Lecture 2: Integers and divisors.

In the previous lecture we learned

(1) what a group is; and

(2) several examples: $\mathrm{Isom}(S^1)$; $\mathrm{Isom}(\Delta)$;

S_n : symmetric group;

$(\{1,-1\},\cdot)$; $(\mathbb{Z},+)$.

Today we will recall some of the basic properties of $\mathbb{Z}$.

For two main reasons:

(1) Some of these properties are crucial in studying an arbitrary group.

(2) Later we will generalize some of the properties of $\mathbb{Z}$ to an arbitrary group, e.g. construction of a factor group as a generalization of modular arithmetic and Lagrange's theorem as a generalization of Euler's theorem.

One of the key properties of positive integers is the well-ordering principle.

Well-ordering principle

Every non-empty subset of positive integers has a smallest element.

This property is equivalent to the induction principle.

Strong induction $\Rightarrow$ Well-ordering principle

(You can skip this if you wish.)

Suppose to the contrary that there is a non-empty subset A of $\mathbb{Z}^{>0}$ with no smallest element.

By strong induction, we prove that $n \notin A$, which implies $A = \emptyset$. And this contradicts our assumption.

Base of induction.

If $1 \in A$, then 1 is the smallest element in A. So $1 \notin A$.

Strong induction step. If $1 \notin A, 2 \notin A, \dots, k \notin A$, then $k+1 \notin A$

If not, then $k+1$ would be the smallest element of A. ■

Whenever you learn a new structure, you should study

(1) functions that preserve the structure.

(2) Subsets that share the same structure.

Let's focus on the group structure of $(\mathbb{Z}, +)$, and try to answer the second question:

What can we say about $X \subseteq \mathbb{Z}$ s.t.

① $0 \in X$.

② $x \in X \Rightarrow -x \in X$.

③ $x_1, x_2 \in X \Rightarrow x_1 + x_2 \in X$?

Exp. $\{0\}$, $\mathbb{Z}$; $2\mathbb{Z}$; $n\mathbb{Z}$ for any $n \in \mathbb{Z}$.

Lemma. Let X be a subgroup of $\mathbb{Z}$.

If $x \in X$, then $nx \in X$ for any $n \in \mathbb{Z}$.

(Alternatively we can write $\mathbb{Z}x \subseteq X$.)

Pf. By induction on n we show that $nx \in X$ for any positive integer n.

Base of induction. $x \in X$. ✓

Induction step $kx \in X \overset{?}{\Longrightarrow} (k+1)x \in X$

$$\left.\begin{matrix} x \in X \\ kx \in X \end{matrix}\right\} \Rightarrow kx + x = (k+1)x \in X.$$

. $0 \cdot x = 0 \in X$

. If $n < 0 \Rightarrow -n > 0 \Rightarrow -nx \in X \Rightarrow nx \in X$. ∎

Thm (Division Algorithm)

$\forall a \in \mathbb{Z}$, $b \in \mathbb{Z}^{>0}$, $\exists!\ q, r \in \mathbb{Z}$,

$$a = bq + r \quad \text{and} \quad 0 \le r < b.$$

Pf. Let $\Sigma := \{a - bk \mid k \in \mathbb{Z} \text{ and } a - bk \ge 0\}$.

Is $\Sigma \neq \emptyset$?

$$a - b(-|a|) = |a|b + a \ge |a|(b-1) \ge 0.$$

So by well-ordering principle for some $q \in \mathbb{Z}$

$$r = a - bq$$

is the smallest element of Σ.

In particular: $0 \le r$ and since $r-b<r$, it is not in $\Sigma \Rightarrow r-b<0 \Rightarrow$

$$\underline{0 \le r < b}.$$

Uniqueness. $\left.\begin{aligned} a = bq_1 + r_1 \\ a = bq_2 + r_2 \end{aligned}\right\} \Rightarrow \quad r_1 - r_2 = b(q_1 - q_2) \Rightarrow$

$0 \le r_1, r_2 < b \Rightarrow -b < r_1 - r_2 < b$

$|r_1 - r_2| = b\,|q_1 - q_2| < b \Rightarrow |q_1 - q_2| = 0$

$\Rightarrow q_1 = q_2.$

$\Rightarrow r_1 = r_2.$ ∎

Thm. Any (additive) subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some integer n.

Pf. If $X = 0$, we are done.

$x \in X \setminus \{0\} \Rightarrow$ either $x > 0$ or $-x > 0$, and $x, -x \in X$

$\Rightarrow X \cap \mathbb{Z}^{>0} \neq \emptyset$

$\Rightarrow \exists\, x_0 \in X \cap \mathbb{Z}^{>0}$ which smallest in $X \cap \mathbb{Z}^{>0}$.

Hence, by Lemma, $\mathbb{Z}x_0 \subseteq X$

Claim $\mathbb{Z}x_0 = X$.

Suppose $y \in X$.

By the division algorithm, $\exists\, q, r \in \mathbb{Z}$ s.t.

$$y = qx_0 + r \quad \text{and} \quad 0 \le r < x_0$$

By Lemma, $qx_0 \in X$, $y \in X$ $\Rightarrow$ $r = y - qx_0 \in X$, $r < x_0$ $\Rightarrow$ $r = 0$

x_0 : smallest positive integer in X

$\Rightarrow y \in \mathbb{Z}x_0$. ∎

Def ① $d \mid a$: d divides a if $a \in d\mathbb{Z}$

a is a multiple of d

d is a divisor of a.

a is divisible by b.

② The greatest common divisor of a and b is the largest positive integer which divides a and b.

It is denoted by gcd(a,b).

A few properties

① $a \mid 0 \quad \forall a \in \mathbb{Z}$.

② $a \mid b$ and $b \neq 0 \Rightarrow |a| \leq |b|$.

③ $1 \mid a \quad \forall a \in \mathbb{Z}$.

④ $\gcd(0,0)$ does NOT exists.

⑤ $\gcd(a,b) \leq \min(|a|, |b|)$ if either $a \neq 0$ or $b \neq 0$.

Thm. Suppose $a, b \in \mathbb{Z}$ and $a \neq 0$. Let $d = \gcd(a,b)$.

Then $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. In particular,

$d = ax_0 + by_0$ for some integers x_0 and y_0.

Pf .. $a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of $\mathbb{Z}$

* $0 \in a\mathbb{Z} + b\mathbb{Z}$

* $-(ax+by) = a(-x) + b(-y) \in a\mathbb{Z} + b\mathbb{Z}$

* $(ax_1 + by_1) + (ax_2 + by_2) = a(x_1 + x_2) + b(y_1 + y_2)$

$\in a\mathbb{Z} + b\mathbb{Z}$

$a\mathbb{Z} + b\mathbb{Z} \neq 0$ as $a \neq 0 \Rightarrow$

$d'\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ where d' is the smallest positive

integer in $a\mathbb{Z}+b\mathbb{Z}$.

We will prove $d=d'$.

Claim. $d \mid d'$.

Pf. $\exists\, x_0, y_0 \in \mathbb{Z}$ s.t. $d' = ax_0 + by_0$

$$\left.\begin{array}{l} d \mid a \Rightarrow d \mid ax_0 \\ d \mid b \Rightarrow d \mid by_0 \end{array}\right\} \Rightarrow d \mid ax_0 + by_0 = d' \Rightarrow d = d'.$$

Claim. $d' \le d$

Pf.
$$\left.\begin{array}{l} d' \mid a \\ d' \mid b \\ 0 < d' \end{array}\right\} \Rightarrow d' \le \gcd(a,b) = d.$$

■

Corollary.
$$\left.\begin{array}{l} d \mid a \\ d \mid b \\ a \neq 0 \end{array}\right\} \Rightarrow d \mid \gcd(a,b)$$

Pf. $\exists\, x_0, y_0 \in \mathbb{Z}$, $\gcd(a,b) = ax_0 + by_0$

$$\left.\begin{array}{l} d \mid a \Rightarrow d \mid ax_0 \\ d \mid b \Rightarrow d \mid by_0 \end{array}\right\} \Rightarrow d \mid ax_0 + by_0.$$

■

Corollary
$$\left.\begin{array}{l} a \mid bc \\ \gcd(a,b) = 1 \end{array}\right\} \Rightarrow a \mid c$$

Pf. $\gcd(a,b) = 1 \Rightarrow \exists\, x_0, y_0 \in \mathbb{Z},\ ax_0 + by_0 = 1$

$$\Rightarrow (x_0 c)\, a + y_0 (bc) = c$$

$$\left.\begin{array}{l} a \mid a \\ a \mid bc \end{array}\right\} \Rightarrow a \mid (x_0 c)a + y_0(bc) = c$$

$$\Rightarrow a \mid c.$$

Alternatively

$$a\mathbb{Z} \supseteq bc\mathbb{Z}$$

$$a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z} \Rightarrow ac\mathbb{Z} + bc\mathbb{Z} = c\mathbb{Z}$$

$$\cap$$

$$a\mathbb{Z} + a\mathbb{Z} = a\mathbb{Z}.$$

$$\Downarrow$$

$$a \mid c.$$

■