A visit to group theory and elementary number theory

Zhen DING ✉

March 1, 2023

This lecture note will present some basic results in elementary number theory from a viewpoint of group theory. I will try my best to show how natural is a group in this section and followed by a short survey on the plot-line of our main topics.

1 What is a group?

Claim 1.1. *Group theory is a study of symmetry.*

Mathematics is essentially the study of universally existing structures. We study the components within structures, as well as the connections between structures. The Bourbaki school classifies mathematical structures into three main classes as follows:

. Order structures . Algebraic structures . Topological structures

The reason for studying these structures is that they are ubiquitous.

Higher-order mathematical structures are basically regroups of the three basic types of structure, for example, a Lie group is an algebraic structure called a group and a topological/differential structure called a smooth manifold embedded in each other.

Let us first imagine an arbitrary new universe which may contain any thing which may not have any physical properties known to us

Assuming that these things are different in any way, so it is conceivable that we can compare them, even if all of them are identical, so that their "spatial" positions can be used for comparison, and any kind of comparison can confirm the existence of an order.

Suppose these things are lined up in front of us, and we can give them new names, for example naming the nearest thing in front of us '1' and the next closest '2', even though the number of things in front of us is finite, we can imagine that the process can go on indefinitely. And we name ourselves at the very front of the queue as "0"

In other words, we get one of the most familiar mathematical concepts: the natural numbers

Definition 1.2 (Natural Number)**.**

$$\mathbb{N} := \{0, 1, 2, 3, 4, \cdots, \infty\}$$

/

The notion of a set is also extremely natural. We can imagine a bubble in space that encloses certain things, in other words, forms a scope of the description, which then constitutes a set.

For example, if we can imagine a bubble A containing two things and another bubble, B, containing three things, it is also easy to imagine a larger bubble C enclosing these two bubbles, so that C would contain five things.

In other words, we are defining so called addition here. Addition is essentially a binary operation *i.e.* a function that sends two elements of a set onto one element of that set according to certain rules.

Definition 1.3 (Binary Operation)**.** *A Binary operation on a set E is a function from the catersien product of E to E itself, given by*

$$\circ : E \times E \to E, (x, y) \mapsto x \circ y$$

We can also imagine the inverse procedure of addition *i.e.* bursting the big bubble C and splitting the whole into two smaller components A and B. This is what we know as subtraction. We can define equivalently that subtraction procedure by a number as a new number, for example by adding -3 instead of subtracting 3.*i.e.* for every natural number x, there is a number symmetric to it about 0, called $-x$, so that we have invented integer.

Definition 1.4 (Integer)**.**

$$\mathbb{Z} := \{-\infty, \cdots, -2, -1, 0, 1, 2, \cdots, \infty\}$$

It is significant to note that we have used the word 'symmetry' in the description just given. Let us better characterise this symmetry.

For any number x in the integers, there exists $-x$. and the following conditions are satisfied:

Notation.

- $\forall x \in E$: for all elements in E
- $\exists x \in E$: there exists an element in E named x

Summary. $\forall x, y, z \in \mathbb{Z}$

1. $(x + y) \in \mathbb{Z}$
2. $(x + y) + z = x + (y + z)$
3. $x + (-x) = (-x) + x = 0$
4. $x + 0 = 0 + x = x$

/

Multiplication is defined as an accumulation of addition By the same mechanism, we can treat the inverse of multiplying a number as a new number, e.g. the inverse of multiplying by 3 as multiplying by $\frac{1}{3}$. In this way, we have the concept of a fraction.

Putting all the fractions together, we get $\mathbb{Q}$: the rational numbers

And, we will see that rational numbers have the same properties about multiplication as the above Summary few flats:

Summary. $\forall a, b, c \in \mathbb{Q}$

1. $(a \cdot b) \in \mathbb{Q}$
2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. $a \cdot \left(\frac{1}{a}\right) = \left(\frac{1}{a}\right) \cdot a = 1$
4. $a \cdot 1 = 1 \cdot a = a$

We name the centres of symmetry such as 0 for addtion or 1 for multiplication as Neutral elements or Zero elements, and the image of an element after symmetry as its inverse element such as $-x$ for addtion or x^{-1} for multiplication.

Note! Here x^{-1} does not refer necessarily to $\frac{1}{x}$, but to the inverse of x in the context

Definition 1.5 (Group)**.** *A Group $(G, \circ)$ is a set G together with a binary operation $\circ : G \times G \to G$ such that*
1.Closure: $\forall a, b \in G; (a \circ b) \in G$
2.Associativity: $\forall a, b, c \in G, (a \circ b) \circ c = a \circ (b \circ c)$
3.Existence of Zero element: $\forall a \in G, a \circ a^{-1} = a^{-1} \circ a = 1$
4.Existence of inverse: $\forall a \in G, a \circ 1 = 1 \circ a = a$

If a group satisfies the following condition. We call it an abelian group.

Definition 1.6 (Abelian Group)**.**

(G, $\circ$) : Abelian $\iff \forall a, b \in G, a \circ b = b \circ a$

2 A short survey into groups

2.1 A sense of category

When we study any field or topic, we are more interested in the connections between things than in the things themselves. Chemistry, for example, is essentially a study of "connections between atoms", and sociology is essentially a study of connections between people.

Definition 2.1 (Category)**.** *A Category is the content of a specific "set" of things and the possible connections between things.*

Example 2.2 (**Set**)**.** *The category* **Set** *contains all sets and all possible functions between sets*

So, naturally, there may exist a so called "category of Groups" where every groups is an object in that category. But what is the analog of "functions between sets" in group theory? Since group is a structure that is built on sets and therefore contains more information than its underlying sets. So it is natural to ask this "functions between groups" to transmit more information *i.e.* maintain the structure on set after transformation.

Definition 2.3 (Homomorphism)**.** *Suppose* $(G, \circ)$ *and* $(H, \cdot)$ *two groups. a function* $\phi : G \to H$ *is a Homomorphism iff* $\forall x, y \in G, \phi(x \circ y) = \phi(x) \cdot \phi(y)$

Hence, we get our category of groups, we denote it as **Grp**

Definition 2.4 (**Grp**)**.** *The category* **Grp** *contains all groups and all possible homomorphism between groups*

2.2 Two isomorphic groups

Two sets are the same if they contain the same things. But how to capture the sameness of two groups? We require their structure to be the same.

Definition 2.5 (Isomorphism)**.** *A homomorphism* $\phi : G \to H$ *is a Isomorphism* $\iff$ *it is bijective* i.e. *there is a one-to-one correspondence of elements between their underlying sets.*

To make sure that everything goes in a precise litterature. I present here two examples of groups that are familiar to most of you and then establish an isomorphism between them

Definition 2.6.

1. $(G_{po}, +)$, *where* $G_po = \{pair, odd\}$ *and* $+$ *is the ordinary addition*
2. $(Z_2, +)$, *where* $\mathbf{Z}_2 = \{0, 1\}$ *and* $+$ *is the ordinary addition*

Claim 2.7. *Multiplication table for* $(G_{po}, +)$ *and* $(\mathbb{Z}_2, +)$

$(G_{po}, +)$:

$+$	*pair*	*odd*
pair	*pair*	*odd*
odd	*odd*	*pair*

$(\mathbb{Z}_2, +)$:

$+$	0	1
0	0	1
1	1	0

We could easily verify that an odd number plus a pair number gives an odd number *etc.*
.

Exercise 2.1.

1. Verify that the two groups defined above are actually groups
2. What are zero elements in each group?
3. What is the inverse element of "odd" in G_{po}?
4. What is the inverse element of "0" in Z_2?
5. Give two homomorphism from G_{po} to Z_2?
6. Are G_{po} and Z_2 isomorphic?

2.3 Ring

Remember what makes $\mathbb{Z}$ into $\mathbb{Q}$? by adding the multiplicative inverse into $\mathbb{Z}$. which means $(Z, \cdot)$ only need to satisfy "inverse element condition" to be a group. Another famous triplet that shares the same properties is $(\mathcal{M}_n(\mathbb{R}), +, \times)$. The $n \times n$ matrices with matrices addition and matrices multiplication.

The property of the triplet $(Z, +, \cdot)$ and $(\mathcal{M}_n(\mathbb{R}), +, \times)$ is quite common in mathematics or everywhere else that it deserves a name.

Definition 2.8 (Ring)**.** *A Ring $(R, +, \times)$ is a set R together with two binary operation called "addition" and "multiplication" such that $(R, +)$ is a abelian group and $(R, \times)$ satisfies all conditions except the "inverse element condition" to be a group. Besides that, we require $\times$ deeply interact $+$ by satisfying "distribution law"*

With the same mindset of defining group homomorphism, we require a "function between rings" to preserve its "ring" structure. Hence we get our definition here.

Definition 2.9 (Ring Homomorphism)**.** *Supposed R, S are rings, a function $\varphi : R \to S$ is a ring homomorphism if it preserves both operations and the (multiplicative) identity element. That is, φ must be a homomorphism of the underlying abelian groups,*

$$(\forall a, b \in R): \quad \varphi(a + b) = \varphi(a) + \varphi(b),$$

it must preserve the operation of multiplication,

$$(\forall a, b \in R): \quad \varphi(ab) = \varphi(a)\varphi(b),$$

and finally

$$\varphi(1_R) = 1_S$$

Definition 2.10 (field)**.** *A field $(F, +, \times)$ is a Ring $(F, +, \times)$ satisfies the "multiplicative inverse element condition"*

Example 2.11. *$(Q, +, \times)$is a field.*

2.4 Equivalence classes and modular arithmetic

In the above example, two elements of G_{po}, odd and pair, is given by considering all odd numbers or all pair numbers are equivalent. Actually, what we do to classify whether a number is pair or odd is nothing but dividing this number by 2. if the rest is 0, then it's pair. and if the rest is 1, then it's odd. This notion could be generalized.

Let n be a positive integer. Consider the equivalence relation on $\mathbb{Z}$ defined by

$$(\forall a, b \in \mathbb{Z}): \quad a \equiv b \mod n \iff n \mid (b - a).$$

This is called congruence modulo n. We have encountered this relation already, for $n = 2$. the set of equivalence classes is often denoted by $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$. We will opt for $\mathbb{Z}/n\mathbb{Z}$. We will denote by $[a]_n$ the equivalence class of the integer a modulo n, or simply $[a]$ if no ambiguity arises.

The reader should check carefully that $\mathbb{Z}/n\mathbb{Z}$ consists of exactly n elements, namely

$$[0]_n, \quad [1]_n, \cdots, \quad [n]_n$$

We can use the ring structure on $\mathbb{Z}$ to induce a ring structure on $\mathbb{Z}/n\mathbb{Z}$. In order to do this, we define operations $+$ and $\times$ on $\mathbb{Z}/n\mathbb{Z}$, by setting $\forall a, b \in \mathbb{Z}$

$$[a + b] := [a] + [b], \qquad [a \times b] := [a] \times [b]$$

Claim 2.12. *$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ is a ring*

Claim 2.13. *So called Modular arithmetic is essentially the natural ring homomorphism from $(\mathbb{Z}, +, \times)$ to $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.*

3 Number theory

A popular alternative notation for the group $(\mathbb{Z}/n\mathbb{Z}, +)$ is C_n, called cyclic groups. Since C_n is generated by one element x, we record the fact that the element

$$[1]_n \in \mathbb{Z}/n\mathbb{Z}$$

generates the group, in the sense that every other element may be obtained as a multiple of this element. For example, if $m \geq 0$ is an integer, then

$$[m]_n = [\underbrace{1 + \cdots + 1}_{m \text{ times}}]_n = \underbrace{[1]_n + \cdots + [1]_n}_{m \text{ times}} = m \cdot [1]_n.$$

Equivalently, we may phrase this fact by observing that the order of $[1]_n$ in $\mathbb{Z}/n\mathbb{Z}$ is n : this implies that the n multiples $0 \cdot [1]_n, 1 \cdot [1]_n, \ldots, (n-1) \cdot [1]_n$ must all be distinct, and hence they must fill up $\mathbb{Z}/n\mathbb{Z}$.

Proposition 3.1. *The class $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(m, n) = 1$.*

Proof.

Corollary 3.2. *p is a prime $\iff \mathbb{Z}/p\mathbb{Z}$ is a field.*

Theorem 3.3 (Lagrange's theorem)**.** *If G is a finite group and $H \subseteq G$ is a subgroup, then $|H|$ is a divisor of $|G|$.*

Corollary 3.4. *The order $|g|$ of any element g of a finite group G is a divisor of $|G|$: $|g|$ equals the order of the subgroup $\langle g \rangle$ generated by g.*
Note: Therefore, $g^{|G|} = e_G$ for all finite groups G, all $g \in G$.

Corollary 3.5 (Fermat's little theorem)**.** $\forall a \in \mathbb{Z}$

$$p \text{ is a prime} \Longrightarrow a^p \equiv a \bmod p$$

Proof. This is immediate if a is a multiple of p; if a is not a multiple of p, then the class $[a]_p$ modulo p is nonzero, so it is an element of the group $(\mathbb{Z}/p\mathbb{Z})^*$, which has order $p-1$. Thus

$$[a]_p^{p-1} = [1]_p$$

hence $[a]_p^p = [a]_p$ as claimed.

Corollary 3.6 (Wilson's Theorem)**.**

$$p \text{ is a prime} \Longrightarrow (p-1)! = [-1]_p$$

Proof. Each a in $\{1, 2, \ldots, p-1\}$ has an inverse $a^* \in \{1, 2, \ldots, p-1\}$ modulo p, that is $aa^* \equiv 1 (\mathrm{mod} p)$. This inverse is unique and it follows that $(a^*)^* = a$. If $a = a^*$ then $1 \equiv aa^* = a^2 (\mathrm{mod} p)$. We have seen that this necessitates $a \equiv \pm 1 (\mathrm{mod} p)$ and so $a = 1$ or $a = p-1$. In the product $(p-1)! = 1 \times 2 \times 3 \times \cdots \times (p-2) \times (p-1)$ we pair off each term, save for 1 and $p-1$ with its inverse modulo p. We thus get $(p-1)! \equiv 1 \times (p-1) \equiv -1 \ (\bmod p)$

Example 3.7. *As an illustration, consider the case $p = 11$. Then*

$$\begin{aligned} 10! &= 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \\ &= 1 \times (2 \times 6) \times (3 \times 4) \times (5 \times 9) \times (7 \times 8) \times 10 \\ &\equiv 1 \times 1 \times 1 \times 1 \times 1 \times 10 = 10 \equiv -1 \pmod{11} \end{aligned}$$