mid g^d = 1\right\}\right| \leq d.$$

Then G is cyclic.

Proof. For every $d|n$, let us denote

$$n_d := \left|\{g \in G \mid o_g = d\}\right|.$$

Then

$$n = \sum_{d|n} n_d.$$

Notice, however, that is for some $d|n$ we have $n_d \neq 0$, then if we pick $g \in G$ with $o_g = d$, the elements h of $\langle g \rangle$ all satisfy $h^d = 1$ and there are precisely d such elements, and therefore by the assumption those are all the elements h in G which satisfy $h^d = 1$. In particular, there are precisely $\phi(d)$ elements h in G which satisfy $o_h = d$ (the generators of $\langle g \rangle$), i.e. $n_d = \phi(d)$. Thus, we obtained that either $n_d = 0$ or $n_d = \phi(d)$. But, recall that

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

Therefore, by considering the two sum-expressions for n, it is clear that we must have $n_d = \phi(d)$ for all $d|n$. In particular, for $d = n$, we have $n_n \neq 0$, i.e. there exists an element in G of order n, which means that G is cyclic. □

Proof (of Theorem 9.30). Recall that, since k is a field, for every monic polynomial $f \in k[x]$ of degree $d \in \mathbb{Z}_{\geq 1}$, we have

$$|\{c \in k \mid f(c) = 0\}| \leq d.$$

Let us denote $n := |k^\times|$. Given $d \in \mathbb{Z}_{\geq 1}$ for which $d|n$, considering the polynomial $f(x) := x^d - 1$, we obtain

$$\left|\left\{c \in k^\times \mid c^d = 1\right\}\right| \leq d.$$

By the previous lemma, $k^\times$ is therefore cyclic. □

9.8 Diffie-Hellman secret sharing and Al-Gamal encryption

A beautiful idea (formulated vaguely) is that there are bijections $\phi : X \to Y$ such that for any given $x \in X$ it is easy to compute $\phi(x)$, while for any given $y \in Y$ it is hard (to the point of impracticality) to compute $\phi^{-1}(y)$. We can call such a bijection a **one-way bijection**.

Suppose that we can find $n \in \mathbb{Z}_{\geq 1}$, an abelian group M (for which let us use additive notation) and an isomorphism of groups $e : \mathbb{Z}_n \to M$ which is a

one-way bijection. In other words, M is cyclic of order n, with some generator $m_0 := e([1]_n) \in M$. Let us note that given $\alpha \in \mathbb{Z}_n$ and $m \in M$ we give a meaning to $\alpha m \in M$ by choosing $a \in \mathbb{Z}$ such that $\alpha = [a]_n$ and letting αm be am - since m has order dividing n, the result will not depend on the choice of the representative a. Notice also that we have the property $\alpha e(\beta) = e(\alpha\beta)$ for $\alpha, \beta \in \mathbb{Z}_n$.

Now suppose that Bob wants to send alice a message $m \in M$, over a non-secure channel. First, Alice picks $\alpha \in \mathbb{Z}_n$, called her **private key**, and shares with everybody $e(\alpha) \in M$, called her **public key**. Now, if Bob wants to send alice a message $m \in M$, Bob picks randomly $\beta \in \mathbb{Z}_n$ (his momentary private key) and sends Alice $(m_1, m_2) := (e(\beta), \beta e(\alpha) + m)$. Notice that he used Alice's public key. Now, Alice can find m:

$$m = m_2 - \alpha m_1,$$

because

$$\beta e(\alpha) = e(\beta\alpha) = e(\alpha\beta) = \alpha e(\beta)!$$

One also expresses this, without thinking about the message m, as the ability of Alice and Bob to share a secret - $e(\alpha\beta)$ can be read from $(\alpha, e(\beta))$ (information that Alice knows) and also from $(e(\alpha), \beta)$ (information that Bob knows), but not from $(e(\alpha), e(\beta))$ (information that everybody listening to the channel knows).

As a side remark, let us notice that here Bob uses with each transmission a new private key, because otherwise someone who reads the channel transmission (the massages (m_1, m_2)) could start figuring out frequencies of the messages, and start figuring things out.

A common choice for M is $\mathbb{Z}_p^\times$, where p is a (large) prime number. We saw that this group is cyclic. If one finds a generator of it, one obtains an isomorphism $e : \mathbb{Z}_{p-1} \xrightarrow{\sim} \mathbb{Z}_p^\times$, and it is well-believed to be a one-way bijection. Another choice for M is an appropriately chosen cyclic subgorup of an elliptic curve over a finite field.

10 Basic notions of ring theory

10.1 The definition and examples

Definition 10.1. A **ring** is a triple $(R, +, \cdot)$ where R is a set and $+, \cdot : R \times R \to R$ are functions (we again write $r_1 + r_2$ instead of $+(r_1, r_2)$ and $r_1 \cdot r_2$ or even $r_1 r_2$ instead of $\cdot(r_1, r_2)$, and also the notational convention is that when we don't have brackets, we perform $+$ before $\cdot$) satisfying the following properties:

1. $(R, +)$ is an abelian group.
2. $r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3$ for all $r_1, r_2, r_3 \in R$.
3. There exists an element $1 \in R$ such that $1 \cdot r = r$ and $r \cdot 1 = r$ for all $r \in R$.

4. We have $r \cdot (r_1 + r_2) = r \cdot r_1 + r \cdot r_2$ and $(r_1 + r_2) \cdot r = r_1 \cdot r + r_2 \cdot r$ for all $r, r_1, r_2 \in R$.

A ring $(R, +, \cdot)$ is called **commutative** if $r_1 \cdot r_2 = r_2 \cdot r_1$ for all $r_1, r_2 \in R$.

Remark 10.2. As before, given a ring $(R, +, \cdot)$, the element $1 \in R$ (neutral with respect to $\cdot$) is uniquely determined. We also always write $0 \in R$ for the (uniquely determined) neutral element with respect to $+$.

Remark 10.3. As before, we usually denote a ring $(R, +, \cdot)$ by R, keeping the operations $+$ and $\cdot$ implicit notationally.

Example 10.4. *The trivial commutative ring is the one with one element; a commutative ring having one element is equivalent to* $0 = 1$ *being satisfied in it.*

Example 10.5. *Notice that a field is simply a non-trivial commutative ring* $(R, +, \cdot)$ *such that, in addition, to every* $0 \neq r \in R$ *there exists an inverse, i.e.* $s \in R$ *such that* $r \cdot s = 1$ *and* $s \cdot r = 1$.

Example 10.6. *We have the ring of integers* $(\mathbb{Z}, +, \cdot)$.

Example 10.7. *Given* $n \in \mathbb{Z}_{\geq 1}$, *we have the ring of integers modulo* n, *denoted* $\mathbb{Z}_n$ *- we already defined addition and multiplication elements of* $\mathbb{Z}_n$, *and all the properties required in the definition of a ring are satisfied.*

Example 10.8. *Given a field* k *and* $n \in \mathbb{Z}_{\geq 0}$, *we have the ring* $M_k(n)$ *of* n*-by-*n *matrices over* k, *where addition is the usual element-wise addition and multiplication is the usual matrix multiplication.*

Example 10.9. *Given a field* k, *we have the commutative ring* $k[x]$ *of polynomials over* k *in one variable* x. *If we want a formal definition, we can define* $k[x]$ *to consist of sequences*

$$(c_0, c_1, \ldots) \in k^{\mathbb{Z}_{\geq 0}}$$

satisfying the condition that there exists $n_0 \in \mathbb{Z}_{\geq 0}$ *(depending on the sequence) such that* $c_n = 0$ *for all* $n \geq n_0$. *Addition of such sequences is element-wise, while multiplication is by "convolution":*

$$(c_0, c_1, \ldots) \cdot (d_0, d_1, \ldots) = (c_0 d_0, c_0 d_1 + c_1 d_0, c_0 d_2 + c_1 d_1 + c_2 d_0, \ldots).$$

However, we can think of x *as denoting the sequence* $(0, 1, 0, 0, \ldots)$, *and then instead of* $(c_0, c_1, \ldots, c_n, 0, \ldots)$ *we can write*

$$c_0 + c_1 x + c_2 x^2 + \ldots + c_n x^n.$$

Example 10.10. *Given a field* k *and a vector space* V *over* k, *we have the ring* $\mathrm{End}_k(V)$ *of* k*-linear endomorphisms of* V, *where addition is element-wise and multiplication is composition.*

Example 10.11. *Given an abelian group* A, *we have the ring* $\mathrm{End}(A)$ *of endomorphisms of* A *as a group, where addition is element-wise and multiplication is composition.*

Example 10.12. *A ring R is called a* ***skew field*** *if every non-zero element in it has an inverse. Thus, a field is a commutative skew field. The most famous example of a non-commutative skew field is* ***Hamilton's quaternions****. We can construct them first as a vector space over $\mathbb{R}$, with basis $1, i, j, k$. This gives the addition. As for multiplication, we define it to be the $\mathbb{R}$-bilinear map characterized by the following effect on our basis elements: of course, as the notation hints, $1 \cdot x = x$ and $x \cdot 1 = x$ for all $x \in \{1, i, j, k\}$. Next,*

$$i \cdot i = -1,\ j \cdot j = -1, k \cdot k = -1,$$

and finally

$$i \cdot j = k,\ j \cdot k = i,\ k \cdot i = j$$

and

$$j \cdot i = -k,\ k \cdot j = -i,\ i \cdot k = -j.$$

So, in some sense, the quaternions are like a "three-headed complex-number mutation".

Remark 10.13. Given a ring R, a subset $S \subset R$ is called a **subring** if it is a subgroup with respect to $+$, closed under $\cdot$, and contains 1. A subring of a ring is a ring itself, inheriting the addition and multiplication.

10.2 Ring homomorphisms and isomorphisms

Definition 10.14. Let R and S be rings. A **ring homomorphism** from R to S is a map $\phi : R \to S$ satisfying $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ and $\phi(r_1 \cdot r_2) = \phi(r_1) \cdot \phi(r_2)$ for all $r_1, r_2 \in R$, and also $\phi(1) = 1$.

Remark 10.15. In the definition above, the preservation of addition by ϕ implies that $\phi(0) = 0$, but the preservation of multiplication does not necessarily imply that $\phi(1) = 1$ - for example, we can take ϕ to be constant with value 0, it will preserve addition and multiplication, but will not in general send 1 to 1.

Example 10.16. *Let k be a field, and let $k[x]$ be the ring of polynomials in one variable x over k. Let $d \in k$. We then have a ring homomorphism*

$$\mathrm{ev}_d : k[x] \to k,$$

given by sending $\sum_{i=0}^{n} c_i x^i$ to $\sum_{i=0}^{n} c_i d^i$, called ***evaluation at*** *d. One also denotes, given $p \in k[x]$, $p(d) := \mathrm{ev}_d(p)$.*

Remark 10.17. Given a ring homomorphism $\phi : R \to S$, we define its kernel and image by

$$\mathrm{Ker}(\phi) := \{r \in R \mid \phi(r) = 0\}$$

and

$$\mathrm{Im}(\phi) := \{\phi(r)\ :\ r \in R\}.$$

It is immediate that $\mathrm{Im}(\phi)$ is a subring of S, but $\mathrm{Ker}(\phi)$ is not, in general, a subring of R - it does not contain 1 in general. It also has some extra properties - we will discuss it in the next subsection.

Remark 10.18. We of course have the notion of a **ring isomorphism** - it is a ring homomorphism which admits an inverse ring homomorphism. This is equivalent to it being bijective. We then have the notion of isomorphic rings.

Example 10.19. *Let k be a field and let V be a finite-dimensional vector space over k; denote its dimension by $n \in \mathbb{Z}_{\geq 0}$. Choosing a basis $e_1, \ldots, e_n$ for V over k, we obtain an isomorphism of rings*

$$\phi : \mathrm{End}_k(V) \to M_n(k)$$

as follows. Given $T \in \mathrm{End}_k(V)$, write $T(e_j) = \sum_{1 \leq i \leq n} c_{ij} e_i$ for $c_{ij} \in k$, and then let the (i,j)-element of $\phi(T)$ to be c_{ij}.

10.3 Two-sided ideals and quotient rings

Again we have some natural questions. First, given a surjective ring homomorphism $\phi : R \to S$, what can we say about $\mathrm{Ker}(\phi)$? We want to characterize its properties so that every subset of R with such properties will be the kernel of some surjective ring homomorphism. The relevant definition is:

Definition 10.20. Let R be a ring. A subset $I \subset R$ is called a **two-sided ideal** if:

1. I is a subgroup of R with respect to $+$.
2. For $r \in R$ and $s \in I$ we have $r \cdot s \in I$ and $s \cdot r \in I$.

Remark 10.21. The second condition in the definition above, stronger than being closed under multiplication, can be vaguely thought of as the analog of the condition we had for a normal subgroup, of being closed under multiplication and under conjugation.

Remark 10.22. If R is commutative, we simply say "ideal" instead of a "two-sided ideal". One has also notions of left ideals (where one requires $r \cdot s \in I$ but not $s \cdot r \in I$ above) and right ideals (where one requires $s \cdot r \in I$ but not $r \cdot s \in I$ above), but for commutative rings these are all the same.

Exercise 10.1. *Let $\phi : R \to S$ be a homomorphism of rings. Then* $\mathrm{Ker}(\phi)$ *is a two-sided ideal in R.*

Definition 10.23. Let R be a ring and let $I \subset R$ be a two-sided ideal. We define a ring, denoted R/I and called the **quotient ring** of R by I, as follows. As an abelian group, we let R/I be the quotient group of $(R, +)$ by its subgroup I. we define multiplication by $(r_1 + I) \cdot (r_2 + I) := r_1 \cdot r_2 + I$ for $r_1, r_2 \in I$. One checks that this does not depend on the choice of representatives, and that in this way we obtain a ring R/I. We have the **canonical projection ring homomorphism** $\pi : R \to R/I$, sending r to $r + I$. It is surjective, and its kernel is I.

Example 10.24. *We constructed $\mathbb{Z}_n$ as the quotient group of $\mathbb{Z}$ by the subgroup $\langle n \rangle$. However, in fact, $\langle n \rangle$ is an ideal in $\mathbb{Z}$, and the ring structure on $\mathbb{Z}_n$ is gotten by thinking about it as the quotient ring of $\mathbb{Z}$ by $\langle n \rangle$.*

Exercise 10.2. *We have the **first isomorphism theorem** for rings. Namely, let $\phi : R \to S$ be a ring homomorphism and let $I := \mathrm{Ker}(\phi)$. Then we have an isomorphism of rings*

$$R/I \to \mathrm{Im}(\phi)$$

given by sending $r + I$ to $\phi(r)$.

Definition 10.25. Let R be a ring. Let $\Sigma \subset R$ be a subset. The two-sided ideal in R **generated** by Σ is a two-sided ideal $I \subset R$ satisfying the following two properties:

1. $\Sigma \subset I$.
2. Given a two-sided ideal $J \subset R$ such that $\Sigma \subset J$, we have $I \subset J$.

In other words, it is the "smallest" two-sided ideal in R containing Σ. It always exists - it can be constructed as the intersection of all two-sided ideals in R which contain Σ (there is always one, namely the whole R).

Definition 10.26. Let R be a commutative ring. Given $r, s \in R$ we say that r **divides** s (or that s is **divisible** by r) if there exists $q \in R$ such that $s = qr$. Given $r \in R$, we denote by (r) the subset of R which consists of elements which are divisible by r. It is an ideal in R. In fact (check this!) it is the ideal generated by the subset $\{r\}$. An ideal in R is called a **principal ideal** if it has the form (r) for some $r \in R$.

Exercise 10.3. *Show that there is a bijection between $\mathbb{Z}_{\geq 0}$ and the set of ideals in $\mathbb{Z}$, given by sending n to $(n) = \langle n \rangle$. This bijection satisfies: $n_1 | n_2$ if and only if $(n_2) \subset (n_1)$.*

Exercise 10.4. *Let us consider the evaluation homomorphism $\mathrm{ev}_d : k[x] \to k$. Its kernel is*

$$I_d := \{p \in k[x] \mid p(d) = 0\}.$$

Show that $I_d = (x - d)$. In other words, a polynomial has d as a root if and only if it is divisible by the polynomial $x - d$. Since ev_d is surjective, we obtain an isomorphism of rings

$$k[x]/(x - d) \cong k.$$

Exercise 10.5. *Recall **division with reminder** for polynomials. Given a field k and given $f, g \in k[x]$ with $g \neq 0$, there exist $q, r \in k[x]$ with the degree of r smaller than the degree of g, such that $f = qg + r$.*

Claim 10.27. *Let k be a field. Every ideal in $k[x]$ is a principal ideal. Moreover, given $f_1, f_2 \in k[x]$, we have $(f_1) = (f_2)$ if and only if for some $c \in k^\times$ we have $f_2 = c \cdot f_1$. Thus, there is a bijection between the set of monic polynomials in $k[x]$ and the set of ideals in $k[x]$, given by sending f to (f). This bijection satisfies: $f_1 | f_2$ if and only if $(f_2) \subset (f_1)$.*

Proof. Let us first see the second ("uniqueness") assertion. If $f_1 = 0$ then we immediately see that $f_2 = 0$ and the claim is clear. So let us assume that $f_1 \neq 0$. We have $f_2 = gf_1$ and $f_1 = hf_2$ for some $g, h \in k[x]$. We then have $f_1 = hgf_1$. Since $f_1 \neq 0$, by considering degrees we see that the degree of h and g must be zero, and so in particular $g \in k^\times$ and the claim follows.

Let us now be given an ideal $I \subset k[x]$; let us see that I is a principal ideal. If $I = \{0\}$ then the claim is clear, so assume that $I \neq \{0\}$. Let $f \in I$ be non-zero of minimal possible degree. We claim that $I = (f)$. It is immediate that $(f) \subset I$. To see the converse, let $g \in I$ (we want to see that $g \in (f)$). Using division with reminder, there exist $q, r \in k[x]$ such that $g = qf + r$ and the degree of r is less than the degree of f. But $r = g - qf \in I$, and therefore by the minimality assumption on f we must have $r = 0$. Thus $g = qf \in (f)$, as desired. □

10.4 Simple rings

Definition 10.28. A ring R is called simple if $R \neq \{0\}$ and $\mathrm{Idl}_R = \{0, R\}$.

Claim 10.29. *Skew fields are simple. Partially conversely, a commutative simple ring is a field.*

Proof. Let R be a skew field. Let $I \subset R$ be a two-sided ideal, and assume that $I \neq \{0\}$. We want to see that $I = R$. It is enough to see that $1 \in I$ (why?). Let $0 \neq r \in I$. Since r is invertible, we have $1 = r^{-1}r \in I$.

Now, let R be a commutative simple ring (we want to see that R is a field). Let $0 \neq r \in R$. We want to see that r is invertible, i.e. that there exists $s \in R$ such that $sr = 1$. Consider the ideal $(r) \subset R$. Since it is non-zero (as it contains r), by our assumption it must be equal to R. In particular, $1 \in (r)$, i.e. there exists $s \in R$ such that $sr = 1$, as desired. □

Example 10.30. *Let k be a field and let $n \in \mathbb{Z}_{\geq 1}$. Then $M_n(k)$ is a simple ring.*

Proof. I prefer to think about an n-dimensional vector space V over k and $\mathrm{End}_k(V)$, which is isomorphic to $M_n(k)$. Let $I \subset \mathrm{End}_k(V)$ be a two-sided ideal, and assume that $I \neq \{0\}$. We want to see that $I = \mathrm{End}_k(V)$. Let $0 \neq T \in I$. Let $0 \neq v \in \mathrm{Im}(T)$ and let$w \in T^{-1}(v)$. Let us choose a basis $e_1, \ldots, e_n$ for V over k. Given $1 \leq i \leq n$, let us consider $S_i \in \mathrm{End}_k(V)$ sending e_i to w and e_j to 0, for $j \neq i$. Also, let $T_i \in \mathrm{End}_k(V)$ be arbitrary such that $T_i(v) = e_i$. Then let us denote $M_{i,j} := T_j \circ T \circ S_i \in I$. We have $M_{i,j}(e_r) = e_j$ if $r = j$ and $M_{i,j}(e_r) = 0$ if $r \neq j$. Then $\mathrm{Id}_V = \sum_{1 \leq i \leq n} M_{i,i} \in I$ and so $I = \mathrm{End}_k(V)$, as desired. □

10.5 Maximal ideals

Exercise 10.6. *We have the **correspondence theorem** for rings. Namely, to state a basic version, let us, given a ring R, denote by Idl_R the set of two-sided*

ideals in R. let R be a ring and let $I \subset R$ be a two-sided ideal. Let us denote

$$\mathrm{Idl}_R^I := \{J \in \mathrm{Idl}_R \mid I \subset J\}.$$

Then there is a bijection between Idl_R^I and $\mathrm{Idl}_{R/I}$, given by sending $J \in \mathrm{Idl}_R^I$ to

$$J/I := \{j + I \mid j \in J\} \in \mathrm{Idl}_{R/I},$$

and in the other direction, given by sending $\overline{J} \in \mathrm{Idl}_{R/I}$ to

$$\{r \in R \mid r + I \in \overline{J}\} = \pi^{-1}(\overline{J}) \in \mathrm{Idl}_R^I,$$

where we have denoted by $\pi : R \to R/I$ the canonical projection.

Definition 10.31. Given a ring R, a two-sided ideal $I \subset R$ is called **maximal** if $I \neq R$ and for every two-sided ideal $J \subset R$ satisfying $I \subset J$ we have either $J = I$ or $J = R$.

Exercise 10.7. *Let R be a ring and let $I \subset R$ be a two-sided ideal. Show that I is maximal in R if and only if R/I is a simple ring. In particular, if R is commutative, an ideal $I \subset R$ is maximal if and only if R/I is a field.*

Claim 10.32. *There is a bijection between the set of prime numbers and the set of maximal ideals in $\mathbb{Z}$, given by sending p to (p).*

Proof. This follows from Exercise 10.3. Namely, translating in terms of the bijection there, we are interested in $\mathbb{Z}_{\geq 0}$ with the partial order of division. We have the minimum 1 (which corresponds to $(1) = \mathbb{Z}$), and we are interested in minimal elements in $\mathbb{Z}_{\geq 0} \smallsetminus \{1\}$. Those are clearly the prime numbers. □

Claim 10.33. *Let k be a field. There is a bijection between the set of irreducible monic polynomials in $k[x]$ and the set of maximal ideals in $k[x]$, given by sending p to (p). In particular, if k is algebraically closed, there is a bijection between k and the set of maximal ideals in $k[x]$, given by sending d to $(x - d)$.*

Proof. This follows from Claim 10.27. Namely, translating in terms of the bijection there, we are interested in the set Mon of monic polynomials in $k[x]$, with the partial order of division. In Mon we have the minimum 1 (which corresponds to $(1) = k[x]$), and we are interested in minimal elements in $\mathrm{Mon} \smallsetminus \{1\}$. Those are clearly the irreducible (monic) polynomials. □

A powerful idea in mathematics is a duality between (some sorts of) spaces and (some sorts of) commutative rings. Roughly, given a space, we can associate to it the commutative ring of (some sorts of) functions on that space (where addition and multiplication are point-wise). How to go back, i.e. how to associate (at least on some rough intuitive level) a space to a commutative ring? If we take our space to be the "line" k, where k is an algebraically closed field, an algebraic substitute for "functions" on k is the ring $k[x]$ of polynomials over k in one variable x (indeed, every $p \in k[x]$ defines a function $k \to k$ given

by $d \mapsto p(d)$). There is a natural bijection between k and the set of maximal ideals in $k[x]$, given by sending $d \in k$ to the maximal ideal $(x-d)$. Thus, a general idea is that the set of maximal ideals in a given commutative ring is some sort of "space", such that the ring can be thought of as the ring of functions on that space. In this way, $\mathbb{Z}$ becomes the "ring of functions" on the "space" consisting of prime numbers! More precisely, if R is a commutative ring and $\mathfrak{m} \subset R$ is a maximal ideal, recall that $k(\mathfrak{m}) := R/\mathfrak{m}$ is a field. We can think of it as the "field of possible values of functions in R at the point $\mathfrak{m}$", and given a "function" $f \in R$, its value at the "point" $\mathfrak{m}$ is given by $f + \mathfrak{m} \in R/\mathfrak{m}$. Then a number $n \in \mathbb{Z}$ gives a "function" on the set of prime numbers, whose value at a prime p is $[n]_p$.

10.6 Integral domains, principal ideal domains

Definition 10.34. Given a ring R, we denote by $R^\times$ the subset of R consisting of invertible elements (with respect to the multiplicatiom). We call elements in $R^\times$ the **units** in R. The set $R^\times$ is equipped with the multiplication it inherits from R and, together with it, it becomes a ring.

Lemma-Definition 10.35. *Let R be a commutatvie ring. The relation "divides" (i.e., given $r, s \in R$, $r|s$ if there exists $q \in R$ such that $r = qs$) is transitive and reflexive. If, for $r, s \in R$, we have $r|s$ and $s|r$, we say that r and s are **associates**, and denote $r \sim s$. If r and s are associates then given any $t \in R$ we have $r|t$ if and only if $s|t$ (and also $t|r$ if and only if $t|s$). Put differently, r and s are associated if and only if $(r) = (s)$. The relation $\sim$ is an equivalence relation.*

Definition 10.36. A commutative ring R is called an **integral domain** if for $r, s \in R$, if $rs = 0$ then $r = 0$ or $s = 0$.

Exercise 10.8. *Let R is an integral domain. Given $r, s \in R$, we have $r \sim s$ if and only if $s = qr$ for some $q \in R^\times$.*

Definition 10.37. Let R be an integral domain. An element $p \in R$ is called **prime** if p is not zero and not a unit, and given $r, s \in R$ such that $p|rs$, we have either $p|r$ or $p|s$. An element $p \in R$ is called **irreducible** if p is not zero and not a unit, and given $r, s \in R$ such that $p = rs$, we have either $s \sim p$ (i.e. $r \in R^\times$) or $r \sim p$ (i.e. $s \in R^\times$).

Exercise 10.9. *In an integral domain, prime elements are irreducible.*

Definition 10.38. An integral domain is called a **principal ideal domain** if every ideal in it is principal.

Example 10.39. *The rings $k[x]$ and $\mathbb{Z}$ are principal ideal domains.*

Claim 10.40. *In principal ideal domains, irreducible elements are prime.*

Proof. Let R be a principal ideal domain and let $p \in R$ be an irreducible elements. Let $r, s \in R$ and suppose that $p|rs$ (we want to see that $p|r$ or $p|s$). Let us consider the ideal

$$(p, r) := \{q_1 p + q_2 r \ : \ q_1, q_2 \in R\} \subset R.$$

Since R is a principal ideal domain, there exists $t \in R$ such that $(p, r) = (t)$. So $(p) \subset (p, r) = (t)$ and therefore $t|p$. Since p is irreducible, we have either $t \sim 1$ or $t \sim p$. Notice that $t|r$ (since $r \in (p, r) = (t)$) and therefore in the latter case (that $t \sim p$) we obtain $p|t|r$ as desired. So let us assume that $t \sim 1$. This means that $(p, r) = (1)$ and therefore there exist $q_1, q_2 \in R$ such that $1 = q_1 p + q_2 r$. Then

$$s = s \cdot 1 = s(q_1 p + q_2 r) = s q_1 p + q_2 s r.$$

The first summand is divisible by p, and the second summand is also divisible by p, since sr is. Thus s is divisible by p, as desired. □