Algebra-02

Yifan Wei

May 11, 2018

"This one's from *The Book*!"

Paul Erdős

1 More About Groups

1.1 Subgroup

A subgroup H of a group G is a non-empty subset of G which is a group under the group operation of G, and this is denoted by $H \leq G$ and $H < G$ when H is a proper subset of G. For example, $\mathbb{Z}$ is a group under integer addition and the set of even numbers $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Here's a useful criterion to see whether a non-empty subset H of G is a subgroup:

Theorem 1.1. *$H \leq G$ iff $\forall a, b \in H$, $a^{-1}b \in H$.*

Obviously for a group G, $\{e\}$ and G itself are two subgroups of G, they are called the trivial subgroups of G.

A beautiful connection to number theory is the famous Lagrange Theorem.

Theorem 1.2 (Lagrange)**.** *If G is a finite group and $H \leq G$, then $|H|$ is a factor of $|G|$.*

The proof of this theorem is left as an exercise.

1.2 Homomorphism

Definition 1.1 (Homomorphism)**.** Homomorphism between two groups G_1 and G_2 is a function $\sigma : G_1 \to G_2$ that preserves the group operation:

$$\forall a, b \in G_1,\ \sigma(ab) = \sigma(a)\sigma(b).$$

It can be easily seen that $\sigma(e_1) = e_2$. The image of G_1 under σ is denoted by $\sigma(G_1)$ or $\mathrm{im}(\sigma)$ and the inverse image of e_2 is denoted by $\sigma^{-1}(e_2)$ or, most commonly, $\ker(\sigma)$.

When σ happens to be a bijection, we say G_1 and G_2 are *isomorphic* (written as $G_1 \cong G_2$) and σ is an *isomorphism*. When σ is surjective we call it an *epimorphism* and denote it by $G_1 \twoheadrightarrow G_2$. When σ is injective we call it a *monomorphism* and denote it by $G_1 \hookrightarrow G_2$.

1.3 Examples About Groups

1.3.1 Abelian Group

A group is abelian when the group operation commutes, that is $ab = ba$. The name is in memorial to Henrik Abel, a Norwegian Mathematician. Usually in an abelian group the operation is written as $+$ and the identity element is written as 0.

1.3.2 Cyclic Group

Cyclic groups are those who are isomorphic with $\mathbb{Z}/n\mathbb{Z}$. They are usually denoted as C_n.

Haven't we talked about $\mathbb{Z}/n\mathbb{Z}$? This is the so-called *Modulo Addition Group*, a special quotient set of $\mathbb{Z}$ under the equivalence relation defined as $a \sim b \leftrightarrow n|a-b$. The group operation is the addition of equivalent classes i.e.$\langle a\rangle + \langle b\rangle := \langle a+b\rangle$. It's convenient to abuse this notation $\mathrm{GCD}(x, n)$ for $x \in \mathbb{Z}/n\mathbb{Z}$, simply because $\mathrm{GCD}(a+kn, n) = \mathrm{GCD}(a, n)$.

An interesting thing about cyclic group is that any group contains a cyclic group as subgroup! Just consider the set $\{g^n | n \in \mathbb{Z}\}$. The smallest positive integer k which satisfy $g^k = e$ is called the order of g, from Lagrange's theorem we can see k must be a factor of $|G|$.

1.3.3 Dihedral Group

Dihedral group consists of rotations and reflection symmetries of a polygon. Usually written as D_n for an n-gon.

1.3.4 Symmetric Group

The set of all the bijections from a non-empty set X to itself, forms a group under composition of functions. This group is denoted by S_X, $\mathfrak{S}_X$, Σ_X, or $\mathrm{Sym}(X)$. When X has the cardinality of n then the symmetric group on X is also denoted as S_n, $\mathfrak{S}_n$, Σ_n, or $\mathrm{Sym}(n)$.

2 Rings & Fields

Definition 2.1 (Ring)**.** A ring is a set R with two associative binary operations $+$ and $\cdot$, where $(R, +)$ forms an Abelian group and $\cdot$ is distributive over $+$.

Usually $+$ will be called *addition* and the identity element of the group $(R, +)$ will be called *zero* denoted by 0. And $\cdot$ is called *multiplication*. When

it has a multiplicative identity, i.e. there exists an element 1 such that $\forall a \in R$ $a1 = 1a = a$, we'll call this ring a unitary ring. If a unitary ring forms an Abelian group under multiplication when 0 is omitted, we call it a *field*.

When there exists a smallest positive integer n which satisfies $\sum_{k=1}^{n} 1 = 0$ (or alternatively $n1 = 0$) in a field F, then $nx = 0$ holds for every $x \in F$. This smallest positive integer is called the *characteristic* of F and we denote this as $\chi(F) = n$. When such positive integer dose not exist we will say the corresponding field has characteristic of 0 with $\chi(F) = 0$.

3 Vector Spaces

A vector space or *linear space* V over a certain field F is a set with two operations $+ : V \times V \to V$ (vector addition) and $\cdot : F \times V \to V$ (scalar multiplication) which satisfies the following properties:

1. $(V, +)$ forms an abelian group.
2. $\forall r \in F$, $\forall X, Y \in V$, $rX + rY = r(X + Y)$
3. $\forall r, s \in F$, $\forall X \in V$, $(rs)X = r(sX)$
4. $\forall r, s \in F$, $\forall X \in V$, $(r + s)X = rX + sX$
5. $\forall X \in V$, $1X = X1 = X$.

4 Exercise

1. Prove that *any* intersection of subgroups is a subgroup.
2. Prove $\cong$ is an equivalence relation.
3. Prove Lagrange's theorem. If $H \leq G$, show that this relation,

   $$a \sim b \text{ iff } a^{-1}b \in H,$$

   is an equivalence relation and each equivalent class can be written as $aH := \{ah | h \in H\}$. Then use the property of quotient set under this equivalence relation to conclude when G is a finite group, then $|H|$ divides $|G|$.
4. Prove $|\mathfrak{S}_n| = n!$.
5. Prove that if $a \equiv r \mod n$ and $b \equiv s \mod n$ then $ab \equiv rs \mod n$, this indicates $\mathbb{Z}/n\mathbb{Z}$ is a ring with multiplication defined as $\langle a \rangle \langle b \rangle := \langle ab \rangle$.
6. Prove that if $\chi(F) \neq 0$ then it must be a prime number.

   (**Hint:** is it possible to have two non-zero element a and b in a field with $ab = 0$?)
7. Prove the space consists of all convergent complex sequences is a vector space when addition and scalar multiplication are defined component wise.

5 Problem

1. Number theory is the most alluring branch of mathematics! This little problem intends to give an interesting example of the application of group theory on number theory.

   Euler's totient function $\phi(n)$ is an important number theoretical function defined as

   $$\phi(n) := \#\{k \in \mathbb{N} \mid k \leq n \text{ and } \mathrm{GCD}(k, n) = 1\}.$$

   We now will study some behaves of this function.

   1) Construct the set $M_n := \{a \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{GCD}(a, n) = 1\}$. For an arbitrary element $a \in M_n$, define $\sigma_a(x) := ax$, show that σ_a is a injection from the finite set M_n to itself thus a bijection. Now prove M_n is a group under multiplication defined on $\mathbb{Z}/n\mathbb{Z}$. This group is the so-called *modulo multiplication group*.

   2) Prove Euler's totient function theorem:

   $$a^{\phi(n)} \equiv 1 \bmod n,\ (a, n) = 1.$$

   Then Fermat's little theorem:(when p is a prime)

   $$a^p \equiv a \bmod p,$$

   can be seen as a simple corollary because $\phi(p) = p - 1$. A traditional approach to Fermat's little theorem is from the fact $(a+1)^p \equiv a^p + 1$ and use induction.

   3) Prove ϕ is a *multiplicative* number theoretical function, i.e.

   $$\phi(mn) = \phi(m)\phi(n),\ \mathrm{GCD}(m, n) = 1.$$

   Then prove the product formula for totient function:

   $$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

   (**Hint:** use $\tau : M_m \times M_n \to M_{mn}$ defined as $\tau(a, b) := an + bm$, show τ is bijective)