

CONTENTS

1. Review: subgroups of the integers and greatest common divisors	1
2. Group homomorphisms	2

1. REVIEW: SUBGROUPS OF THE INTEGERS AND GREATEST COMMON DIVISORS

Last time we classified all subgroups of $\mathbb{Z}$ using the following result.

Theorem 1.1. *Let $H \leq (\mathbb{Z}, +)$ be a subgroup. Then $H = \mathbb{Z}d$, the set of all multiples of d , for a unique integer $d \geq 0$. The case $d = 0$ gives the trivial subgroup $\{0\}$.*

We also stated the following result:

Lemma 1.1 (Divisibility and inclusion). *For integers r, s ,*

$$r \mid s \iff \mathbb{Z}s \subseteq \mathbb{Z}r. \quad (1.1)$$

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

$$2 \mid 6, \quad 6\mathbb{Z} \subseteq 2\mathbb{Z}. \quad (1.2)$$

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

Recall that $\mathbb{Z}a + \mathbb{Z}b = \{ma + nb : m, n \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$: it contains 0 and is closed under sums and additive inverses. If a and b are not both zero, this subgroup is nonzero, so the preceding classification gives $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d$ for a unique $d > 0$.

Proposition 1.1. *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,*

$$\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}\gcd(a, b). \quad (1.3)$$

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

$$\mathbb{Z}a \subseteq \mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d, \quad \mathbb{Z}b \subseteq \mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d \quad (1.4)$$

imply $d \mid a$ and $d \mid b$ by Lemma 1.1.

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

$$\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b \subseteq \mathbb{Z}\ell. \quad (1.5)$$

By Lemma 1.1, $\ell \mid d$. Every positive common divisor ℓ therefore satisfies $\ell \leq d$. Since $d > 0$ is itself a common divisor, it is the greatest common divisor. $\square$

This gives Bézout's identity.

Corollary 1.1 (Bézout's identity). *Let $a, b \in \mathbb{Z}$ be not both zero. There exist integers m, n such that*

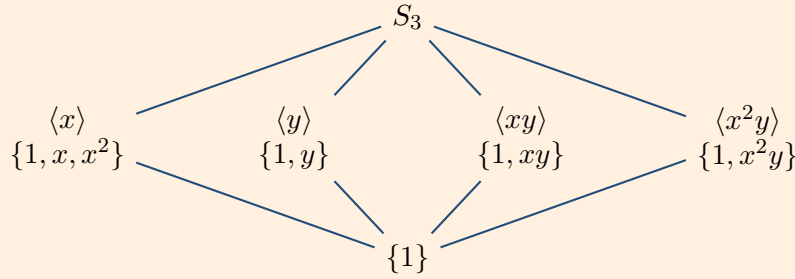
$$\gcd(a, b) = ma + nb. \quad (1.6)$$

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 $m, n \in \mathbb{Z}$. $\square$

Exercise 1.2 (Subgroups of S_3). Determine all subgroups of S_3 and draw the diagram of all such subgroups, indicating the inclusions between them. Use the presentation

$$S_3 = \langle x, y \mid x^3 = 1, y^2 = 1, yx = x^2y \rangle.$$

Answer. The subgroup lattice is shown below; inclusions run upward.



2. GROUP HOMOMORPHISMS

Definition 2.1 (Homomorphism). Let G and H be groups. A map $\varphi : G \rightarrow H$ is a *group homomorphism* if

$$\varphi(ab) = \varphi(a)\varphi(b) \quad \text{for every } a, b \in G. \quad (2.1)$$

The products on the two sides are taken in G and H , respectively.

An *isomorphism* is a bijective homomorphism.

From the product rule, we may compute:

$$\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)^2,$$

and cancellation in H gives $\varphi(e_G) = e_H$. Similarly,

$$e_H = \varphi(e_G) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}),$$

so

$$\varphi(a^{-1}) = \varphi(a)^{-1}. \quad (2.2)$$

Definition 2.2 (Kernel and image). Let $\varphi : G \rightarrow H$ be a homomorphism. Its *kernel* and *image* are

$$\ker(\varphi) = \{x \in G : \varphi(x) = e_H\}, \quad (2.3)$$

$$\operatorname{im}(\varphi) = \{y \in H : y = \varphi(x) \text{ for some } x \in G\}. \quad (2.4)$$

Example 2.1 (Reduction modulo n). Let $n \geq 1$ be an integer. Write $\bar{a}$ for the congruence class of a modulo n . The group $\mathbb{Z}/n\mathbb{Z}$ consists of these classes, with addition $\bar{a} + \bar{b} = \overline{a+b}$. The natural projection

$$\pi_n : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad a \longmapsto \bar{a}, \quad (2.5)$$

is a homomorphism of additive groups, since

$$\pi_n(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \pi_n(a) + \pi_n(b).$$

Every congruence class has an integer representative, so π_n is surjective. Its kernel is

$$\ker(\pi_n) = \{a \in \mathbb{Z} : \bar{a} = \bar{0}\} = \{a \in \mathbb{Z} : n \mid a\} = n\mathbb{Z}.$$

Thus $\text{im}(\pi_n) = \mathbb{Z}/n\mathbb{Z}$, while π_n is not injective: the distinct integers 0 and n both map to $\bar{0}$.

Proposition 2.1. *The kernel $\ker(\varphi)$ and image $\text{im}(\varphi)$ are subgroups of G and H , respectively.*

Proof. The kernel contains e_G . If $a, b \in \ker(\varphi)$, then $\varphi(ab) = e_H e_H = e_H$, and $\varphi(a^{-1}) = \varphi(a)^{-1} = e_H$. Thus the kernel is a subgroup. The image contains $e_H = \varphi(e_G)$; it is closed under products because $\varphi(a)\varphi(b) = \varphi(ab)$ and under inverses because $\varphi(a)^{-1} = \varphi(a^{-1})$. $\square$

Lemma 2.1 (Fibres of a homomorphism). *Let $\varphi : G \rightarrow H$ be a homomorphism. For $a, b \in G$,*

$$\varphi(a) = \varphi(b) \iff a^{-1}b \in \ker(\varphi) \iff b^{-1}a \in \ker(\varphi). \quad (2.6)$$

In particular,

$$\varphi \text{ is injective} \iff \ker(\varphi) = \{e_G\}. \quad (2.7)$$

Proof. If $\varphi(a) = \varphi(b)$, then

$$\varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b) = e_H.$$

The converse follows by reversing this calculation. The equivalent statement with $b^{-1}a$ follows by taking inverses. If φ is injective, then $\varphi(a) = e_H = \varphi(e_G)$ forces $a = e_G$, so its kernel is trivial. Conversely, if the kernel is trivial and $\varphi(a) = \varphi(b)$, the first equivalence gives $a^{-1}b = e_G$, hence $a = b$. $\square$

Corollary 2.1. *A homomorphism $\varphi : G \rightarrow H$ is an isomorphism if and only if*

$$\ker(\varphi) = \{e_G\} \quad \text{and} \quad \text{im}(\varphi) = H. \quad (2.8)$$

We have defined an isomorphism as a bijective homomorphism. I prefer to think of it as a homomorphism with a homomorphic inverse: a homomorphism $\varphi : G \rightarrow H$ together with a homomorphism $\psi : H \rightarrow G$ satisfying

$$\varphi \circ \psi = \text{id}_H, \quad \psi \circ \varphi = \text{id}_G. \quad (2.9)$$

The following proposition shows that these two descriptions are equivalent.

Proposition 2.2. *If a homomorphism $\varphi : G \rightarrow H$ is bijective, then its set-theoretic inverse $\psi : H \rightarrow G$ is also a homomorphism.*

Proof. Given $h_1, h_2 \in H$, choose $g_1, g_2 \in G$ with $\varphi(g_i) = h_i$. Then

$$\psi(h_1 h_2) = \psi(\varphi(g_1)\varphi(g_2)) = \psi(\varphi(g_1 g_2)) = g_1 g_2 = \psi(h_1)\psi(h_2).$$

$\square$

Example 2.2 (Homomorphisms determined by generators and relations). Consider the six-element group from Section 1:

$$G = \{1, x, x^2, y, xy, x^2y\}, \quad x^3 = 1, \quad y^2 = 1, \quad yx = x^2y,$$

and let

$$H = S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}.$$

Here (1) denotes the identity permutation, and permutations are composed from right to left. What maps $\varphi : G \rightarrow S_3$ are homomorphisms?

Step 1: choose the images of the generators. Put $\sigma = \varphi(x)$ and $\tau = \varphi(y)$. If φ is a homomorphism, all its values are forced by these two choices:

g	1	x	x^2	y	xy	x^2y
$\varphi(g)$	(1)	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$

In particular, we cannot choose the images of the six elements independently.

Step 2: preserve the relations. Applying φ to each defining relation gives

$$\sigma^3 = (1), \quad \tau^2 = (1), \quad \tau\sigma = \sigma^2\tau.$$

Thus σ is either (1) or a 3-cycle, while τ is either (1) or a transposition. The order of an image may be smaller than the order of the original element: for example, $\varphi(x) = (1)$ is allowed. The last relation imposes an additional compatibility condition.

These conditions are also sufficient. Indeed, write each element of G uniquely as $x^i y^j$, where $0 \leq i < 3$ and $0 \leq j < 2$. Since $yx = x^{-1}y$, multiplication in G is given by

$$(x^i y^j)(x^k y^\ell) = x^{i+(-1)^j k} y^{j+\ell},$$

with the exponents reduced modulo 3 and 2, respectively. If σ, τ satisfy the three displayed relations, then $\tau\sigma = \sigma^{-1}\tau$, so their products obey the same rule:

$$(\sigma^i \tau^j)(\sigma^k \tau^\ell) = \sigma^{i+(-1)^j k} \tau^{j+\ell}.$$

Consequently, $\varphi(x^i y^j) = \sigma^i \tau^j$ defines a homomorphism.

Step 3: list the possibilities.

- (1) If $\sigma = (1)$, the compatibility condition is automatic. We may take $\tau = (1)$ or any of the three transpositions. The first choice gives the trivial homomorphism, with kernel G and image $\{(1)\}$. For each transposition τ , we obtain a homomorphism with

$$\ker(\varphi) = \{1, x, x^2\}, \quad \text{im}(\varphi) = \{(1), \tau\}.$$

These are four homomorphisms in total.

- (2) If σ is a 3-cycle, we cannot take $\tau = (1)$: the last relation would give $\sigma = \sigma^2$, hence $\sigma = (1)$. Every transposition does work, because conjugating a 3-cycle by a transposition reverses it:

$$\tau\sigma\tau^{-1} = \sigma^{-1} = \sigma^2.$$

There are two choices for σ and three for τ , giving six homomorphisms. Each is an isomorphism: the three elements $(1), \sigma, \sigma^2$ are distinct, as are $\tau, \sigma\tau, \sigma^2\tau$, and these two sets are disjoint. Indeed, an equality $\sigma^i \tau = \sigma^k$ would make the transposition τ a power of a 3-cycle. Thus all six images are distinct, so $\ker(\varphi) = \{1\}$ and $\text{im}(\varphi) = S_3$.

For instance, choosing $\varphi(x) = (1\ 2\ 3)$ and $\varphi(y) = (1\ 2)$ gives the isomorphism

g	1	x	x^2	y	xy	x^2y
$\varphi(g)$	(1)	(1 2 3)	(1 3 2)	(1 2)	(1 3)	(2 3)

There are therefore exactly $4 + 6 = 10$ homomorphisms $G \rightarrow S_3$, of which six are isomorphisms.