

CONTENTS

1. Recollections on subgroups	1
2. Subgroups of $\mathbb{Z}$ and greatest common divisors	2

1. RECOLLECTIONS ON SUBGROUPS

Definition 1.1 (Subgroup). Let $(G, \cdot, e)$ be a group. A subset $H \subseteq G$ is a *subgroup* if it satisfies the following conditions:

- (1) $e \in H$.
- (2) H is closed under products: if $h_1, h_2 \in H$, then $h_1 h_2 \in H$.
- (3) H is closed under inverses: if $h \in H$, then $h^{-1} \in H$, where the inverse is taken in G .

For any group G , the set $\{e\}$ is a subgroup, called the *trivial subgroup*. The whole group G is also a subgroup of itself. A subgroup H is called a *proper subgroup* if $H \neq G$. If $\{e\} \subsetneq H \subsetneq G$, then H is called a *nontrivial proper subgroup*.

Recall that we also proved the following result earlier in Lecture 2.

Proposition 1.1 (Finite subgroup criterion). *If $H \subseteq G$ is finite, contains e , and is closed under products, then H is a subgroup. In this case, closure under inverses follows from the other two conditions.*

Remark. For an infinite subset, closure under inverses must still be checked. For example, $\{0, 1, 2, \dots\} \subseteq (\mathbb{Z}, +, 0)$ contains the identity and is closed under addition, but it is not closed under additive inverses.

We have also already introduced the following notion.

Definition 1.2 (Cyclic subgroup). Let G be a group, with identity denoted by 1, and let $x \in G$. The *cyclic subgroup generated by x* is

$$\langle x \rangle = \{x^m : m \in \mathbb{Z}\} = \{1, x^{\pm 1}, x^{\pm 2}, x^{\pm 3}, \dots\}. \quad (1.1)$$

The order of $x \in G$ is equal to $\#\langle x \rangle$ (it could be ∞): it is the smallest positive integer $n > 0$ so that $x^n = 1$.

We generalize this definition as follows.

Definition 1.3 (Subgroup generated by a subset). For a subset $W \subseteq G$, let $\langle W \rangle$ be the set of all finite products

$$w_1 w_2 \cdots w_k, \quad k \geq 0, \quad (1.2)$$

where each factor w_i is an element of W or the inverse of an element of W . Repetitions are allowed, and the order of the factors matters. When $k = 0$, the product is the identity 1. This is called the *subgroup generated by W* .

Indeed, concatenating two such products gives another such product. As for inverses, let's mention the following important but simple identity that you may remember from a course in linear algebra.

$$(w_1 w_2 \cdots w_k)^{-1} = w_k^{-1} \cdots w_2^{-1} w_1^{-1} \quad (1.3)$$

The product on the right is again of the required form. Hence $\langle W \rangle$ is a subgroup.

Remark. The subgroup $\langle W \rangle$ is the *smallest subgroup containing* W . Indeed, it contains W by taking products of length one. If H is any subgroup containing W , then closure under inverses and products implies that H contains every product used to define $\langle W \rangle$. Thus $\langle W \rangle \subseteq H$.

Intersecting subgroups provides another useful way to manufacture new groups.

Proposition 1.2. *If H and K are subgroups of G , then $H \cap K$ is a subgroup of G .*

Proof. Since $e \in H$ and $e \in K$, we have $e \in H \cap K$. If $a, b \in H \cap K$, then $ab \in H$ and $ab \in K$, because both subgroups are closed under products. Thus $ab \in H \cap K$. Similarly, if $a \in H \cap K$, then $a^{-1} \in H$ and $a^{-1} \in K$, so $a^{-1} \in H \cap K$. $\square$

Remark. The union $H \cup K$ need not be a subgroup. For example, $2\mathbb{Z} \cup 3\mathbb{Z}$ contains 2 and 3, but does not contain their sum 5.

2. SUBGROUPS OF $\mathbb{Z}$ AND GREATEST COMMON DIVISORS

Now we would like to study subgroups of a particular group, namely $\mathbb{Z} = (\mathbb{Z}, +, 0)$ the additive group of integers.

For $a \in \mathbb{Z}$, we now define

$$\mathbb{Z}a = \langle a \rangle = \{ma : m \in \mathbb{Z}\} = \{0, \pm a, \pm 2a, \pm 3a, \dots\}, \quad (2.1)$$

the set of all multiples of a . It is clearly a subgroup as it is closed under addition (the sum of two multiples of a is again a multiple of a , etc.)

Lemma 2.1. *Every subgroup of $(\mathbb{Z}, +, 0)$ is either $\{0\}$ or $\mathbb{Z}d$ for some positive integer d .*

Proof. Let $H \subseteq \mathbb{Z}$ be a subgroup with $H \neq \{0\}$. Since H contains a nonzero integer and its negative, it contains a positive integer. By the well-ordering principle, H has a smallest positive element d . We claim that $H = \mathbb{Z}d$.

First, $\mathbb{Z}d \subseteq H$, since $d \in H$ and H is closed under addition and additive inverses.

For the reverse inclusion, let $m \in H$. By division with remainder, write

$$m = qd + r, \quad q \in \mathbb{Z}, \quad 0 \leq r < d. \quad (2.2)$$

Since $m, qd \in H$, we have $r = m - qd \in H$. If $r > 0$, this contradicts the choice of d as the smallest positive element of H . Thus $r = 0$, so $m = qd \in \mathbb{Z}d$. Hence $H \subseteq \mathbb{Z}d$, proving the claim. $\square$

Greatest common divisors. Let $a, b \in \mathbb{Z}$ be not both zero. Consider the set of all integer linear combinations of a and b :

$$\mathbb{Z}a + \mathbb{Z}b = \{ma + nb : m, n \in \mathbb{Z}\}. \quad (2.3)$$

This is a subgroup of $(\mathbb{Z}, +, 0)$: it contains 0, and sums and negatives of integer linear combinations are again integer linear combinations. Therefore the preceding lemma gives

$$\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d \quad (2.4)$$

for some $d > 0$, since this subgroup contains a nonzero element. We will show that this positive generator is $\gcd(a, b)$.

Lemma 2.2 (Divisibility and inclusion). *For integers r, s ,*

$$r \mid s \iff \mathbb{Z}s \subseteq \mathbb{Z}r. \quad (2.5)$$

Proof. If $s = kr$ for some $k \in \mathbb{Z}$, then every multiple of s is a multiple of r . Conversely, if $\mathbb{Z}s \subseteq \mathbb{Z}r$, then $s \in \mathbb{Z}r$, so $r \mid s$. $\square$

Example 2.1. The direction of inclusion reverses the order in the divisibility relation:

$$2 \mid 6, \quad 6\mathbb{Z} \subseteq 2\mathbb{Z}. \quad (2.6)$$

Indeed, every multiple of 6 is a multiple of 2.

Proposition 2.1. *Let $a, b \in \mathbb{Z}$ be not both zero, and let $d > 0$ satisfy $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d$. Then $d = \gcd(a, b)$. In particular,*

$$\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}\gcd(a, b). \quad (2.7)$$

Proof. We check two properties:

- (1) d divides both a and b .
- (2) Every common divisor of a and b divides d .

For the first property, the inclusions

$$\mathbb{Z}a \subseteq \mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d, \quad \mathbb{Z}b \subseteq \mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d \quad (2.8)$$

imply $d \mid a$ and $d \mid b$ by Lemma 2.2.

For the second property, suppose $\ell \mid a$ and $\ell \mid b$. Then $\mathbb{Z}a \subseteq \mathbb{Z}\ell$ and $\mathbb{Z}b \subseteq \mathbb{Z}\ell$. Adding elements from these two subgroups gives

$$\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b \subseteq \mathbb{Z}\ell. \quad (2.9)$$

By Lemma 2.2, $\ell \mid d$. Every positive common divisor ℓ thus divides d . $\square$

This gives Bézout's identity.

Corollary 2.1 (Bézout's identity). *Let $a, b \in \mathbb{Z}$ be not both zero. There exist integers m, n such that*

$$\gcd(a, b) = ma + nb. \quad (2.10)$$

Proof. Set $d = \gcd(a, b)$. Since $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d$ and $d \in \mathbb{Z}d$, we have $d \in \mathbb{Z}a + \mathbb{Z}b$. By the definition of this subgroup, $d = ma + nb$ for some $m, n \in \mathbb{Z}$. $\square$