Contents

Preface

These notes are going to cover group theory and ring theory. They are copied from the notes I took as an undergraduate.

Last update: 2025 August 7

Chapter 1

Group Theory

§ 1.1. Basic Definitions and Examples

Definition 1.1.1. Let S be a nonempty set. A map $* : S \times S \to S$ is called a *binary operation* on S.

Definition 1.1.2. Let G be a nonempty set and $*$ a binary operation on G. We say $(G, *)$ is a *group* if the following conditions are satisfied:

(1) $g_1 * g_2 \in G$ for all $g_1, g_2 \in G$;

(2) $(g_1 * g_2) * g_2 = g_1 * (g_2 * g_3)$ for all $g_1, g_2, g_3 \in G$;

(3) there exists $e \in G$ so that $g * e = g = e * g$ for all $g \in G$.

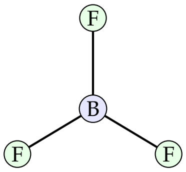
(4) For all $g \in G$, there exists $g^{-1} \in G$ so that $g * g^{-1} = e = g^{-1} * g$.

If G also satisfies:

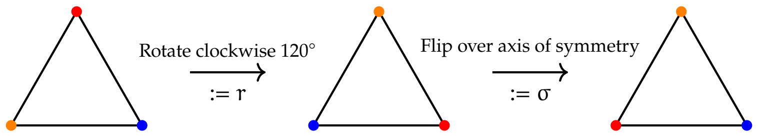
(5) $g_1 * g_2 = g_2 * g_1$ for all $g_1, g_2 \in G$,

then we say G is an *abelian* group.

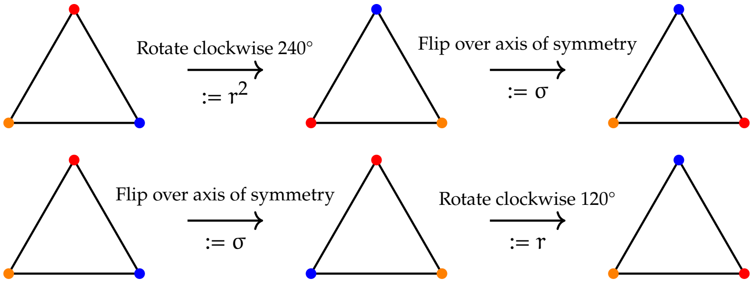
Example 1.1.1. Groups are really the study of symmetries. Consider the molecule Boron Triflouride BF_3:



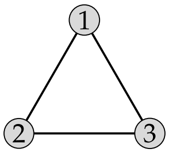
We want to describe the symmetries of this molecule.



We denote the composition of r and σ as σr. Note that, no matter the position of our triangle, σ^2 results in no change. Consider the following moves of the same triangle:



From this we can see $\sigma r^2 = r\sigma$. We denote the set of symmetries of this triangle as $D_3 = \{e, r, r^2\sigma, \sigma r, \sigma r^2\}$. Given the following triangle:



we can use the following notation to compute its end position:

$$r = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Note that the top row of each matrix represents the triangles initial state, and the bottom row represents where each vertex gets sent to. Observe that:

$$r\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Since we work from right to left, we can see that the "1" in the matrix representing σ gets sent to "1" by itself, and then sent to "2" by the matrix representing r. Similarly, the "2" in the matrix representing σ gets sent to "3", and then sent to "1".

We can represent these operations in a terser way. Define:

$$r = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} := (123),$$
$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} := (1)(23) = (23).$$

The notation comes from the fact that $1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 1$, hence 1, 2, and 3 are grouped together by parenthesis. We drop the 1 from the σ notation since it is only telling us that 1 gets sent to itself. Consider:

$$r\sigma = (123)(23).$$

Working from right the left, since $2 \xrightarrow{\sigma} 3 \xrightarrow{r} 1 \xrightarrow{r} 2 \xrightarrow{r} 3$, the first part of the computation is (23). We also have that $3 \xrightarrow{\sigma} 2 \xrightarrow{r} 3$. Since 3 gets sent to itself, we have that $r\sigma = (23)$. Consider:

$$\sigma r = (23)(123)$$

Since $1 \xrightarrow{\sigma} 2 \xrightarrow{\sigma} 3 \xrightarrow{r} 2 \xrightarrow{r} 3$, $2 \xrightarrow{\sigma} 3 \xrightarrow{r} 2$, and $3 \xrightarrow{\sigma} 1 \xrightarrow{\sigma} 2 \xrightarrow{r} 3$, we have that $\sigma r = (13)$. Note that we keep cycling through until we reach the closing parenthesis of σ.

The set D_3 is a group under function composition. This is referred to as the *dihedral group* in three elements.

Example 1.1.2. Let $n \in \mathbb{Z}$. Define $a \sim b$ by $a \equiv b \pmod n$ (or, equivalently $n \mid (a-b)$). We can show that this relation is reflexive, symmetric, and transitive, hence it is an equivalence relation on $\mathbb{Z}$. For $a \in \mathbb{Z}$, define the *equivalence class* of a as:

$$\begin{aligned}[a]_n &:= \{b \in \mathbb{Z} \mid b \equiv a \pmod n\} \\ &= \{b \in \mathbb{Z} \mid n \mid (b-a)\} \\ &= \{a + nk \mid k \in \mathbb{Z}\}.\end{aligned}$$

For each $a \in \mathbb{Z}$, the division algorithm says we can *uniquely* write $a = nq + r$, for some $q, r \in \mathbb{Z}$ with $0 \leqslant r \leqslant n$. Hence all equivalence classes are given by $[0]_n$, $[1]_n$, ... $[n-1]_n$. Define:

$$\mathbb{Z}/n\mathbb{Z} := \{[0]_n, [1]_n, ...[n-1]_n\}$$

Now consider the binary operation $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $[a]_n + [b]_n = [a+b]_n$. Note that the addition within the equivalence classes is the standard notion of integer addition, whereas the binary operation between each equivalence class is something different. Since the domain of our map "+" contains elements which are equivalence classes, we must verify that our map is well-defined. Let $[a_1]_n = [a_2]_n$ and $[b_1]_n = [b_2]_n$. Then $a_1 = a_2 + ns$ for some $s \in \mathbb{Z}$ and $b_1 = b_2 + nt$ for some $t \in \mathbb{Z}$. Observe that:

$$\begin{aligned}[a_1]_n + [b_1]_n &= [a_1 + b_1]_n \\ &= [(a_2 + ns) + (b_2 + nt)]_n \\ &= [a_2]_n + [b_2]_n + [n(s+t)]_n \\ &= [a_2]_n + [b_2]_n.\end{aligned}$$

Thus our binary operation is well-defined. It can be shown that the set $\mathbb{Z}/n\mathbb{Z}$ is an abelian group, called the *group of integers modulo* n.

We will now present some basic results about integers and modular arithmetic. The proofs are left out but can be found in any introductory number theory text, or online.

Theorem 1.1.1. *If* $a_1, a_2, ..., a_n$ *are integers, not all 0, then* $\gcd(a_1, a_2, ..., a_n)$ *exists. Furthermore, there are integers* $k_1, k_2, ..., k_n$ *such that*

$$\gcd(a_1, a_2, ..., a_n) = k_1 a_1 + k_2 a_2 + ... + k_n a_n.$$

Theorem 1.1.2. *If* a *and* b *are relatively prime integers (that is,* $\gcd(a, b) = 1$*) and* $a \mid bc$*, then* $a \mid c$*. If* p *is prime and* $p \mid a_1 a_2 ... a_n$*, then* $p \mid a_i$ *for some* i*.*

Using these facts, we can generalize Example 1.1.2 to the following theorem.

Theorem 1.1.3. *Let* $m > 0$ *be an integer and* $a, b, c, d \in \mathbb{Z}$*.*

(i) *Congruence modulo* m *is an equivalence relation on the set of integers* $\mathbb{Z}$, *which has precisely* m *equivalence classes.*

(ii) *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $a + c \equiv b + d \pmod{m}$ *and* $ac \equiv bd \pmod{m}$.

(iii) *If* $ab \equiv ac \pmod{m}$ *and* a *and* m *are relatively prime, then* $b \equiv c \pmod{m}$.

The structure of these objects we've defined are extremely rich. In fact, many of the properties which we find interesting are completely independent of the elements comprising each set. This can be seen through the following definition and theorem. The proof of the theorem is left out, as it immediately follows from what has been presented earlier in this discussion.

Definition 1.1.3. A *semigroup* is a nonempty set G together with a binary operation on G which is:

(1) associative: $a(bc) = (ab)c$ for all $a, b, c \in G$;

A *monoid* is a semigroup G which contains a

(2) (two-sided) identity element $e \in G$ such that $ae = ea = a$ for all $a \in G$.

A *group* is a monoid G such that

(3) for every $a \in G$ there exists a (two-sided) inverse element $a^{-1} \in G$ such that $a^{-1}a = aa^{-1} = e$.

A semigroup G is said to be *abelian* if its binary operation is

(4) commutative: $ab = ba$ for all $a, b \in G$.

Theorem 1.1.4. *Let* $\sim$ *be an equivalence relation on a monoid* G *such that* $a_1 \sim a_2$ *and* $b_1 \sim b_2$ *imply* $a_1b_1 \sim a_2b_2$ *for all* $a_i, b_i \in G$. *Then the set* $G/\sim$ *of all equivalence classes of* G *under* $\sim$ *is a monoid under the binary operation defined by* $\overline{a}\overline{b} = \overline{ab}$, *where* $\overline{x}$ *denotes the equivalence class of* $x \in G$. *If* G *is an (abelian) group, then so is* $G/\sim$.

Example 1.1.3. Let $X = \{1, 2, 3\}$. Define $S_3 := \{f : X \to X \mid f \text{ is bijective}\}$. It is easily verifiable that $|S_3| = 6$, and moreover that S_3 is a group under composition of functions. The elements of S_3 are:

$$\begin{aligned}
\text{id} &: \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1), \\
\sigma_1 &: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12), \\
\sigma_2 &: \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13), \\
\sigma_3 &: \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23), \\
\sigma_4 &: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123), \\
\sigma_5 &: \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132).
\end{aligned}$$

We say S_3 is the *symmetric group* on 3 letters.

Example 1.1.4. Consider the regular n-gon. Set r_n as rotation by $\frac{2\pi}{n}$ radians clockwise. Then $r_n^2 = r_n \circ r_n$ is a rotation by $2\left(\frac{2\pi}{n}\right)$ radians clockwise. Similarly, r_n^{n-1} is a rotation by $(n-1)\left(\frac{2\pi}{n}\right)$ radians clockwise, and r_n^n is a rotation by 2π radians, hence no rotation. So $\mathrm{id}, r_n, r_n^2, ..., r_n^{n-1}$ are distinct rigid motions. Define $C_n := \{\mathrm{id}, r_n, r_n^2, ..., r_n^{n-1}\}$. This is an abelian group of order n. This is referred to as the *cyclic group of order* n.

Given C_n, if we also allow flips over an axis of symmetry, then we get D_n.

Example 1.1.5. Define $(\mathbb{Z}/n\mathbb{Z})^* := \{[a]_n \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n) = 1\}$. This set is a group under the operation:

$$\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad [a]_n \cdot [b]_n = [ab]_n.$$

The only non-trivial aspects to prove are closure under $\cdot$ and the existence of inverse elements. Let $[a]_n, [b]_n \in (\mathbb{Z}/n\mathbb{Z})^*$. To show $[ab]_n \in (\mathbb{Z}/n\mathbb{Z})^*$, we must prove that $\gcd(ab,n) = 1$. Suppose towards contradiction $\gcd(ab,n) \neq 1$. Then there is a prime p such that $p \mid \gcd(ab,n)$. So $p \mid n$ and $p \mid ab$. Since p is prime, $p \mid ab$ implies $p \mid a$ and $p \mid b$. Thus $p \mid \gcd(a,n)$ or $p \mid \gcd(b,n)$. This is a contradiction, since it implies $\gcd(a,n) \neq 1$ or $\gcd(b,n) \neq 1$; i.e., either $[a]_n \notin (\mathbb{Z}/n\mathbb{Z})^*$ or $[b]_n \notin (\mathbb{Z}/n\mathbb{Z})^*$. It must be the case that $\gcd(ab,n) = 1$.

Given $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^*$, we will now show the existence of an inverse element. Since $\gcd(a,n) = 1$, there exists $s,t \in \mathbb{Z}$ such that $as + nt = 1$. Observe that:

$$\begin{aligned}[1]_n &= [as + nt]_n \\ &= [a]_n[s]_n + [nt]_n \\ &= [a]_n[s]_n.\end{aligned}$$

Thus $[s]_n$ is the inverse of $[a]_n$. However, is $[s]_n \in (\mathbb{Z}/n\mathbb{Z})^*$? If $gcd(s,n) \neq 1$, then there is a prime p such that $p \mid \gcd(s,n)$. So $p \mid s$ and $p \mid n$. Equivalently, $p \mid as$ and $p \mid nt$, so $p \mid (as + nt)$. But this contradicts $as + nt = 1$.

Theorem 1.1.5. *Let G be any group.*

(1) The identity element is unique.

(2) Inverses are unique.

(3) For all $a,b,c \in G$, if $ab = ac$, then $b = c$.

(4) For all $a,b \in G$, there exists $x \in G$ such that $ax = b$.

§ 1.2. Subgroups and Cyclic Groups

Definition 1.2.1. Let $(G,*)$ be a group. We say a nonempty subset $H \subseteq G$ is a *subgroup* if $(H,*)$ is a group. We denote this as $H \leqslant G$.

Proposition 1.2.1. *Let $(G,*)$ be a group and $H \subseteq G$. Then H is a subgroup if and only if $H \neq \emptyset$ and $x * y^{-1} \in H$ for all $x,y \in H$.*

Proof. The forward direction is clear. Suppose for all $x, y \in H$ that $x * y^{-1} \in H$. Take $y = x$. Then $x * x^{-1} = e_G \in H$. Thus H admits an identity. Now take $x = e$. Then $e * y^{-1} = y^{-1} \in H$. Thus H admits inverse elements. Now take $y = y^{-1}$. Then $x * y \in H$, hence H is closed under $*$. It is clear that associativity follows from this. Thus H is a subgroup of G. □

Proposition 1.2.2. *Let* G *be a group with* $H, K \leqslant G$*. Then* $H \cap K \leqslant G$*.*

Proof. Note that $H \cap K \neq \emptyset$ since $e_G \in H$ and $e_G \in K$. Let $x, y \in H \cap K$. Then $x, y \in H$ and $x, y \in K$. Since $H \leqslant G$, $xy^{-1} \in H$. Since $K \leqslant G$, $xy^{-1} \in K$. Thus $xy^{-1} \in H \cap K$; i.e., $H \cap K \leqslant G$. □

In general $H \cup K$ is not a subgroup. Suppose $H = \{\text{id}, \sigma r\}$ and $K = \{\text{id}, \sigma r^2\}$. Then $H \cup K = \{\text{id}, \sigma r, \sigma r^2\}$, which is not closed under multiplication because $\sigma r \sigma r^2 = r^2 \notin H \cup K$.

Definition 1.2.2. Let G be a group and $a \in G$. The *cyclic subgroup generated by* a is the set $\langle a \rangle := \{a^k \mid k \in \mathbb{Z}\}$.

Definition 1.2.3. Let G be a group. We say G is *cyclic* if there exists a $a \in G$ such that $G = \langle a \rangle$.

Definition 1.2.4. Let $a \in G$ with $a^n = e$ for some $n \in \mathbb{N}$. If $a^m \neq e$ for all $0 < m < n$, we say n is the *order of* a and write $|a| = n$. If there is no such n, we say a have infinite order and write $|a| = \infty$.

Proposition 1.2.3. **** Let* G *be a group and* $a \in G$ *with* $|a| = n$*.*

(1) $a^k = e$ *if and only if* $k \equiv 0 \pmod{n}$*.*

(2) $a^i = a^j$ *if and only if* $i \equiv j \pmod{n}$*.*

(3) $|\langle a \rangle| = |a|$*.*

(4) $\langle a^k \rangle = \langle a \rangle$ *if and only if* $\gcd(k, n) = 1$*.*

(5) $\langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle$*.*

(6) ***$|a^k| = \frac{n}{\gcd(k,n)}$*.*

Proof. (1) This is a special case of (2).

(2) ($\Rightarrow$) If $a^i = a^j$, then $a^{i-j} = e$. Apply the division algorithm to $i - j$ and n. Then there exists unique $q, r \in \mathbb{Z}$ such that $i - j = nq + r$, where $0 \leqslant r < n$. Thus:

$$\begin{aligned} e &= a^{i-j} \\ &= a^{nq+r} \\ &= a^{nq} a^r \\ &= a^r. \end{aligned}$$

But since $r < n$, and n is the smallest number such that $a^n = e$, it must be the case that $r = 0$. Thus $i - j = nq$; i.e., $i \equiv j \pmod{n}$.

($\Leftarrow$) If $i \equiv j \pmod{n}$, then $i = j + nq$ for some $q \in \mathbb{Z}$. Thus $a^i = a^{j+nq} = a^j a^{nq} = a^j$.

(3) Suppose $k > n$. Apply the division algorithm to k and n. There exists $q, r \in \mathbb{Z}$ such that $k = nq + r$, $0 \leqslant r < n$. Thus $a^k = a^{nq+r} = a^r$, $0 \leqslant r < n$. If $a^i = a^j$ where $0 \leqslant i < n$ and $0 \leqslant j < n$, then $a^{i-j} = e$. Clearly $i - j < n$, and since n is the smallest number such that $a^n = e$, it must be the case that $i - j = 0$. Hence $i = j$. From these two observations, we can deduce that $\langle a \rangle = \{e, a, a^2, ..., a^{n-1}\}$. Thus $|\langle a \rangle| = n = |a|$.

(4) This is a special case of (5)

(5) Let $a^b \in \langle a^k \rangle$. Then $a^b = a^{ky}$ for some $y \in \mathbb{Z}$. Note that $\gcd(n,k) \,\big|\, n$ and $\gcd(n,k) \,\big|\, k$. So there exists $u \in \mathbb{Z}$ such that $\gcd(n,k) \cdot u = k$. This gives:

$$\begin{aligned} a^b &= a^{ky} \\ &= a^{\gcd(n,k) \cdot uy} \\ &= \left(a^{\gcd(n,k)}\right)^{uy} \in \langle a^{\gcd(n,k)} \rangle. \end{aligned}$$

Hence $\langle a^k \rangle \subseteq \langle a^{\gcd(n,k)} \rangle$. Now let $a^b \in \langle a^{\gcd(n,k)} \rangle$ Then $a^b = a^{\gcd(n,k) \cdot y}$ for some $y \in \mathbb{Z}$. There exists $s, t \in \mathbb{Z}$ such that $\gcd(n,k) = ns + kt$. This gives:

$$\begin{aligned} a^b &= a^{\gcd(n,k) \cdot y} \\ &= a^{nsy + kty} \\ &= a^{nsy} a^{kty} \\ &= \left(a^k\right)^{ty} \in \langle a^k \rangle. \end{aligned}$$

Hence $\langle a^{\gcd(n,k)} \rangle \subseteq \langle a^k \rangle$. Thus $\langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle$.

(6) ***First note that:

$$\begin{aligned} \left(a^k\right)^{\frac{n}{\gcd(k,n)}} &= \left(a^n\right)^{\frac{k}{\gcd(k,n)}} \\ &= e^{\frac{k}{\gcd(k,n)}} \\ &= e. \end{aligned}$$

Now suppose $0 < m < \frac{n}{\gcd(k,n)}$. Then $0 < m \cdot \gcd(k,n) < n$. Since $|a| = n$, it must be the case that $\left(a^{\gcd(k,n)}\right)^m \neq e$. We showed in (4) that $\langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle$. Since $\left(a^{\gcd(k,n)}\right)^m \in \langle a^{\gcd(k,n)} \rangle$, it must be the case that $\left(a^k\right)^m = \left(a^{\gcd(k,n)}\right)^m \neq e$. Thus $\frac{n}{\gcd(k,n)}$ is the smallest number such that $\left(a^k\right)^{\frac{n}{\gcd(k,n)}} = e$, hence $|a^k| = \frac{n}{\gcd(k,n)}$. □

Theorem 1.2.4. **** Let G be a finite cyclic group.*

(1) Any subgroup of G is cyclic.

(2) If $H \leqslant G$, then $|H| \,\big|\, |G|$

*(3) ***For any divisor $d \,\big|\, |G|$, there is a unique subgroup $H \leqslant G$ so that $|H| = d$.*

Proof. (1) Let $H \leqslant G$ be nontrivial. Since G is cyclic, there exists $a \in G$ such that $\langle a \rangle = G$. Let m be the smallest positive integer so that $a^m \in H$. It is clear that $\langle a^m \rangle \subseteq H$. Let $a^n \in H$

with $n > 0$. Write $n = mq + r$ for some $q, r \in \mathbb{Z}$, $0 \leqslant r < m$. Then:

$$\begin{aligned} a^r &= a^{n-mq} \\ &= a^n(a^m)^{-q} \\ &\in H. \end{aligned}$$

Since m is the smallest positive integer such that $a^m \in H$, it must be the case that $r = 0$. Thus $a^n = (a^m)^q \in \langle a^m \rangle$; i.e., $H \subseteq \langle a^m \rangle$. Since $H = \langle a^m \rangle$, H is cyclic.

(2) Since G is cyclic, there exists $a \in G$ such that $\langle a \rangle = G$. Let m be the smallest positive integer such that $a^m \in H$. By the same construction in (1) we have $H = \langle a^m \rangle$. By Proposition 1.2.3, we have:

$$\begin{aligned} |H| &= |\langle a^m \rangle| \\ &= |a^m| \\ &= \frac{|a|}{\gcd(m, |a|)} \\ &= \frac{|\langle a \rangle|}{\gcd(m, |a|)} \\ &= \frac{|G|}{\gcd(m, |a|)}. \end{aligned}$$

Since $|H| \cdot \gcd(m, |a|) = |G|$, we've shown $|H| \,\big|\, |G|$.

(3) *** □

§ 1.3. Homomorphisms and Isomorphisms

Definition 1.3.1. Let G and H be groups. A *group homomorphism* is a map $\varphi : G \to H$ that satisfies $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ for all $g_1, g_2 \in G$. If in addition φ is bijective, we say that φ is a *group isomorphism*. If φ is a group isomorphism between G and H, we say G is *isomorphic* to H, and write $G \cong H$.

Example 1.3.1. Let G be a cyclic group of order n. Then there exists $a \in G$ such that $\langle a \rangle = G$. Define $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$ by $[x]_n \mapsto a^x$. This is an isomorphism.

Proposition 1.3.1. *Let* $\varphi : G \to H$ *be a homomorphism. Then for all* $g \in G$*:*

(1) $\varphi(e_G) = e_H$

(2) $\varphi(g^n) = \varphi(g)^n$

(3) $|\varphi(g)| \,\big|\, |g|$

(4) $\varphi(g^{-1}) = \varphi(g)^{-1}$

Proof. We only prove (3). Let $|g| = m$. We have:

$$\begin{aligned} \varphi(g)^m &= \varphi(g^m) \\ &= \varphi(e_G) \\ &= e_H. \end{aligned}$$

Since $\varphi(g)^m = e_H$, we have $|\varphi(g)| \,|\, m$. □

Definition 1.3.2. Let $\varphi : G \to H$ be a group homomorphism.

(1) The *kernel* of φ is $\ker\varphi = \{g \in G \mid \varphi(g) = e_H\}$.

(2) The *image* of φ is $\operatorname{im}\varphi = \{\varphi(g) \mid g \in G\}$.

Proposition 1.3.2. *Let* $\varphi : G \to H$ *be a group homomorphism.*

(1) $\ker\phi \leqslant G$

(2) $\operatorname{im}\phi \leqslant H$

(3) $\ker\varphi = \{e_G\}$ *if and only if* φ *is injective.*

(4) $\operatorname{im}\varphi = H$ *if and only if* φ *is surjective.*

Proof. (1) Note that $\ker\varphi \neq \emptyset$ since $\varphi(e_G) = e_H$. Let $g_1, g_2 \in \ker\varphi$. Observe that:

$$\begin{aligned}\varphi(g_1 g_2^{-1}) &= \varphi(g_1)\varphi(g_2^{-1})\\ &= \varphi(g_1)\varphi(g_2)^{-1}\\ &= e_H.\end{aligned}$$

Thus $g_1 g_2^{-1} \in \ker\varphi$, giving $\ker\varphi$ as a subgroup of G.

(2) Let $h_1, h_2 \in \operatorname{im}\varphi$. Then there exists $g_1, g_2 \in G$ with $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$. We have:

$$\begin{aligned}h_1 h_2^{-1} &= \varphi(g_1)\varphi(g_2)^{-1}\\ &= \varphi(g_1)\varphi(g_2^{-1})\\ &= \varphi(g_1 g_2^{-1}).\end{aligned}$$

Whence $h_1 h_2^{-1} \in \operatorname{im}\varphi$, giving $\operatorname{im}\varphi$ as a subgroup of H.

(3) Let $\ker\varphi = \{0\}$. Let $g_1, g_2 \in G$ and suppose $\varphi(g_1) = \varphi(g_2)$. Then $\varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1 g_2^{-1}) = e_H$. It must be that $g_1 g_2^{-1} = e_G$, giving $g_1 = g_2$. Conversely, suppose φ is injective and let $g \in \ker\varphi$. Then $\varphi(g) = e_H = \varphi(e_G)$. Hence $g = e_G$, establishing $\ker\varphi = \{e_G\}$.

(4) This is by definition of surjectivity. □

Example 1.3.2. The map $\varphi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ defined by $\varphi(a) = [a]_2$ is a well-defined homomorphism. In particular:

$$\begin{aligned}\ker\varphi &= \{m \in \mathbb{Z} \mid \varphi(m) = [0]_2\}\\ &= \{m \in \mathbb{Z} \mid [m]_2 = [0]_2\}\\ &= \{m \in \mathbb{Z} \mid m \equiv 0 \pmod 2\}\\ &= \{m \in \mathbb{Z} \mid m = 2k,\ k \in \mathbb{Z}\}\\ &= 2\mathbb{Z}.\end{aligned}$$

Example 1.3.3. The map $\varphi : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ defined by $\varphi([a]_{10}) = [a]_2$ is a well-defined homomorphism. In particular, one can prove that $\ker\varphi = \{[m]_{10} \in \mathbb{Z}/10\mathbb{Z} \mid [m]_2 = [0]_2\} = 2\mathbb{Z}/10\mathbb{Z}$.

§ 1.4. Cosets, Normal Subgroups, and Quotient Groups

Definition 1.4.1. Let G be a group, $g \in G$ and $H \leqslant G$. A left (resp. right) *coset* of g is the set $gH = \{gh \mid h \in H\}$ (resp. $Hg = \{hg \mid h \in H\}$). The collection of left (resp. right) cosets is denoted $G/H = \{gH \mid g \in G\}$ (resp. $H \setminus G = \{Hg \mid g \in G\}$).