Algebra
Lecture Notes

Dima Trushin

2023

Contents

1 Sets

In modern math everything can be formulated in terms of Set Theory, that is in terms of sets and maps. Let me remind some basic facts about sets and maps.

1.1 Definition

Definition 1. A set is a collection of elements.

We denote sets by capital letters like X and Y. If an element x belongs to the collection X, we write $x \in X$. If y does not belong to X, we write $y \notin X$. There is a special set containing no elements. This set is called an empty set and is denoted by $\varnothing$.

If you think of a set you should imagine a sack full of elements. The sack is your set and the elements in the sack are the elements belonging to the set. An empty set becomes a sack with no elements inside.

1.2 Constructors

If you are given a definition of a new math object, the first question to ask is: "How do I construct such an object?" To define a set we need to specify the elements inside the set. For doing that, we use the following notation

$$X = \{x \mid \textbf{condition} \text{ on } x\}$$

Here, we mean that the set X consists of all elements x such that the **condition** on x holds. Let me demonstrate this on examples.

- The set of natural numbers
$$\mathbb{N} = \{x \mid x \text{ is a natural number}\} = \{0, 1, 2, 3, \dots, n, \dots\}$$
- The set of integer numbers
$$\mathbb{Z} = \{x \mid x \text{ is an integer number}\} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$
- The set of real numbers
$$\mathbb{R} = \{x \mid x \text{ is a real number}\}$$
We think of the real numbers as a line containing all possible numbers we use in our calculations.
- The closed interval $[0, 1]$
$$[0, 1] = \{x \in \mathbb{R} \mid 0 \leqslant x \leqslant 1\}$$
Here, I use a slightly different notation. I specified that $x \in \mathbb{R}$ before $|$, this simply means that x must be a real number and the additional condition (the number is between zero and one) is written after $|$.

1.3 Operations on sets

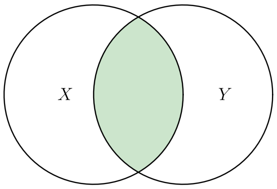
There are several useful procedures you can apply to sets in order to construct new sets. Let us discuss them.

1.3.1 Intersection

If we are given two sets X and Y, then we define the intersection of X and Y as follows

$$X \cap Y = \{z \mid z \in X \text{ and } z \in Y\}$$

If we denote the sets X and Y by discs on a plain then the intersection of X and Y is denoted as below

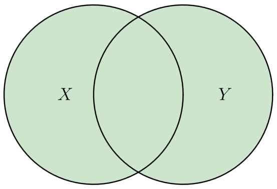


1.3.2 Union

If we are given two sets X and Y, then we define the union of X and Y as follows

$$X \cup Y = \{z \mid z \in X \text{ or } z \in Y\}$$

If we denote the sets X and Y by discs on a plain then the union of X and Y is denoted as below

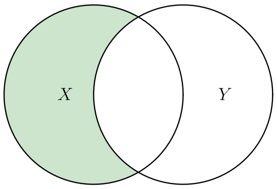


1.3.3 Difference

If we are given two sets X and Y, then we define the difference between X and Y as follows

$$X \setminus Y = \{z \mid z \in X \text{ and } z \notin Y\}$$

If we denote the sets X and Y by discs on a plain then the difference between X and Y is denoted as below



1.3.4 Cartesian product

If we are given two sets X and Y, then their Cartesian product is defined as follows

$$X \times Y = \{(x, y) \mid x \in X,\ y \in Y\}$$

The Cartesian product is simply the set of all possible pairs (x, y) where the first element is taken from X and the second from Y. We will use it every time when we need pairs of elements and not just elements.

1.4 Maps

Definition 2. Suppose we are given two sets X and Y, a map $f\colon X \to Y$ is a rule that takes elements of X to elements of Y. If $x \in X$, then its image in Y is denoted by $f(x)$. In this case, we will write $x \mapsto f(x)$.

The set X is called the source of f and the set Y is called the target of f.

Here is a way to think about maps. Suppose we are given a map $f\colon X \to Y$. Then f is a callable object with an operator $(-)$. You give it any element x of X, then it returns you some specific element $f(x)$ of Y. For each input $x \in X$, the result $f(x) \in Y$ will be the same every time you call it. So, a map is the same thing as a function.

Examples 3. Here are some examples of maps and non maps.

1. The rule $f\colon \mathbb{R} \to \mathbb{R}$ by $x \mapsto 2x + 3$ is a map.

2. The rule $f\colon \mathbb{R} \to \mathbb{R}$ by $x \mapsto \sin(x)$ is a map.

3. The rule $f\colon \mathbb{R} \to \mathbb{R}$ by $x \mapsto \frac{1}{x}$ is not a map because it is not defined at $x = 0$. It becomes a map if we change the source for f. If $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \neq 0\}$, then $f\colon \mathbb{R}^* \to \mathbb{R}$ by $x \mapsto \frac{1}{x}$ is a map.

4. The rule $f\colon \mathbb{R} \to \mathbb{R}$ by $x \mapsto \ln x$ is not a map because it is only defined for positive x. It becomes a map if we change the source for f. If $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$, then $f\colon \mathbb{R}_+ \to \mathbb{R}$ by $x \mapsto \ln x$ is a map.

2 Binary operations

The simplest object in Algebra is a set with a good binary operation. I am going to explain what a binary operation is and the meaning of the word good. Our goal is to define an object called a Group.

2.1 Definition

Definition 4. Suppose X is a set. A binary operation is a map $\circ\colon X \times X \to X$ by the rule $(x, y) \mapsto x \circ y$ for $x, y \in X$.

In this case the notation $\circ$ is the name of the operation. Simply speaking, the operation is a rule that takes two elements of the set X and produce a new element called $x \circ y$ of the same set X. This element $x \circ y$ is usually called the product of x and y.[1]

You should have noticed that we use the name of the operation in a quite unusual way. We write the name between the arguments and not before. This is just for convenience. However, there is a function-like notation (or map-like notation) for binary operations. Let me show you

Definition 5. Suppose X is a set. A binary operation is a map $\mu\colon X \times X \to X$ by the rule $(x, y) \mapsto \mu(x, y)$ for $x, y \in X$.

This is just a different notation for the same mathematical notion. You may denote an operation in operator-like stile (the first definition) or in a function-like style (the second definition). To clarify the situation, let me proceed to a series of examples.

Examples 6. Binary operations:

1. Addition of integral numbers. In an operator-like form

$$+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m + n$$

   In a function-like notation

$$\mathrm{add}\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto \mathrm{add}(m, n) = m + n$$

   Since we got used to addition of numbers in a form $m+n$, we want a general definition to be in a similar form. From the other hand, many programming languages allow us using operator-like and function-like notations for addition. Here I want to emphasize that $\mathrm{add}(m, n)$ and $m+n$ are the same things. These are just different notations of the same addition that we use with integers.

2. Integer multiplication. In an operator-like form

$$\cdot\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m \cdot n$$

   In a function-like notation

$$\mathrm{mult}\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto \mathrm{mult}(m, n) = m \cdot n$$

   Again, these are just two different notations for exactly the same operation, that is, multiplication of integer numbers.

3. Integer maximum. In an operator-like form

$$\vee\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m \vee n$$

   In a function-like notation

$$\max\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto \max(m, n) = m \vee n$$

   Just to clarify $\max(m, n) = m \vee n$ and this is the maximum between m and n.

[1] The operation could be usual addition of integer numbers or taking maximum between two numbers, but from the general point of view the name of the result is product. So, mathematics is the art to call different things in a similar way and similar things in a different way. I will clarify the situation every time when it may lead to confusion.

4. Integer minimum. In an operator-like form

$$\wedge\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\quad (m,n)\mapsto m\wedge n$$

In a function-like notation

$$\min\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\quad (m,n)\mapsto \min(m,n)=m\wedge n$$

Just to clarify $\min(m,n)=m\wedge n$ and this is the minimum between m and n.

5. Some random binary operation on integers

$$\phi\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\quad (m,n)\mapsto m^2-n^2$$

So, in general a binary operation on X is any map $f\colon X\times X\to X$. You are free to define it in a way you wish. But different operations have different properties. Some of the operations are better than the others in a certain way. Since we want to deal with good operations only, I am starting a discussion of operation properties.

2.2 Properties

There are several properties important for our goal. I am going to deal with them one-by-one explaining everything on examples.

2.2.1 Associativity

Definition 7. An operation $\circ\colon X\times X\to X$ is called associative if for every elements $x,y,z\in X$ we have $(x\circ y)\circ z = x\circ(y\circ z)$.

If you have a binary operation $\circ$ on a set X, you can compute the product of three elements x, y, and z in two different ways:

- first compute $w=x\circ y$ and then compute $w\circ z=(x\circ y)\circ z$.
- first compute $u=y\circ z$ and then compute $x\circ u=x\circ(y\circ z)$.

If an operation is arbitrary it may happen that these two products are different for some specific elements x, y, and z. Associativity means that the order of the operations does not matter. Moreover, if $(x\circ y)\circ z=x\circ(y\circ z)$ for any $x,y,z\in X$, then it does not matter how to place parentheses in any product of elements. In particular, we may not use parentheses to specify the order, because in general there is no difference between $(x\circ y)\circ(z\circ w)$, $x\circ(y\circ(z\circ w))$ and $((x\circ y)\circ z)\circ w$, we may call it simply $x\circ y\circ z\circ w$.

Examples 8. Here are examples of associative and non-associative operations.

1. Integer addition is associative. Our operation is

$$+\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\quad (m,n)\mapsto m+n$$

Let $m,n,k\in\mathbb{Z}$ be arbitrary. Then we know that $(m+n)+k=m+(n+k)$.

2. Integer subtraction is not associative. Our operation is

$$-\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\quad (m,n)\mapsto m-n$$

Then the equality $(m-n)-k=m-(n-k)$ does not hold for any integer numbers. Indeed, let us take $m=n=0$ and $k=1$. Then the left-hand side is equal to -1 and the right-hand side is equal to 1. So, $(0-0)-1\neq 0-(0-1)$.

2.2.2 Neutral element

Definition 9. Let $\circ\colon X \times X \to X$ be an operation on X. An element $e \in X$ is called neutral (or identity element) if for every element $x \in X$ we have $x \circ e = x$ and $e \circ x = x$.

So, a neutral element $e \in X$ is such an element that does not change anything when we multiply by it.

Examples 10. A neutral element may exist or may not.

1. Integral addition has a neutral element. Our operation is

$$+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m + n$$

Then it is clear that element $e = 0$ satisfies the required properties. Indeed, for every natural $m \in \mathbb{Z}$ we have $m + 0 = m$ and $0 + m = m$.

2. Integer subtraction has no neutral element. Our operation is

$$-\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m - n$$

Let us show that there is no element $e \in \mathbb{Z}$ such that $e - m = m$ for every $m \in \mathbb{Z}$. Indeed, if such e exists, then $e = 2m$ for any $m \in \mathbb{Z}$. But this is impossible because for $m = 0$, $e = 0$ and for $m = 1$, $e = 2$, a contradiction e must be a specific fixed element not depending on m. From the other hand, it is clear that $m - 0 = m$ for any $m \in \mathbb{Z}$.

The second example shows that it is not enough to check only one condition $x \circ e = x$ or $e \circ x = x$. This is a very common mistake to forget one of these conditions. You are warned!

A reasonable question is: "How many neutral elements may exist?" The answer is: "Not more than one." So, there may be no neutral element at all or just one.

Claim 11. *Let X be a set and $\circ\colon X \times X \to X$ be a binary operation. Then there exists at most one neutral element.*

Proof. If there is no neutral elements, we are done. Suppose that e and e' are neutral elements. We should show that they are the same. Consider the product $e \circ e'$. Since e is a neutral element $e \circ x = x$ for any $x \in X$. In particular, this holds for $x = e'$, that is, $e \circ e' = e'$. From the other hand, since e' is a neutral element $x \circ e' = x$ for any $x \in X$. In particular, this holds for $x = e$, that is, $e \circ e' = e$. Thus $e = e \circ e' = e'$. □

2.2.3 Inverse element

I want to start with a warning. This property depends on the previous one, that is, if an operation does not have a neutral element it is impossible to define inverse elements. This property does not make any sense in case the operation has no neutral element.

Definition 12. Let $\circ\colon X \times X \to X$ be an operation such that there is a neutral element $e \in X$. An element $y \in X$ is called inverse to an element $x \in X$ if $x \circ y = e$ and $y \circ x = e$.

I want to recall that a neutral element is unique if it exists. So, element e is well-defined and there is no confusion.

An excellent question is: "How many inverse elements are there for a particular element $x \in X$?" The answer is: "Not more than one if the operation is associative".

Claim 13. *Let $\circ\colon X \times X \to X$ be an associative binary operation and $e \in X$ is a neutral element. Then, every element $x \in X$ has at most one inverse element.*

Proof. Let us fix an element $x \in X$. If there is no inverse element for x, we are done. Now, suppose that y_1 and y_2 are inverse elements for x. The latter means that

$$\begin{cases} x \circ y_1 = e \\ y_1 \circ x = e \end{cases} \quad \text{and} \quad \begin{cases} x \circ y_2 = e \\ y_2 \circ x = e \end{cases}$$

Now consider the product $y_1 \circ x \circ y_2$. Since, $\circ$ is associative, it does not matter how to put parentheses, that is $(y_1 \circ x) \circ y_2 = y_1 \circ (x \circ y_2)$. Let us compute the left-hand side:

$$(y_1 \circ x) \circ y_2 = e \circ y_2 = y_2$$

And for the right-hand side, we get

$$y_1 \circ (x \circ y_2) = y_1 \circ e = y_1$$

So, $y_2 = (y_1 \circ x) \circ y_2 = y_1 \circ (x \circ y_2) = y_1$ and we are done. □

Hence in general, for every element x if an inverse y exists, then its the only inverse of x. In this case, we denote y as x^{-1}.

Examples 14. 1. Suppose our operation is an integer addition

$$+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m + n$$

Then the only neutral element is 0. If $n \in \mathbb{Z}$, then its inverse is $-n$. Indeed, $n + (-n) = 0$ and $(-n) + n = 0$. Hence, every element has inverse.

2. Suppose our operation is an integer multiplication

$$\cdot\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m \cdot n$$

The only neutral element is 1. If $n = 1$, then its inverse is 1. If $n = -1$, then its inverse is -1. If $n \neq \pm 1$, then there is no inverse in $\mathbb{Z}$. Indeed, if $n = 2$, then there is no integer m such that $nm = 2m = 1$. Hence, only two elements have inverse.

2.2.4 Commutativity

Definition 15. A binary operation $\circ\colon X \times X \to X$ is called commutative if, for every $x, y \in X$, we have $x \circ y = y \circ x$.

So, commutativity means that the order of operands does not matter.

Examples 16. 1. Integral addition is commutative. Our operation is

$$+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m + n$$

Let $m, n \in \mathbb{Z}$ be arbitrary. Then we know that $m + n = n + m$.

2. Integer subtraction is not commutative. Our operation is

$$-\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m - n$$

Then the equality $m - n = n - m$ does not hold for any integer m, n. Indeed, if $m = 0$ and $n = 1$, then the left-hand side is -1 and the right-hand side is 1.

3 Groups

3.1 Definition

Now we are ready to give the most important definition in Algebra, that is the definition of a Group. Before we proceed, I want to clarify the general structure of definitions in Algebra. Every definition of an abstract object consists of two parts: 1) in the first part we list all the data required for the definition, 2) in the second part we list all the axioms the data must satisfy.

Definition 17. Definition of a group.

- **Data:**
  1. A set G.
  2. An operation $\circ\colon G \times G \to G$.
- **Axioms:**
  1. The operation $\circ$ is associative.
  2. The operation $\circ$ has a neutral element.
  3. Every element $x \in G$ has an inverse.

In this case, we say that the pair $(G, \circ)$ is a group. In order to simplify the notation, we usually say simply that G is a group assuming that the operation in use is clear. If in addition we have

4. The operation $\circ$ is commutative.

Then the group G is called abelian or simply commutative.

In short, a group is a set with a good operation. Here, good means that we do not care about parentheses, we have neutral element and every element is invertible but the order of the elements still matters. Abelian group means that additionally the order of the elements does not matter.

Examples 18. 1. Integers with addition $(\mathbb{Z}, +)$ is an abelian group. Indeed, the operation $+$ is associative, has an identity element 0, every element n has inverse $-n$ and the order in addition does not matter, that is $n + m = m + n$. We usually call this group simply $\mathbb{Z}$ assuming the addition as our operation by default.

2. Integers with multiplication $(\mathbb{Z}, \cdot)$ is not a group. Indeed, the operation $\cdot$ is associative, has an identity element 1, but there are a lot of non-invertible elements (the only invertible elements are ± 1).

3. Non-zero real numbers with multiplication $(\mathbb{R}^*, \cdot)$ is an abelian group. Indeed, the operation $\cdot$ is associative, has an identity element 1, every element x as inverse $1/x$, and the order in multiplication does not matter, that is $xy = yx$.

4. Let n be any positive integer, then the set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with operation $a + b \pmod n$ is an abelian group. The operation on $\mathbb{Z}_n$ we will simply be denote by $+$.

5. Let n be any positive integer and $\mathbb{Z}_n^* = \{m \in \mathbb{Z}_n \mid (m, n) = 1\}$ (that is the set of all integers in $\mathbb{Z}_n$ coprime with n) with operation $a \cdot b \pmod n$ is an abelian group. The operation on $\mathbb{Z}_n^*$ will simply be denoted by $\cdot$.

3.2 Multiplicative and additive notations

If we are given a group G, we usually denote its operation by $\circ$. However, it is very cumbersome to use this notation. Instead, people use symbols for usual multiplication or addition and there are two different types of notation: multiplicative and additive. Let me introduce the notation

	Multiplicative	Additive
Operation	$\cdot \colon G \times G \to G$	$+ \colon G \times G \to G$
On elements	$(x, y) \mapsto xy$	$(x, y) \mapsto x + y$
Neutral Element	1	0
Inverse Element	x^{-1}	$-x$
Power of Element	$x^n = \underbrace{x \cdot \ldots \cdot x}_{n}$	$nx = \underbrace{x + \ldots + x}_{n}$

Usually the multiplicative notation is used in case of an arbitrary non-abelian group and the additive notation is used in case of an abelian group. I will mostly stick to the multiplicative notation and use the additive only in case of abelian groups.

I want to emphasize that these are just two different notations for the operation $\circ$. That is $xy = x \circ y$ or $x + y = x \circ y$. You just denote $\circ$ by $\cdot$ or $+$ depending on your preferences. Do not confuse these notations with the usual multiplication and addition. In case of an arbitrary group G, there is no confusion because there is no addition and multiplication on an arbitrary set G. However, If we deal with integer numbers (real, rational, complex, etc.), the operations $+$ and $\cdot$ denote usual addition and multiplication.

3.3 Subgroups

Definition 19. Let G be a group.[2] We define a subgroup H of G.

- **Data:**

  1. A subset $H \subseteq G$.

- **Axioms:**

[2] Strictly speaking $(G, \cdot)$ but I am going to use the short notation all the time.

1. The neutral element 1 of G belongs to H.
2. $xy \in H$ whenever $x, y \in H$.
3. $x^{-1} \in H$ whenever $x \in H$.

In this case, we say that H is a subgroup of G.

It should be noted that if H is a subgroup of G, then $\cdot$ is a well-defined operation on H and $(H, \cdot)$ becomes a group.

Examples 20. Let $G = \mathbb{Z}$ with addition.

1. If $H \subseteq \mathbb{Z}$ is the set of even numbers, that is $H = 2\mathbb{Z}$, then H is a subgroup.
2. If $H \subseteq \mathbb{Z}$ is the set of odd numbers, that is $H = 1 + 2\mathbb{Z}$, then H is not a subgroup. For example, the neutral element 0 is not in H. Also, H is not closed under addition.

3.4 Cyclic subgroups

Let G be a group and $g \in G$ be an arbitrary element. Then we may take any integer power of g as follows

Multiplicative notation	Additive notation
$g^n = \begin{cases} \underbrace{g \cdot \ldots \cdot g}_{n}, & n > 0 \\ 1, & n = 0 \\ \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{-n}, & n < 0 \end{cases}$	$ng = \begin{cases} \underbrace{g + \ldots + g}_{n}, & n > 0 \\ 0, & n = 0 \\ \underbrace{(-g) + \ldots + (-g)}_{-n}, & n < 0 \end{cases}$

Claim 21. *Let G be a group. Then*

1. *For any $x, y \in G$, $(xy)^{-1} = y^{-1}x^{-1}$.*
2. *For any $g \in G$, $(g^{-1})^n = (g^n)^{-1}$.*
3. *For any $g \in G$, $g^n g^m = g^{n+m}$ whenever $n, m \in \mathbb{Z}$.*

Proof. 1) We need to show that $(xy)^{-1} = y^{-1}x^{-1}$. Let us denote $y^{-1}x^{-1}$ by z. If we show that $(xy)z = z(xy) = 1$, this will mean that $z = (xy)^{-1}$ by definition. Now, we compute

$$(xy)z = xyz = xyy^{-1}x^{-1} = xx^{-1} = 1$$

In a similar way, we show the other equality.

2) We apply the previous property several times, that is

$$(g_1 \cdot \ldots \cdot g_n)^{-1} = g_n^{-1} \cdot \ldots \cdot g_1^{-1}, \quad \text{whenever } g_1, \ldots, g_n \in G$$

If we substitute $g_1 = \ldots = g_n = g$, this proves the required for $n > 0$.

If $n = 0$, then by definition $(g^{-1})^0 = 1$. From the other hand, $(g^0)^{-1} = 1^{-1} = 1$ because the inverse for 1 is 1.

If $n < 0$, then by definition

$$(g^{-1})^n = \underbrace{(g^{-1})^{-1} \cdot \ldots \cdot (g^{-1})^{-1}}_{-n}$$

On the other hand,

$$(g^n)^{-1} = (\underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{-n})^{-1} = \underbrace{(g^{-1})^{-1} \cdot \ldots \cdot (g^{-1})^{-1}}_{-n}$$

The latter equality follows from the previous item.

3) We should consider 4 cases:

1. $n \geqslant 0$ and $m \geqslant 0$.
2. $n < 0$ and $m \geqslant 0$.
3. $n \geqslant 0$ and $m < 0$.

4. $n < 0$ and $m < 0$.

In the first case, we have

$$g^n g^m = \underbrace{g \cdot \ldots \cdot g}_{n} \cdot \underbrace{g \cdot \ldots \cdot g}_{m} = \underbrace{g \cdot \ldots \cdot g}_{n+m} = g^{n+m}$$

For convenience, we consider $g^{-n}g^m$ for $n > 0$ and $m \geqslant 0$ in the second case.

$$g^{-n}g^m = \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{n} \cdot \underbrace{g \cdot \ldots \cdot g}_{m}$$

We cancel the factors at the middle of the expression. If $n > m$, we get

$$\underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{n-m} = g^{-n+m}$$

If $n < m$, we get

$$\underbrace{g \cdot \ldots \cdot g}_{m-n} = g^{m-n}$$

if $n = m$ we get $1 = g^{m-n}$. Other cases I leave as an exercise. □

Definition 22. Let G be a group and $g \in G$ be an arbitrary element. Then the set of all integer powers of g, that is,

$$\langle g \rangle = \{\ldots, g^{-2}, g^{-1}, 1, g, g^2, \ldots\}$$

is a subgroup of G. This group is called the cyclic subgroup generated by g. The element g is called a generator of $\langle g \rangle$.

The cyclic subgroup $\langle g \rangle$ is the smallest possible subgroup containing the element g.

Examples 23. 1. The group $(\mathbb{Z}, +)$ is cyclic. There are two different generators 1 and -1.

2. The group $(\mathbb{Z}_n, +)$ is cyclic.

3. The group of permutations on n elements S_n is not cyclic if $n > 2$.

4. The group $(\mathbb{R}, +)$ is not cyclic.

Claim 24. *Let G be a group and $g \in G$ be an arbitrary element. Then there are two options:*

- *If $\operatorname{ord} g = \infty$, then the elements g^n and g^m are different whenever $n, m \in \mathbb{Z}$ are different.*
- *If $\operatorname{ord} g = n < \infty$, then elements $1, g, g^2, \ldots, g^{n-1}$ are different. In this case, the powers are repeated in cycles, that is in the series*

$$\underbrace{\ldots, g^{-2}, g^{-1}}, \underbrace{1, g, g^2, \ldots, g^{n-1}}, \underbrace{g^n, g^{n+1}, \ldots, g^{2n-1}}, \underbrace{g^{2n}, \ldots}$$

$g^{kn}, g^{1+kn}, \ldots, g^{n-1+nk}$ are the same elements as $1, g, \ldots, g^{n-1}$ for any $k \in \mathbb{Z}$. In particular,

$$\langle g \rangle = \{1, g, \ldots g^{n-1}\}$$

Proof. If $g^n \neq g^m$ for all different $m, n \in \mathbb{Z}$, we are in the first case.

Now suppose that $g^n = g^m$ for some integer $m \neq n$. Then we may multiply this equality by g^{-m} and get $g^{n-m} = 1$. Hence, we may assume that for some $n \neq 0$, we have $g^n = 1$. If $n < 0$, multiply by g^{-n}. Thus, we may assume that for some positive integer n, we have $g^n = 1$.

Consider the minimal positive integer n such that $g^n = 1$. I claim that the elements $1, g, \ldots, g^{n-1}$ are different. Indeed, if $g^k = g^s$ for some $k, s \in [0, n-1]$ and $k \geqslant s$, then $g^{k-s} = 1$ and $k - s$ is not zero and is strictly less than n. The latter contradicts to the choice of n. □

It should be noted that n may equal 1 in case g is the neutral element 1.

Definition 25. Let G be a group and $g \in G$ be an arbitrary element. The order of g is the minimal positive natural number such that $g^n = 1$ and ∞ if there is no such a number. The order of g is denoted by $\operatorname{ord} g$.

From the previous Claim it follows that $\operatorname{ord} g$ equals the number of elements in $\langle g\rangle$. Note that $g = 1$ if and only if $\operatorname{ord} g = 1$.

If we use additive notation, that is the operation on the group G is denoted by $+$, then, the order of $g \in G$ is the small positive integer n such that $ng = 0$. The cyclic subgroup generated by g is

$$\langle g\rangle = \{\dots, -2g, -g, 0, g, 2g, \dots\}$$

Definition 26. Let G be a group. If there is an element $g \in G$ such that $\langle g\rangle = G$, then the group G is called cyclic.

Now, I want to describe all subgroups of the integers with addition.

Claim 27. *Every subgroup H of $\mathbb{Z}$, that is $(\mathbb{Z}, +)$, is of the form $k\mathbb{Z}$ for some natural k.*

Proof. Let us check that $k\mathbb{Z}$ is indeed a subgroup for any k. We need to check three properties of the subgroup. First, $k\mathbb{Z}$ is closed under addition. But this is clear by definition. Second, the neutral element, which is zero, belongs to $k\mathbb{Z}$. This is also clear since $0 = k \cdot 0$. Third, for each $m = kh \in k\mathbb{Z}$, its inverse $-m = k(-h)$ is also in $\mathbb{Z}$, and we are done with this part.

Now, let us check that every subgroup H is of the form $k\mathbb{Z}$. If H contains only the neutral element 0, then $H = 0\mathbb{Z}$ and we are done. Suppose H contains non-zero elements. Take an arbitrary non-zero $n \in H$. If $n < 0$, then $-n$ must belong to H by definition of a subgroup. And hence, we may assume that H contains some positive numbers. Let k be the smallest positive number in H. Let us show that $H = k\mathbb{Z}$.

First, $H \supseteq k\mathbb{Z}$. Indeed, if $k \in H$, then by definition of a subgroup every "power" of k is in H. For additive notation this means

$$mk = \underbrace{k + \dots + k}_{m} \in H \quad\text{and}\quad (-n)k = \underbrace{(-k) + \dots + (-k)}_{n} \in H \quad\text{for any}\quad m, n \in \mathbb{N}$$

Hence, $k\mathbb{Z} \subseteq H$.

Now, let us show that $H \subseteq k\mathbb{Z}$. If $n \in H$ is an arbitrary element, let us divide n by k: $n = qk + r$, where $q \in \mathbb{Z}$ and $0 \leqslant r < k$. We already know that $qk \in k\mathbb{Z} \subseteq H$, that is $qk \in H$. Hence, $r = n - qk \in H$. But r is a natural number in H smaller than k. Since k is the smallest positive in H, the only option is $r = 0$. Thus, $n = qk \in k\mathbb{Z}$ and we are done. □

Claim 28. *Every subgroup H of $\mathbb{Z}_n$, that is $(\mathbb{Z}_n, +)$, is of the form $k\mathbb{Z}_n = \{kh \in \mathbb{Z}_n \mid h \in \mathbb{Z}_n\}$ for some positive $k \mid n$.*

Proof. First, let us check that all numbers divisible by k such that $k \mid n$ form a subgroup in $\mathbb{Z}_n$. First, we need to check that $k\mathbb{Z}_n$ is closed under addition modulo n. Suppose $m_1 = kh_1$ and $m_2 = kh_2$ are elements of $k\mathbb{Z}_n$. Then their sum modulo n is a remainder r such that $m_1 + m_2 = r \pmod{n}$. In this case,

$$r = m_1 + m_2 + qn = kh_1 + kh_2 + qn$$

Since k divides n the whole expression above is divisible by k. Hence r is divisible by k. The latter means that $k\mathbb{Z}_n$ is closed under addition modulo n. Second, we need to check that $k\mathbb{Z}_n$ contains the neutral element. This is clear, since $0 = k \cdot 0 \in k\mathbb{Z}_n$. Third, if $m \in k\mathbb{Z}_n$ is a nonzero element, then its inverse is $n - m$. Since n is divisible by k, $n - m$ is divisible by k. Hence, it belongs to $k\mathbb{Z}_n$. In case $m = 0$ its inverse is 0 and is already in $k\mathbb{Z}_n$. Hence, for each $k \mod n$, $k\mathbb{Z}_n$ is a subgroup of $\mathbb{Z}_n$.

Now, let us show, that every subgroup H in $\mathbb{Z}_n$ coincides with a subgroup of the form $k\mathbb{Z}_n$ for $k \mid n$. The subgroup H must contain the neutral element 0. If this is the only element of H, then $H = \{0\} = n\mathbb{Z}_n$ and we are done. So, we may suppose there is a non-zero, and hence positive, element in H. Let k be the smallest positive element of H. By definition the cyclic subgroup of k, that is $k\mathbb{Z}_n$, belongs to H. Thus, we need to show, that $H \subseteq k\mathbb{Z}_n$ and k divides n.

First, let me show that k divides n. Let us divide n with remainder by k, we will get $n = qk + r$, where $0 \leqslant r < k$. Now, $r = n - qk$, hence $r = -qk \pmod{n}$. Since $k \in H$, the latter means that r is also in H. But this contradicts the choice of k (it was the smallest nonzero integer in H). Hence, r must be zero, thus k divides n. Second, let me show that every element of H is in $k\mathbb{Z}_n$. Suppose $h \in H$ is an arbitrary element. Let us divide h with remainder by k, we will get $h = qk + r$. Hence, $r = h - qk$. Since $h \in H$ and $k \in H$, the whole expression $h - qk$ is in H. Hence, $r \in H$. Since k was the smallest positive integer of H, we must have $r = 0$. The latter means that h is divisible by k, that is, h belongs to $k\mathbb{Z}_n$, and we are done. □

3.5 Cosets

Algebra usually tends to study groups using subgroups rather than elements. The main tool here is cosets.

Definition 29. Let G be a group, $H \subseteq G$ a subgroup and $g \in G$ an arbitrary element. Then the set

$$gH = \{gh \mid h \in H\}$$

is called the left coset of H with respect to g. In a similar way, we define right cosets. The set

$$Hg = \{hg \mid h \in H\}$$

is called the right coset of H with respect to g.

Remarks 30.

1. It should be noted that if G is commutative, then there is no difference between left and right cosets for any subgroup $H \subseteq G$.

2. The group H itself is a left coset as well as a right coset. Indeed, $H = 1 \cdot H = H \cdot 1$.

3. In general, the left cost gH need not be the same as the right coset Hg as an example below shows.

Examples 31. Here are some examples of cosets.

1. Let $G = (\mathbb{Z}, +)$ and $H = 2\mathbb{Z}$ the subgroup of even numbers. Then $2\mathbb{Z}$ and $1 + 2\mathbb{Z}$ are the only cosets of H.

2. Let $G = S_3$ and $H = \langle (1,2) \rangle$ the cyclic subgroup generated by the cycle $(1,2)$. We may list all the elements of G and H
$$G = \{1, (1,2), (1,3), (2,3), (1,2,3), (3,2,1)\},\ H = \{1, (1,2)\}$$
Then there are three different left cosets of H
$$H = \{1, (1,2)\},\ (1,3)H = \{(1,3), (1,2,3)\},\ (2,3)H = \{(2,3), (3,2,1)\}$$
And there are three different right cosets of H
$$H = \{1, (1,2)\},\ H(1,3) = \{(1,3), (3,2,1)\},\ H(2,3) = \{(2,3), (1,2,3)\}$$
This example shows that $(1,3)H \neq H(1,3)$. Also, it should be noted that
$$(1,2)H = H,\ (1,3)H = (1,2,3)H,\ (2,3)H = (3,2,1)H$$
So, cosets with respect to different elements may be the same.

3. Let $G = S_n$ be the group of permutations on n elements and $H = A_n$ be the subgroup of even permutations. Then, for any even permutation $\sigma \in A_n$, the set σA_n consists of all even permutations. Similarly, for any odd permutation $\sigma \in S_n \subseteq A_n$, the set σA_n consists of all odd permutations. Hence, there are only two left cosets of A_n
$$A_n \text{ and } (1,2)A_n$$
In a similar way, we can show that there are only two right cosets of A_n
$$A_n \text{ and } A_n(1,2)$$
Moreover, we have shown that $\sigma A_n = A_n \sigma$ for any $\sigma \in S_n$.

Definition 32. Let G be a group and H its subgroup. The subgroup H is normal if its left and right cosets are the same, that is, $gH = Hg$ whenever $g \in G$.

Claim 33. *Let G be a group and H its subgroup. Then, the following are equivalent*

1. *$gH = Hg$ for each $g \in G$.*

2. *$gHg^{-1} = H$ for each $g \in G$.*

3. *$gHg^{-1} \subseteq H$ for each $g \in G$.*

Proof. (1)⇔(2). Suppose $gH = Hg$. Multiply this on the right by g^{-1} and get $gHg^{-1} = H$. And if we are given $gHg^{-1} = H$, multiply this on the right by g and get $gH = Hg$.

(2)⇔(3). We should show that $gHg^{-1} \subseteq H$ for each $g \in G$ implies $gHg^{-1} = H$ for each $g \in G$. The other implication is clear. If $gHg^{-1} \subseteq H$ for each $g \in G$, then it holds for g^{-1} instead of g. Thus, $g^{-1}Hg \subseteq H$ for each $g \in G$. Multiply this on the left by g and get $Hg \subseteq gH$. Then, multiply the latter on the right by g^{-1} and get $H \subseteq gHg^{-1}$. Since $g \in G$ was arbitrary we are done.

□

3.6 The Lagrange Theorem

Properties of cosets Now, I want to prove several properties of the cosets. The important observation here is that all left cosets form a partition of the group G into non-overlapping subsets. The same is true for the right cosets. This observation provides us with some combinatorial tools.

Claim 34. *Let G be a group, $H \subseteq G$ a subgroup and $g_1, g_2 \in G$ be arbitrary elements. Then there are two options:*

1. *The cosets do not intersect each other: $g_1H \cap g_2H = \varnothing$.*
2. *The cosets coincide: $g_1H = g_2H$.*

This means that each element of the group G belongs to exactly one coset.

Proof. If g_1H does not intersect g_2H there is nothing to prove.

Now we assume that the intersection $g_1H \cap g_2H$ is not empty. We need to prove that $g_1H = g_2H$. Suppose $g \in g_1H \cap g_2H$. Since $g \in g_1H$, $g = g_1h_1$ for some $h_1 \in H$. Similarly, $g \in g_2H$ implies $g = g_2h_2$ for some $h_2 \in H$. Hence $g_1h_1 = g_2h_2$. Dividing by h_1 on the right, we get $g_1 = g_2h_2h_1^{-1}$. Since H is a subgroup $h = h_2h_1^{-1} \in H$. We have got $g_1 = g_2h$ for some $h \in H$.

Let us show that $g_1H \subseteq g_2H$. Suppose $g \in g_1H$, that is $g = g_1h'$ for some $h' \in H$. Then, $g = g_2hh' \in g_2H$ because $hh' \in H$. Now, suppose $g \in g_2H$, that is $g = g_2h'$ for some $h' \in H$. Then, $g = g_1h^{-1}h' \in g_1H$ because $h^{-1}h' \in H$. Hence, we have shown $g_2H \subseteq g_1H$. □

Remark 35. It should be noted that $g_1H = g_2H$ if and only if $g_1H \cap g_2H \neq \varnothing$. Moreover, this occurs if and only if there is an element $h \in H$ such that $g_1 = g_2h$. The latter is equivalent to the condition $g_2^{-1}g_1 \in H$. This provides us with a convenient way of checking if two cosets are the same.

Claim 36. *Let G be a group, $H \subseteq G$ be a finite subgroup and $g \in G$ an arbitrary element. Then $|gH| = |H| = |Hg|$.*

Proof. I will prove the claim for left cosets. Let us consider the map

$$\phi\colon H \to gH \quad x \mapsto gx$$

It takes elements of H to elements of gH. From the other hand, there is the inverse map

$$\psi\colon gH \to H \quad x \mapsto g^{-1}x$$

Thus ϕ and ψ are bijections and we are done. □

Claim 37. *Let G be a finite group and $H \subseteq G$ be a subgroup. Then*

1. *The amount of left cosets of H is equal to $|G|/|H|$.*
2. *The amount of right cosets of H is equal to $|G|/|H|$.*

In particular, the number of left and right cosets is the same.

Proof. We will prove the first item. Claim 34 shows that G is a disjoint union of some cosets, that is $G = g_1H \sqcup \ldots \sqcup g_kH$. From the other hand, Claim 36 shows that all the cosets $g_1H, \ldots, g_kH$ have the same amount of elements being equal to $|H|$. Hence

$$|G| = |g_1H| + \ldots + |g_kH| = |H| + \ldots + |H| = k|H|$$

Here k is the number of the distinct left cosets and we are done. □

Definition 38. Let G be a finite group and $H \subseteq G$ be a subgroup. Then the number of the left cosets of H is called index of H and is denoted by $(G : H)$. This number is also coincide with the number of the right cosets of H.

Using this notation, we can rewrite Claim 37 in the following way.

Claim 39 (The Lagrange Theorem)**.** *Let G be a finite group and $H \subseteq G$ be a subgroup. Then, $|G| = (G : H)|H|$*

Corollaries of The Lagrange Theorem

1. Let G be a finite group and $H \subseteq G$ be a subgroup. Then $|H|$ divides $|G|$.

2. Let G be a finite group and $g \in G$ be an arbitrary element. Then $\operatorname{ord}(g)$ divides $|G|$. Indeed, $\operatorname{ord}(g) = |\langle g\rangle|$. But $|\langle g\rangle|$ divides $|G|$ by the previous item.

3. Let G be a finite group and $g \in G$ be an arbitrary element. Then $g^{|G|} = 1$. Indeed, we already know that $|G| = \operatorname{ord}(g)k$. Hence,
$$g^{|G|} = g^{\operatorname{ord}(g)k} = \left(g^{\operatorname{ord}(g)}\right)^k = 1^k = 1$$

4. Let G be a group of prime order p. Then, G is cyclic. Indeed, since the order of G is prime, it is greater than 1. Hence, there is an element $g \in G$ such that $g \neq 1$. Hence $\langle g\rangle$ has order greater than 1. But $|\langle g\rangle|$ divides $|G| = p$. Since p is prime, the only option is $|\langle g\rangle| = p = |G|$. The latter means that $\langle g\rangle = G$ and we are done.

5. The Fermat Little Theorem. Let $p \in \mathbb{Z}$ be a prime number and $a \in \mathbb{Z}$. If p does not divide a, then p divides $a^{p-1} - 1$. Indeed, let us consider the group $(\mathbb{Z}_p^*, \cdot)$. For any element $b \in \mathbb{Z}_p^*$, we have $b^{|\mathbb{Z}_p^*|} = 1 \pmod p$ by item (3). But $\mathbb{Z}_p^*$ has $p-1$ elements. Now, let $a \in \mathbb{Z}$ be comprime with p. We denote its remainder modulo p by b. Then $a^{p-1} = b^{p-1} = 1 \pmod p$ and we are done.

3.7 Homomorphisms and Isomorphisms

We have a lot of different groups in algebra. And we will study a couple of ways to produce new groups from given ones. In this situation, we need a way to compare the groups. How to recognize that we have constructed the same group that we already know? In order to answer this question, we need to explain what it means that two groups are the same. So, we need a way to compare two groups. This leads us to the notions of homomorphism (a way to compare groups) and isomorphism (a way to say that groups are the same). Let me proceed with formal definitions.

Definition 40. Let G and H be groups. We define a homomorphism $\varphi\colon G \to H$.

- **Data** A map $\varphi\colon G \to H$.
- **Axiom** $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ for any $g_1, g_2 \in G$.

In this case φ is called a homomorphism from G to H.

Remark 41. Let me explicitly repeat the definition. We are given a group $(G, \circ)$ and $(H, \cdot)$. A homomorphism $\varphi\colon G \to H$ is a map such that $\varphi(g_1 \circ g_2) = \varphi(g_1)\cdot\varphi(g_2)$. On the left-hand side we take elements g_1 and g_2 from G and multiply them using the operation on G and then send the resulting element to H. On the right-hand side, we send the elements g_1 and g_2 to the group H first and then multiply the images using operation on H.

Examples 42.

1. Let $G = (\mathbb{Z}, +)$ and $H = (\mathbb{Z}_n, +)$, then the map $\pi\colon \mathbb{Z} \to \mathbb{Z}_n$ by the rule $k \mapsto k \pmod n$ is a homomorphism.

2. Let $G = S_n$ be the group of permutations and $H = \mu_2 = \{\pm 1\}$ with multiplication. Then the map $\operatorname{sgn}\colon S_n \to \mu_2$ taking each permutation to its sign (even one goes to 1 and odd one goes to -1) is a homomorphism.

3. Let $G = (\mathrm{GL}_n(\mathbb{R}), \cdot)$ and $H = (\mathbb{R}^*, \cdot)$ be the set of non-zero real numbers with multiplication. Then the map $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ by the rule $A \mapsto \det(A)$ is a homomorphism.

4. Let $G = (\mathbb{R}, +)$ and $H = (\mathbb{R}^*, \cdot)$. Then the map $\exp\colon \mathbb{R} \to \mathbb{R}^*$ by the rule $x \mapsto e^x$ is a homomorphism.

5. Let $G = (\mathbb{Z}, +)$, H be an arbitrary group and $h \in H$ be an arbitrary element. Then the map $\phi\colon \mathbb{Z} \to H$ by the rule $k \mapsto h^k$ is a homomorphism.

6. Let $G = (\mathbb{Z}_n, +)$, H be an arbitrary group and $h \in H$ be an element such that $h^n = 1$. Then the map $\phi\colon \mathbb{Z}_n \to H$ by the rule $k \mapsto h^k$ is a group homomorphism.

Let us prove several properties of homomorphisms.

Claim 43. *Let $\varphi\colon G \to H$ be a homomorphism of groups. Then*

1. $\varphi(1) = 1$, that is the neutral element of G goes to the neutral element of H.

2. *$\varphi(g^{-1}) = \varphi(g)^{-1}$ whenever $g \in G$.*

Proof. 1) We know that $1 = 1 \cdot 1$. Let us apply φ to this equality. Then we get

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1) \in H$$

Now, multiply this equality by $\varphi(1)^{-1}$, we will get $1 = \varphi(1)$.

2) Let $g \in G$ be an arbitrary element. Then, $gg^{-1} = 1$. Let us apply φ to this equality. Then we get

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

Now multiply this on the left by $\varphi(g)^{-1}$. We will get $\varphi(g^{-1}) = \varphi(g)^{-1}$. □

Definition 44. Let G and H be groups. We define an isomorphism $\varphi\colon G \to H$.

- **Data** A homomorphism $\varphi\colon G \to H$.
- **Axiom** φ is bijective.

In this case, φ is called an isomorphism between G and H. If there is an isomorphism between G and H, the groups G and H are called isomorphic.

Let me clarify the definition. First let me explain what it means that $\varphi\colon X \to Y$ is a bijection (between sets). Suppose $X = \{1, 2, 3\}$, $Y = \{a, b, c\}$, and φ works as follows $1 \mapsto a$, $2 \mapsto b$, and $3 \mapsto c$. Then you may think of it like this. The set X is a set of names for your elements and the set Y is a set of some other names for your elements. Than the map φ is a renaming map it just switches the names of the elements. Thus, you may think that Y is the same set as X but with elements named differently.

Now, if $\varphi\colon G \to H$ is an isomorphism of groups, then it is at least a bijection. Hence, it identifies elements of G and H saying that the underlying sets of the groups are the same. Also, the condition $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ means that after this identification the operation on G becomes an operation on H. The latter means that you rename the elements and the operation. Hence, you may think that H is exactly the same group as G but with different set of names for the elements and a different notation for the operation. However, this is essentially the same group. As a corollary, isomorphic groups have exactly the same properties.

Examples 45.

1. Let $G = (\mathbb{Z}_n, +)$ and $H = \mu_n \subseteq \mathbb{C}$ be the set of complex roots of unity with multiplication as an operation. Let us fix a primitive root $\xi \in \mu_n$. Then the map $\mathbb{Z}_n \to \mu_n$ by the rule $k \mapsto \xi^k$ is an isomorphism.

2. Let $G = (\mathbb{Z}, +)$ and
$$H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \;\middle|\; n \in \mathbb{Z} \right\}$$
with multiplication as an operation. Then the map $\varphi\colon \mathbb{Z} \to H$ by the rule $k \mapsto \left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ is an isomorphism.

3. Let $G = (\mathbb{C}, +)$ and $H = (\mathbb{R}^2, +)$. Then the map $\varphi\colon \mathbb{C} \to \mathbb{R}^2$ by the rule $z \mapsto (\operatorname{Re} z, \operatorname{Im} z)$ is an isomorphism.

4. Let $G = (\mathbb{C}^*, \cdot)$ and
$$H = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \text{ such that } a^2 + b^2 \neq 0 \right\}$$
with multiplication as an operation. Then the map $\varphi\colon \mathbb{C}^* \to H$ by the rule $a + bi \mapsto \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ is an isomorphism.

5. Claim 24 says that a cyclic group $G = \langle g \rangle$ is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$ depending on the order of a generator. If $\operatorname{ord} g = \infty$, then $G \simeq \mathbb{Z}$. If $\operatorname{ord} g = n$, then $G \simeq \mathbb{Z}_n$.

With each homomorphism we may associate several subgroups: kernel and image.

Definition 46. Let $\varphi\colon G \to H$ be a homomorphism of groups. Then

1. The kernel of φ is $\ker \varphi = \{g \in G \mid \varphi(g) = 1\} \subseteq G$.

2. The image of φ is $\operatorname{Im} \varphi = \{\varphi(g) \mid g \in G\} = \varphi(G) \subseteq H$.

It should be noted that the kernel is a subset of G (belongs to the source of the map φ) and the image is a subset of H (belongs to the target of the map φ).

Claim 47. *Let $\varphi\colon G \to H$ be a homomorphism of groups. Then*

1. $\operatorname{Im}\varphi \subseteq H$ *is a subgroup.*

2. $\ker\varphi \subseteq G$ *is a normal subgroup.*

3. *The map φ is surjective if and only if* $\operatorname{Im}\varphi = H$.

4. *The map φ is injective if and only if* $\ker\varphi = \{1\}$.

Proof. 1) Let us check all the requirements for being subgroup. First, $1 = \varphi(1) \in \operatorname{Im}\varphi$, hence we have the identity. Second, $\varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) \in \operatorname{Im}\varphi$, thus it is closed under the operation. Third, $\varphi(g)^{-1} = \varphi(g^{-1}) \in \operatorname{Im}\varphi$, therefore it contains the inverse element for every element.

2) Let us check the requirements for the subgroup. First, $\varphi(1) = 1$, hence $1 \in \ker\varphi$ by definition. Second, if $x, y \in \ker\varphi$, then $\varphi(xy) = \varphi(x)\varphi(y) = 1\cdot 1 = 1$. Therefore, $xy \in \ker\varphi$. Third, if $x \in \ker\varphi$, then $\varphi(x^{-1}) = \varphi(x)^{-1} = 1^{-1} = 1$. Hence, $x^{-1} \in \ker\varphi$. We have just verified that $\ker\varphi$ is a subgroup. We should show that $g\ker\varphi = \ker\varphi g$ for every $g \in G$. By Claim 33, we need to show that $g\ker\varphi g^{-1} \subseteq \ker\varphi$ for each $g \in G$. That is we should show that $\varphi(g\ker\varphi g^{-1}) = 1$ for each $g \in G$. Indeed, for each $h \in \ker\varphi$, we have

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)\cdot 1\cdot \varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1) = 1$$

3) This holds trivially by the definition.

4) Suppose φ is injective and $x \in \ker\varphi$. The latter means that $\varphi(x) = 1$. From the other hand, we know that $\varphi(1) = 1$. Hence x and 1 go to the same element 1. This means that $x = 1$ by the injectivity.

Now suppose that $\ker\varphi = \{1\}$. Consider two elements $x, y \in G$ such that $\varphi(x) = \varphi(y)$. Multiplying by $\varphi(x)^{-1}$, we get

$$1 = \varphi(y)\varphi(x)^{-1} = \varphi(y)\varphi(x^{-1}) = \varphi(yx^{-1})$$

Hence $yx^{-1} \in \ker\varphi = \{1\}$. Thus $yx^{-1} = 1$. Therefore $y = x$ and we are done. □

3.8 Product of groups

In general, we do not want to produce new groups from scratch. We want to construct a group using already given ones. There are many different operations in algebra to produce new groups. We are not going to learn all of them. Instead, we discuss the simplest one, which is the most useful one at the same time.

Definition 48. Let G and H be groups, we define a new group $G \times H$ as follows

1. As a set it is a product of underlying sets of the groups: $G \times H = \{(g, h) \mid g \in G,\ h \in H\}$.

2. The operation
$$\cdot\colon (G \times H) \times (G \times H) \to G \times H$$
is given by the rule
$$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2), \quad g_1, g_2, \in G,\ h_1, h_2 \in H$$

The group $G \times H$ is called the product of the groups G and H.

It should be noted that we must show that $G \times H$ is indeed a group. We have just defined the required data for a group. However, we need to check the axioms. Let me recall them.

- The operation is associative, that is
$$(g_1, h_1)\Big((g_2, h_2)(g_3, h_3)\Big) = \Big((g_1, h_1)(g_2, h_2)\Big)(g_3, h_3)$$

- There is an identity, $1 = (1, 1)$.

- Each element has inverse, $(g, h)^{-1} = (g^{-1}, h^{-1})$.

All the properties are verified by a direct computation. I am leaving this as an exercise. If we have several groups $G_1, \ldots, G_k$, we may produce the group $G_1 \times \ldots \times G_k$ in a similar way.

3.9 Finite Abelian Groups

Now I want to focus on the most important class of groups, that is the class of finitely generated abelian groups. Let me start with the definition.

Definition 49. A finite abelian group is a commutative (abelian) group G with finitely many elements.

The definition is not a surprise, the name of the term is clear enough. But pay attention to the next result.

Claim 50. *Let G be a finite abelian group, the G is isomorphic to a group $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$.*

I am not going to prove this result. The proof is not hard but requires some technical tools that we are not going to learn because of the lack of time. Also the proof itself does not reveal any important technique. So it is better to spend our time mastering the way of using the result instead of proving it. Now, I want to show you several examples.

Examples 51. 1. Let $G = \mathbb{Z}_8^*$ with multiplication as an operation. It is obviously a finite abelian group, hence it must be a product of cyclic groups. Indeed, we can check that

$$\mathbb{Z}_8^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$$

and the operation preserving bijection (that is isomorphism) is given by

$$1 \leftrightarrow (0,0),\ 3 \leftrightarrow (1,0),\ 5 \leftrightarrow (0,1),\ 7 \leftrightarrow (1,1)$$

This is not the only way to identify these two groups. We may take a different isomorphism

$$1 \leftrightarrow (0,0),\ 3 \leftrightarrow (1,0),\ 7 \leftrightarrow (0,1),\ 5 \leftrightarrow (1,1)$$

I am not going to describe all possible ways, but it must be clear that there are many different isomorphisms serving our purpose. Note also that the group is not cyclic because there is no element of order 4 in it.

2. Let $G = \mathbb{Z}_9^*$ with multiplication as an operation. This is also a finitely generated abelian group. In this case, we have

$$\mathbb{Z}_9^* \simeq \mathbb{Z}_6$$

and there are two different isomorphisms

$$\begin{aligned} \mathbb{Z}_6 &\to \mathbb{Z}_9^* \\ k &\mapsto 2^k \end{aligned} \quad \text{and} \quad \begin{aligned} \mathbb{Z}_6 &\to \mathbb{Z}_9^* \\ k &\mapsto 5^k \end{aligned}$$

Also note that the group here is cyclic. The elements 2 and 5 are different generators of the group. The isomorphisms above correspond to the choice of a generator.

Claim 52 (The Chinese Remainder Theorem)**.** *Let $m, n \in \mathbb{N}$ be two coprime positive integers, that is $(m,n) = 1$. Then the map*

$$\Phi\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \quad k \mapsto (k \mod m,\ k \mod n)$$

is an isomorphism of groups.

Proof. First, we should check that the map is a homomorphism. We need to show that $\Phi(k+d) = \Phi(k) + \Phi(d)$, that is

$$\Phi(k+d) = ((k+d) \mod m,\ (k+d) \mod n) = ((k \mod m) + (d \mod m),\ (k \mod n) + (d \mod n)) =$$
$$= (k \mod m,\ k \mod n) + (d \mod m,\ d \mod n) = \Phi(k) + \Phi(d)$$

Now, I claim that the homomorphism is injective. Claim 47 item (4) ensures that it is enough to show that the kernel of the homomorphism consists of the identity element only. By definition,

$$\ker \Phi = \{k \in \mathbb{Z}_{mn} \mid k = 0 \pmod m,\ k = 0 \mod n\}$$

Hence $k \in \ker \Phi$ if and only if m divides k and n divides k. Since m and n are coprime, this implies that mn divides k. The latter means that $k = 0$ in $\mathbb{Z}_{mn}$.

In order to prove that Φ is an isomorphism, we need to show that it is surjective. Let us compute the number of elements in both groups. By definition $|\mathbb{Z}_{mn}| = mn$. From the other hand, $|\mathbb{Z}_m \times \mathbb{Z}_n| = |\mathbb{Z}_m| \cdot |\mathbb{Z}_n| = mn$. Hence, Φ is an injective map between two sets of the same size. Hence, it must be bijective and we are done. □

From the previous claim it is clear how to take elements from $\mathbb{Z}_{mn}$ to the product $\mathbb{Z}_m \times \mathbb{Z}_n$. However, It is worth mentioning who to produce the map in the other direction. Since m and n are coprime, we have $1 = um + vn$ for some $u, v \in \mathbb{Z}$ by the Euclidean algorithm. Now consider the element $a_1 = um = 1 - vn$. It is clear that $a_1 \mapsto (0, 1)$ under the action of Φ. Similarly, the element $a_2 = vn = 1 - um$ goes to $(1, 0)$. Hence, the element (a, b) corresponds to the element $aa_1 + ba_2 \pmod{mn}$ in $\mathbb{Z}_{mn}$.

Examples 53.

1. In case $m = 3$ and $n = 2$, we have $\mathbb{Z}_6 \simeq \mathbb{Z}_3 \times \mathbb{Z}_2$. Here element 1 goes to $(1, 1)$. Hence $(1, 1)$ is the generator of the cyclic group $\mathbb{Z}_3 \times \mathbb{Z}_2$. Since $1 = 3 - 2$, we see that 3 goes to $(0, 1)$ and -2 goes to $(1, 0)$ (note that $-2 = 4$ in $\mathbb{Z}_6$). Hence the inverse map is given by $(a, b) \mapsto -2a + 3b = 4a + 3b \pmod 6$.

2. From the other hands, the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic. Hence there is no isomorphism with $\mathbb{Z}_4$.

3. Another example of different presentations of a finite abelian group
$$\mathbb{Z}_{30} \simeq \mathbb{Z}_6 \times \mathbb{Z}_5 \simeq \mathbb{Z}_3 \times \mathbb{Z}_{10} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{15} \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
So, all five different constructions give us the same cyclic group.

4. In general, if $m = p_1^{k_1} \dots p_r^{k_r}$, where p_i are prime, then
$$\mathbb{Z}_m = \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_r^{k_r}}$$

As we saw above, the same finite abelian group may be written in many different ways. How to check quickly that two different representations give us the same group? The answer is given in the next result.

Claim 54. *Let G be a finite abelian group. Then*

1. *G is uniquely presentable in the following form*
$$G = \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_k}, \quad \text{where } 1 < d_1 | d_2 | \dots | d_k \text{ are positive integers}$$

2. *G is uniquely (up to permutation of factors) presentable in the following form*
$$G = \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_r^{k_r}}, \quad \text{where } p_i \text{ are (not necessarily distinct) primes, } k_i \text{ are positive integers}$$

It is important to mention that primes p_i may repeat in the second presentation, that is $\mathbb{Z}_2 \times \mathbb{Z}_4$ is one of the possible cases.

Examples 55.

1. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_6$ and $H = \mathbb{Z}_{12}$. These groups are presented in the first form. Since such a presentation is unique G and H are not isomorphic.

2. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_6$ and $H = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. We see that G is presented in the first form and H is presented in the second one. Let us recompute G into the second form using the Chinese Remainder Theorem
$$G = \mathbb{Z}_2 \times \mathbb{Z}_6 = \mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_3) = H$$
Hence, the groups are isomorphic.

Now I want to formulate a second version of the Chinese Remainder Theorem.

Claim 56. *Let $m, n \in \mathbb{N}$ be two coprime positive integers, that is $(m, n) = 1$. Then the map*
$$\Phi\colon \mathbb{Z}_{mn}^* \to \mathbb{Z}_m^* \times \mathbb{Z}_n^*, \quad k \mapsto (k \mod m, k \mod n)$$
is a well-defined isomorphism of groups.

Proof. We already know that $\Phi\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ is a bijection. It is clear that k is coprime with mn if and only if k is coprime with m and k is coprime with n. The latter means that $\Phi\colon \mathbb{Z}_{mn}^* \to \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ is a bijection.

Second, we should show that Φ preserves multiplication. On the one hand
$$\Phi(k_1 k_2) = (k_1 k_2 \mod m, k_1 k_2 \mod n)$$
From the other hand
$$\Phi(k_1)\Phi(k_2) = (k_1 \mod m, k_1 \mod n)(k_2 \mod m, k_2 \mod n) = (k_1 k_2 \mod m, k_1 k_2 \mod n)$$
□

This result means that we can reduce computation of $\mathbb{Z}_n^*$ to the computation of groups $\mathbb{Z}_{p^k}^*$ where p is prime. Indeed, if $n = p_1^{k_1}\dots p_r^{k_r}$, then

$$\mathbb{Z}_n^* \simeq \mathbb{Z}_{p_1^{k_1}}^* \times \ldots \times \mathbb{Z}_{p_r^{k_r}}^*$$

In order to complete the computation, we need to know the answer for the powers of primes. Here is the required result without proof.

Claim 57. *If p is an odd prime and n is an arbitrary positive integer, then*

$$\mathbb{Z}_{p^n}^* \simeq \mathbb{Z}_{p^{n-1}(p-1)}$$

is a cyclic group. An integer $a \in \mathbb{Z}_{p^n}$ is a generator of $\mathbb{Z}_{p^n}^*$ if and only if a is a generator in $\mathbb{Z}_p^*$ and $a^{p-1} \neq 1 \pmod{p^2}$. Hence, every element of $\mathbb{Z}_{p^n}^*$ is uniquely presented in the form a^k, where $0 \leqslant k < p^{n-1}(p-1)$.

In case of a power of 2, the answer is the following

$$\mathbb{Z}_{2^n}^* \simeq \begin{cases} 0, & n \leqslant 1 \\ \mathbb{Z}_2, & n = 2 \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}, & n \geqslant 3 \end{cases}$$

In case $n = 2$, the group is generated by the element $3 = -1$. In case $n \geqslant 3$, the first factor is generated by $2^n - 1 = -1$ and the second factor is generated by 5. Hence, every element of $\mathbb{Z}_{2^n}^*$ is uniquely presented in the form $\pm 5^k$, where $0 \leqslant k < 2^{n-2}$.

In particular, the group $\mathbb{Z}_p^*$ is cyclic of order $p-1$ for any prime p. We will show this result latter using some abstract algebra.

Claim 58. *An element $m \in \mathbb{Z}_n$ is a generator if and only if m and n are coprime.*

Proof. ($\Rightarrow$). Suppose $(m, n) = d > 1$. Then all elements of $\langle m \rangle$ are divisible by d. In particular, we will never get an element 1. Hence m is not a generator, a contradiction. Therefore m and n are coprime.

($\Leftarrow$). We want to show that $\langle m \rangle = \mathbb{Z}_n$. Since 1 is a generator of $\mathbb{Z}_n$, it is enough to show that $1 \in \langle m \rangle$. Since m and n are coprime, there exist elements $a, b \in \mathbb{Z}$ such that $1 = am + bn$. Hence $1 = am \pmod n$. The latter means that 1 is a-th power of m, thus, $1 \in \langle m \rangle$. □

4 Cryptography

4.1 The setting

Suppose there are you, your spouse, and your lover. And you want to send a message to your lover suggesting a private meeting. Also you have seen recently a receipt from a gun store that someone bought a shotgun and you are one hundred percent sure that it was not you. What to do in such a subtle situation? Cryptography to the rescue! The basic idea behind any cryptographic method is this: there are some procedures that are easy to compute in one direction but are very hard to compute in the opposite one, that is the inverse map is difficult to compute. So, it is easy to encrypt the data but hard to decrypt them. But we do not use these procedures as they are because no one will be able to extract the original data. However, using such procedure, we produce a different one. This new procedure is also easy to compute but the inverse map is hard to compute unless you know some secret information.

Before going straight into details, I need to give you an example of such a procedure. There are two most popular ones.

- The direct procedure is the multiplication of integer numbers and the inverse one is the factorization of an integer.
- The direct procedure is raising to a power in an abelian group and the inverse one is taking logarithm. The inverse one is hard to compute if the abelian group is chosen well enough.

Since we are here to utilize some abstract algebra, I am going to focus on the second case. Suppose G is a group (usually finite abelian, but it does not matter for now), $g \in G$ is an arbitrary element, and $n \in \mathbb{N}$ is a natural number. Then we may compute the element $h = g^n$. It turns out that raising to a power can be done in $O(\log n)$ operations (the algorithm will be explained below). However, suppose now that h is known and either g or n is not. Now, we want to solve one of the following problems

- $h = (?)^n$ for some $? \in G$.
- $h = g^?$ for some $? \in \mathbb{N}$.

Whether these problems are hard to compute or not depends on the choice of the group G and the element h in the first case or g in the second one. But if we chose everything carefully, these problems become hard. The first problem is utilized in RSA problem and the second one in Diffie-Hellman exchange procedure. RSA problem is related to factorization problem of composite numbers and is a very popular method. However, I am going to discuss Diffie-Hellman approach only.

4.2 Exponentiation by squaring

First I want to explain why raising to a power is a very fast operation. Suppose G is a group, $g \in G$ is an element and $n \in \mathbb{N}$ is a positive integer. Then, using multiplicative or additive notation, we have

$$g^n = \begin{cases} g(g^2)^k, & n = 2k+1 \\ (g^2)^k, & n = 2k \end{cases} \quad \text{or} \quad ng = \begin{cases} g + k(2g), & n = 2k+1 \\ k(2g), & n = 2k \end{cases}$$

So, in multiplicative case, the problem is raising to a power and, in additive case, the problem is multiplying by an integer. I will describe the algorithm for the multiplicative notation only.

Input: $g \in G$, $n \in \mathbb{N}$.

Output: $g^n \in G$.

We use three internal variables $r, d \in G$ and $k \in \mathbb{N}$. We maintain the invariant $rd^k = g^n$ all the time. The result will be stored in r. The algorithm terminates when $k = 0$.

Algorithm

```
1. Set $r = 1 \in G$, $d = g \in G$, $k = n \in \mathbb{N}$.
2. In a loop, check if $k$ is odd or even. Terminate the loop if $k = 0$.
    (a) If $k$ is even. Assign $r = r$, $d = d^2$, $k = k/2$.
    (b) If $k$ is odd. Assign $r = r \cdot d$, $d = d^2$, $k = (k-1)/2$.
```

Remarks During the procedure we have $rd^k = g^n$. At the beginning $r = 1$, $d = g$, $k = n$, so this holds. At each step of the loop we have two cases:

- $k = 2m$. Then, $rd^{2m} = r(d^2)^m$. And we update $r = r$, $d = d^2$, and $k = m = k/2$.
- $k = 2m + 1$. Then, $rd^{2m+1} = (rd)(d^2)^m$. And we update $r = rd$, $d = d^2$, and $k = m = (k-1)/2$.

There is a similar procedure as follows. Suppose for simplicity that $n = 11$. Then $11 = 1+2+2^3 = 1+2(1+2(0+2))$. Then

$$g^{11} = g^{1+2(1+2(0+2))} = g(g^{1+2(0+2)})^2 = g(g(g^{0+2})^2)^2 = g(g(g^2)^2)^2$$

If $n = 2^k$, then you need exactly k operations. For example $n = 8 = 2^3$, then $g^8 = ((g^2)^2)^2$. So, there $\log_2 n$ operations. In general, the number of operations is proportional to $\log_2 n$. But I do not want to explain this carefully.

4.3 The Discrete logarithm problem

Let G be a group, $g \in G$, and $h \in \langle g \rangle$. Then the problem to find $n \in \mathbb{N}$ such that $g^n = h$ is called the Discrete logarithm problem. Sometimes this procedure is fast sometimes is not. Here are some examples.

Examples 59.

1. Let $G = \mathbb{Z}$ with addition, $g = 1$, and $h = k$. Then it is clear to everyone that the required $n = k$. Indeed, $ng = h$. The problem here is trivial.

2. Let $G = \mathbb{Z}_m$ with addition, $g = a \in \mathbb{Z}_m$, and $h = b \in \mathbb{Z}_n$. Then, the problem is to find $n \in \mathbb{N}$ such that $na = b \pmod m$. This can be solved effectively using Euclidean division algorithm.

3. Let p be a prime number, $G = \mathbb{Z}_p^*$ with multiplication and $g = a \in \mathbb{Z}_p^*$ be a generator of the group, and $h = b \in \mathbb{Z}_p^*$. Then the problem is to find $n \in \mathbb{N}$ such that $a^n = b \pmod{p}$. Well, the experience of the humankind tells us that this problem should be extremely complicated and there is only on option to solve it: the brute force approach.

4.4 Diffie-Hellman

Here I am going to explain the communication process using Diffie-Hellman approach. First, we need to fix a cyclic group G, its generator $g \in G$, and we denote the order of G by n. A natural choice for G is $\mathbb{Z}_p^*$, where p is prime. Finding a generator is unpleasant but we should do this only once.

Let me recall the situation we are in. We have three participants: you, your spouse, and your lover. The communication process consists of several steps:

1. Transform a message (or a part of a message) into an element t of the group G.
2. Encrypt the element t, that is apply some transformation and get $t' \in G$. The element t' is then broadcasted.
3. The element t' is decrypted using some special information to recover the element t.
4. The element t is transformed to the initial message (or the part of the message).

The steps (1) and (4) are usually performed using some table and the table is known to every participant. Do not worry, your spouse knows how to do these steps.

Key exchange Before sending any messages you and your lover must do some preparations to produce a private key and only then the communication begins.

On the diagram below, we show what each participant knows at any step of the process. Let me recall that $G = \langle g \rangle$ and $n = |G|$.

Participants	You	Your spouse	Your lover
Knowledge	G, g, n	G, g, n	G, g, n

You randomly generate a number $a \in \mathbb{Z}_n^*$ and compute $r = g^a \in G$. Your lover randomly generates a number $b \in \mathbb{Z}_n^*$ and computes $s = g^b \in G$.

Participants	You	Your spouse	Your lover
Knowledge	G, g, n $r{=}g^a$	G, g, n	G, g, n $s{=}g^b$

You and your lover broadcast elements r and s. Hence, everyone knows r and s as the result. But no one knows the elements a and b because this is the discrete logarithm problem in G and we have chosen G and $g \in G$ such that the problem is hard to solve.

Participants	You	Your spouse	Your lover
Knowledge	G, g, n $r{=}g^a$, s	G, g, n r, s	G, g, n $s{=}g^b$, r

You raise element s to the power a and get $s^a = (g^b)^a = g^{ab}$. Your lover raises r to the power b and gets $r^b = (g^a)^b = g^{ab}$. Now you and your lover know the secret key $k = g^{ab}$.

Participants	You	Your spouse	Your lover
Knowledge	G, g, n $r{=}g^a$, s $k{=}s^a$	G, g, n r, s	G, g, n $s{=}g^b$, r $k{=}r^b$

As the result you and your lover know the secret key $k \in G$ and no one even your spouse has a way of finding the key. But in order this to be robust we need to choose G and $g \in G$ carefully. No one wants to find out who bought the shotgun.

Broadcast Now its time to send sweet messages to each other. As I have described already, we should translate all the messages to the elements of the group G. Suppose we use English alphabet with 26 symbols. We will use period, comma, exclamation mark, and space symbol as well. Hence, we have 30 symbols at all. There are 30^m sequences with m symbols. If $30^m \leqslant n$, we may map all the sequences to the elements of the group G. This allows us to transform messages to sequences of elements of the group G.

From now, I am going to ignore the translation stage. Our goal is to send an element of the group G. Suppose you have an element $h \in G$ and want to send it to your lover.

Participants	You	Your spouse	Your lover
Knowledge	G, g, n r=g^a, s k=s^a h	G, g, n r, s	G, g, n s=g^b, r k=r^b

Now you encrypt your element h multiplying it by the secret k and send the result $m = hk$ to your lover.

Participants	You	Your spouse	Your lover
Knowledge	G, g, n r=g^a, s k=s^a h, $m = hk$	G, g, n r, s m	G, g, n s=g^b, r k=r^b m

Your lover decrypts the message by computing $h = mk^{-1} = mk^{n-1}$. It should be noted that the inverse k^{-1} is computed using Corollary 3 of the Lagrange Theorem, that is $k^{-1} = k^{n-1}$, because $n = |G|$.[3]

Participants	You	Your spouse	Your lover
Knowledge	G, g, n r=g^a, s k=s^a h, $m = hk$	G, g, n r, s m	G, g, n s=g^b, r k=r^b m, $h = mk^{n-1}$

And voilà. No one got shot and the private meeting was worth it.

ElGamal encryption In the system described above, the private key k remains the same during the communication process.This fact can be used to compromise the system. In order to increase robustness of the system we may change the secret key after each d messages or even after each message.

Let me describe a one-way communication system based on this idea. First, you must publish your public key. This stage is considered as an invitation to communicate. Now, the lover can send messages to you. On the next stage the lover sends a sequence of messages such that each of the messages is encrypted by its own private key. Below, I will explain the whole process in details.

In order to initiate the incoming transmission, you should invent a secret integer $a \in \mathbb{Z}_n^*$ and publish the open key $r = g^a$.

Participants	You	Your spouse	Your lover
Knowledge	G, g, n r=g^a	G, g, n r	G, g, n r

Now, assume that the lover has a sequence of messages $h_1, \dots, h_k$. For each message h_i she or he should randomly choose a secret integer $b_i \in \mathbb{Z}_n^*$. Then the lover generates the corresponding public and private keys as follows $s_i = g^{b_i}$ and $k_i = r^{b_i}$. Then she or he encrypts each message using the private key $m_i = h_i k_i$. And finally, the lover transmits the sequence $(m_1, s_1), \dots, (m_k, s_k)$.

Participants	You	Your spouse	Your lover
Knowledge	G, g, n r=g^a (m_i, s_i)	G, g, n r (m_i, s_i)	G, g, n r $h_1, \dots, h_k$$\in G$ $b_1, \dots, b_k$$\in \mathbb{Z}_n^*$ $s_i = g^{b_i}$, $k_i = r^{b_i}$ $m_i = h_i k_i$

[3] If the group G has an effective way to compute the inverse, you should apply that specific algorithm. For example, in case $G = \mathbb{Z}_p^*$ such an algorithm exists and is based on the extended Euclidean algorithm.

In order to decrypt the messages, we should produce the corresponding private key using the public key of the lover $k_i = s_i^a$. Now one else can do this, because now one knows a but you. Then, we recover the original message using the rule $h_i = m_i k_i^{-1}$.

Participants	You	Your spouse	Your lover
Knowledge	G, g, n $r{=}g^a$ (m_i, s_i) $k_i = {s_i}^a$, $h_i = m_i {k_i}^{-1}$	G, g, n r (m_i, s_i)	G, g, n r $h_1, \dots, h_k \in G$ $b_1, \dots, b_k \in \mathbb{Z}_n^*$ $s_i = g^{b_i}$, $k_i = r^{b_i}$ $m_i = h_i k_i$

If we want to communicate in the opposite direction, we should repeat the process from the beginning changing the roles. That is, your lover should publish her or his public key as an invitation to receive messages. And then you repeat the whole process from your side.

4.5 RSA

Let me explain the principals of a different encryption system. This one is based on the fact that it is very easy to multiply numbers but hard to factor them. The system is called RSA. This is a one-way communication system.

Suppose we are given $n = pq$, where p and q are distinct prime numbers. Let us take $G = \mathbb{Z}_n^*$. Using the multiplicative version of the Chinese Remainder Theorem we know that

$$\mathbb{Z}_n^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^* \simeq \mathbb{Z}_{p-1} \times \mathbb{Z}_{q-1}$$

Hence $|G| = (p-1)(q-1)$. Usually $|\mathbb{Z}_m^*|$ is denoted by $\varphi(m)$ and is called the Euler function.

Suppose we are given two integers $e, d \in \mathbb{Z}$ and an element $h \in \mathbb{Z}_n^*$. If we raise h to the power of e, we will get h^e. Now we want to recover h by raising h^e to the power d. That is, we want $h^{ed} = h$ whenever h is in $\mathbb{Z}_n^*$. In order to ensure that this happens, it is enough to have $ed = 1 \pmod{\varphi(n)}$. Indeed,

$$h^{ed} = h^{1+|\mathbb{Z}_n^*|k} = h\left(h^{|\mathbb{Z}_n^*|}\right)^k = h \text{ in } \mathbb{Z}_n^*$$

This means that the map $\mathbb{Z}_n^* \to \mathbb{Z}_n^*$ by the rule $h \mapsto h^e$ is a permutation of elements of the group. And if e was chosen randomly, we expect that it is hard to solve the problem $x^e = m$ in $\mathbb{Z}_n^*$. For example it is a bad idea to take e to be 1 or 2 or something like that. If we want to generate e we choose e from $\mathbb{Z}_{\varphi(n)}^*$. And if e was chosen appropriately solving $x^e = m$ is a hard task.

Establishing a connection If you want to make an invitation to receive incoming transmission you need some preparation work to be done. First you need to generate two huge prime numbers p and q and then compute their product $n = pq$. We will use the group $G = \mathbb{Z}_n^*$ as the set of messages. Thus we publish n and G.

Participants	You	Your spouse	Your lover
Knowledge	p, q, $n = pq$	n, $\mathbb{Z}_n^*$	n, $\mathbb{Z}_n^*$

Now, we produce an open key as follows. We generate $e \in \mathbb{Z}_{\varphi(n)}^*$. Then the open key is the pair (e, n).

Participants	You	Your spouse	Your lover
Knowledge	p, q, $n = pq$ e	n, $\mathbb{Z}_n^*$ (e, n)	$\mathbb{Z}_n^*$ (e, n)

The next step is to generate the private key. We find $d \in \mathbb{Z}_{\varphi(n)}^*$ such that $de = 1$ in $\mathbb{Z}_{\varphi(n)}^*$. This can be done using the extended Euclidean algorithm applied to e and $\varphi(n)$. The private key is the pair (d, n).

Participants	You	Your spouse	Your lover
Knowledge	p, q, $n = pq$ e $de = 1 \pmod{\varphi(n)}$	n, $\mathbb{Z}_n^*$ (e, n)	$\mathbb{Z}_n^*$ (e, n)

Communication Suppose the lover wants to send a message $h \in \mathbb{Z}_n^*$. She or he encrypts the message using the rule $m = h^e \pmod{n}$ and sends m by the network.

Participants	You	Your spouse	Your lover
Knowledge	p, q, $n = pq$	n, $\mathbb{Z}_n^*$	$\mathbb{Z}_n^*$
	e	(e, n)	(e, n)
	$de = 1 \pmod{\varphi(n)}$		$h \in \mathbb{Z}_n^*$
	m	m	$m = h^e \pmod{n}$

In order to decrypt the message we apply the map $h = m^d \pmod{n}$. This method works because of the choice of e and d.

Participants	You	Your spouse	Your lover
Knowledge	p, q, $n = pq$	n, $\mathbb{Z}_n^*$	$\mathbb{Z}_n^*$
	e	(e, n)	(e, n)
	$de = 1 \pmod{\varphi(n)}$		$h \in \mathbb{Z}_n^*$
	m	m	$m = h^e \pmod{n}$
	$h = m^d \pmod{n}$		

Let us discuss why this approach is reliable. As we can see at the beginning of the communication process p, q, $\varphi(n) = (p-1)(q-1)$, and d is a secret information. However, everyone knows $n = pq$ and e such that $ed = 1 \pmod{\varphi(n)}$. If we know n, then it is hard to recover p and q because the factorization is a hard problem. One can show, that if you know $n = pq$, then computation of $\varphi(n)$ is equivalent to knowing p and q. Hence, no one knows $\varphi(n)$. Hence, it is impossible to recover d because we do not know two numbers out of three in the equality $ed = 1 \pmod{\varphi(n)}$. Thus we believe that it is impossible to recover the secret key. When we send a message h^e, we believe that solving the equation $x^e = m$ is also hard (there are some requirements on e for this to happen). This more or less explains why the system is robust. If you want to implement this system you should read the official standard explaining details of how to make a good choice of all the parameters.